Indian Journal of Science and Technology, *Vol 7(S4), 80–85, April 2014*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Enhancement of Information Hiding in Audio Signals with Efficient LSB based Methods

P. Rameshkumar[1*], M. Monisha and B. Santhi

[1]School of Computing, SASTRA University, Thanjavur, Tamil Nadu- 613401, India;
rameshkumar6410@gmail.com. , monisha2990@gmail.com, shanthi@cse.sastra.edu

Abstract

In the modern era the easiness in the content alteration and copying in an available digital domain have enriched the security of academic copyrights as well as the anticipation of the illegal inference of data of multimedia have turned into a significant research and technological issue. Steganography is called as an art of secret and secured communication. The basic idea behind this paper is to find the best way to embed text data in audio file using the steganography techniques. Our proposed method uses LSB technique only in specific bit positions which are known only to sender and receiver. Our results have shown that the quality of the audio remains same after embedding the secret text and also very less difference between the original audio and steganographed audio. These results were obtained by the estimation of PSNR, MSE and audio features such as Pitch, Entropy and Flatness etc. The size of the audio signal also remains unaltered.

Keywords: Information Hiding, LSB, MSE, PSNR, Stegnography

1. Introduction

In current trends Information and communication technology main challenge is securing data transmit from one end to the other[1]. There are two traditional approaches which are able to give a safe communication of an audio signal: hiding the signal (steganography) or encrypting the signal[2]. In the second approach, there is a risk that the audio signal may lead to some noise data. In this paper the first case that is technique of data hiding or stegnography is a secretive transmission technology is used to embed an audio file using text data in using steganography technique. Some method embeds text data in sound system using the some properties of Human Auditory System (HAS)[3]. Nowadays, Steganography agrees with a lot of electronic mediums before physical objects in which these Medias have used to digitally embed the messages likely network traffic, hyper text, plain text, video, still images or audio, etc. "Stegnography" is a Greek word which means "Secret or covered writing"[4]. There are three basic methods for steganography as injection, substitution and generation. Audio steganography has various applications like digital watermarking, access control, covert communication, etc. Already there are lots of audio steganography techniques have been used in hiding the data. Such techniques are Echo hiding, LSB technique, Parity coding, Spread Spectrum. In this paper Least Significant Bit (LSB) technique is involved. LSB is one of the existing techniques used to embed data in the audio file[5]. It can be done by substituting the binary digits at the Least Significant Bit. Using this technique large volume of data is able to encode. Data hiding in LSB of an audio sample is the simplest algorithms with the highest data rate of supplementary information. The main aim of this paper is to provide a secure transmission of text data through an audio file using steganography technique of the LSB. The text data is hidden in a secret position which may be known only by the sender and receiver. The features of the audio signal and our enhanced audio signal are compared to show no alteration.

*Author for correspondence

2. Related Works

Kekre et al.[5] proposed two new approaches for audio steganography using the substitution technique in LSB coding, improving the ability of cover audio in order to embed additional data. These methods used utilized 7 LSBs rather than 4 LSBs and shown the result as those methods have improved the ability of cover audio with data hiding at the rate of 35% to 70%. They have limited their work as there are diverse amount of bits have tossed in the samples of audio as well as opponent are not able to recognize accurately that number of bits were used by the data. Juhi Saurabh and Asha Ambhaikar[6] presented an approach to overcome the problems that are related to substitution technique. As a first approach they have used RSA encryption algorithm for encrypting the messages and secondly, encoded those data into an audio file using Genetic Algorithm based LSB. In order to reduce alteration GA operators have also been used. As a result, they have shown important improvements in robustness next to signal processing, treatment, so that secret bits have to be embedded in LSB higher layers and also deeper compared to be in the standard LSB method.

Adhiya et al. and Patil[3] proposed a method for hiding text data within an audio file employing steganography technique of the LSB. Using this system the ability of stego system for hiding the text increases. They have done performance evaluation using the basis of MOS and compared SNR with already existing algorithm and their proposed algorithm. This method required only less capacity to store data and resulted well for 16 bit WAV audio file. Dora M et.al[2] has proposed a hiding method speech-in-speech in the wavelet area as it is appropriate for real-time execution on FPGA. A condensed signal of speech has been concealed about the coarse-host's also the key in the detail-host's of the coefficients.

Bhowal et al.[7] presented a principled approach to overcome the remained problems that are related to the substitution technique of audio steganography using RSA algorithm to encrypt the data and to embed the data into audio file used GA algorithm based LSB algorithm where data are embedded into the higher LSB positions at random. Finally GA operators are used to avoid the distortions. Results shown as rising the deepness of the embedding layer to random LSB higher layers from lower lacking distressing of the perceptual simplicity of the audio signal in steganography. Kumar and Anuradha[8] proposed some techniques in which the audio file has been sampled first and then particular bit is modified. They have shown that their method does not affect the size of the audio file.

Kekre et al.[9] proposed two novel approaches of replacement technique of audio steganography that enhances the capability of covert audio for embedding additional hidden data. These methods utilize up to 7LSBs for embedding the hidden data. And their result shows that capacity has increased up to 35% to 70% as compared to the standard data hiding algorithm which utilizes 4LSBs for embedding the data.

3. Proposed Approach

The proposed approach of LSB based audio Stegnography is as shown in Figure1. The proposed approach consists of following steps in the sender (Encoding) and receiver (decoding) side.

3.1 Encoding Algorithm: At Sender Side

Refer Figure 1(a)

1. Select the audio sample on which the text is to be embedded ("Test1.wav").
2. Removing the noises in the selected audio sample in order to improve accuracy.
3. Identify the positions (square, triangle, circle, etc...) on the audio sample on which the secret text is to be hidden (unique technique).
4. Convert the numbers of identifying positions as 8-bit binary number and identify the LSB on it.
5. Convert the secret text ("Hello SASTRIAN") in to 8-bit binary numbers.
6. Insert the binary value of secret text into the identified LSB of audio sample as done in step 4. First 8-bits of identifying LSB contain the value of the size of text to be hidden.
7. Repeat till the whole secret text is embedded into audio sample.

3.2 Decoding Algorithm: At Receiver Side

Refer Figure 1(b)

1. Receive the stenographic audio sample from sender on which the text is hidden.
2. Identify the positions on which the text is hidden. (Positions should be same as in sender side)

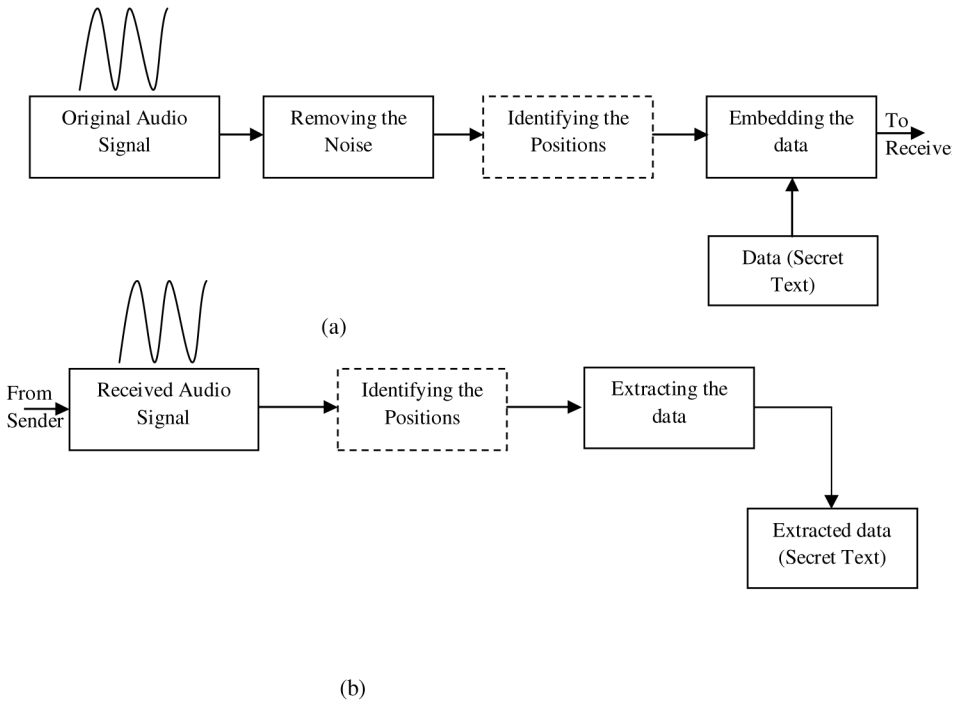


Figure 1. The proposed framework of hiding secret text inside the audio file. (a) Sender Side and (b) Receiver Side.

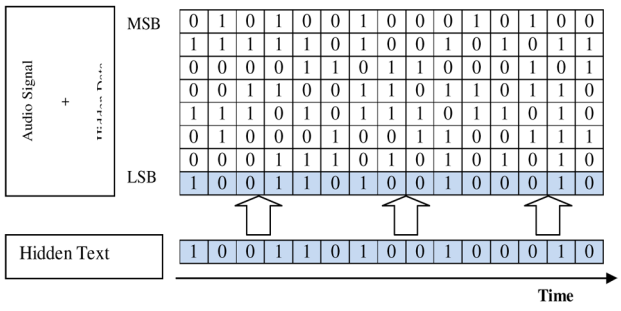


Figure 2. LSB in 8 bits per audio signal is overwritten by one bit of the hidden data.

3. Convert the identified position's value in to 8-bit binary value.
4. LSB of first eight identified positions is used to calculate the size of text hidden.
5. Retrieve the LSB of remaining identified positions until a complete size of hidden text.
6. Convert the binary numbers to string format in order to obtain the original text.

3.3 LSB Encoding

The LSB encoding method is one of the most primitive methods used in the information hiding[10]. Conventionally, it involves the inserting each bit of the message (hiding text) into the least significant bit positions of audio sample in a deterministic way as shown in Figure2. The advantage of using the LSB method is that it allows large amount of data can be embedded into the cover audio signal and also it is comparatively easier to implement than other hiding techniques[11]. On the other hand, this LSB method is portrayed by having less robustness to the noise additions. In order to increase the holding capacity while reducing the error, Cvejic and Seppiinen[9] introduced minimum error-replacement technique of four bits embedding per sample. The error of embedding is then inserted on the next four bits. In order to increase strength of LSB method beside the alteration and noise addition, Cvejic and Seppiinen[12] has improved the process of embedding layer from 4th to 6th and to 8th layers of cover signal without disturbing the perceptual transparency of the stenographic audio signal. In[12] they used only the sixth position in the sixteen bit audio sample of original host signal was replaced by the message bits. For example, if the audio signal sample value is 4 which have binary representation as '0100' and the message bit to be hidden is '1' then after hiding it will look like '0101'. The above sample shows that produce values is much closer to the original value, thus it has only very less impact on the stegno audio signal with respect to its original

signal properties[13]. And also if the bit positions increase to MSB then the difference value between the original and stegno audio signal will increase exponentially. For these purposes LSB embedding is preferred. There are several latest techniques had been introduced in order to increase the capacity of hidden text and also the security of hidden text[14]. The next section contains proposed novel technique of selected bit position embedding which further enhances the security of hidden text.

3.4 Identifying Specific Positions

This is the proposed techniques which involve the selection of particular positions in the original audio sample. The selection of particular position may also based on different shapes like square, triangle, rectangle, hexagonal, circle etc Figure 3(a). The position is identified based on the intersection of the matrix cells and shapes as shown in Figure. The shapes used must be secure and only known to the sender and receiver only. For robustness more than one shape can be used. In our method we have used square shape and identified the particular positions and inserted the bits of hidden text in the selected positions Figure 3 (b). Embedding procedure is same as explained above in LSB encoding. If the data to be hided is large, then recursively utilize the same shapes towards the inner as shown in Figure c. The first 8-bit positions were utilized to store the size of the hidden text embedded in the cover signal. For our experiments we have taken the audio signal (cover signal) "Test1.wav" of size 547kb and then the secret data embedded in the cover signal is "Hello SASTRIAN". The secret data can also be the name of the music artists of the taken audio signal.

4. Performance Measures

The proposed method's efficiency against robustness and other factors was determined by using the PSNR, MSE,

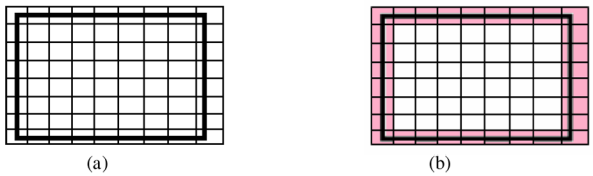


Figure 3. (a) Identified Positions based on shape (eg., square).
(b) Colored position indication in which the hidden data is embedded.

Spectrogram and also other audio features such as pitch, in-harmonicity, root mean square energy and relief. This audio feature estimates the difference between the original audio signal and stego audio signal. In our method both the values of original audio and stego audio were same, its shows that our proposed method is more robust.

4.1 Mean Square Error (MSE)

The MSE determines the Mean Square Error which represents the cumulative squared error between the original audio and stegnographed audio. The lower the MSE represents the less error. It is computed using the formula where I denotes the original audio and K denotes the stegnographed audio signals,

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j)-k(i,j)\right]^2$$

where, m, n is signal size.

4.2 Peak Signal to Noise Ratio (PSNR)

The PSNR determines the Peak Signal to Noise Ratio in decibels between two audio signals. This computed ration is normally used as quality measurement between the original audio and stegnographed audio. The higher PSNR represents the best quality. It is computed using the below formula, where MAX_I represents the maximum possible value of the audio signal, in our result the used sample music signal has the MAX_I value of 0.5009,

$$PSNR = 20.\log_{10}\left(MAX_I\right) - 10.\log_{10}\left(MSE\right)$$

4.3 Audio Features

4.3.1 Root Mean Square Energy

Calculation of the overall energy of the signal x can be cut down by considering the square of the amplitude's average root, principally called as Root-Mean Square Energy (RMS).

4.3.2 Low Energy

Energy curve is used to obtain the evaluation for distribution of energy in temporal. To observe either it remains the same throughout the signal, or if frames are more constrained than others. One of the best ways is computing the Lower Energy rate, i.e., the percentage of frames showing less than average energy.

4.3.3 Rolloff

One of the ways to fairly accurate high frequency quantity in the signal which comprises of analysing the frequency with the aim of the total energy fraction is inhibited below the approximated frequency[15].

4.3.4 Brightness

Dual methods which emphasis on fixing are that cut-off frequency and assess the amount of energy above that frequency[16].

4.3.5 In-harmonicity

The measure of partials that are not belongs to the multiples of the fundamental frequencies are called as Inharmonicity which values between 0 and 1[17].

4.3.6 Flatness

The flatness designates whether the distribution is spiky or smooth and simple ratio that results between the geometric mean and the arithmetic mean[18].

4.3.7 Pitch

Discretized note events or as continuous pitch curves were returned from the extra pitches.

4.4 Quality Measures:

Refer Table 1 and Table 2.

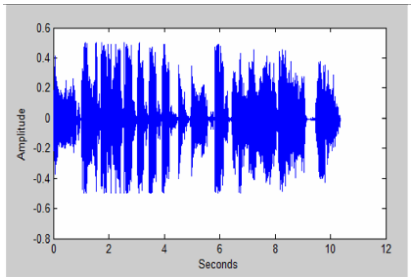
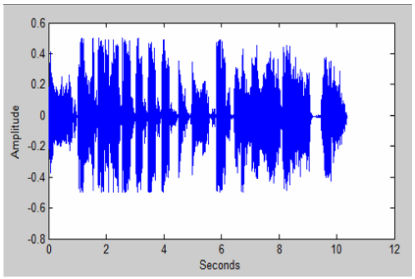
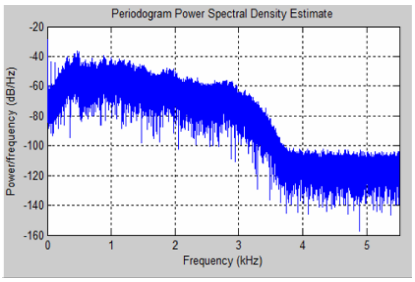
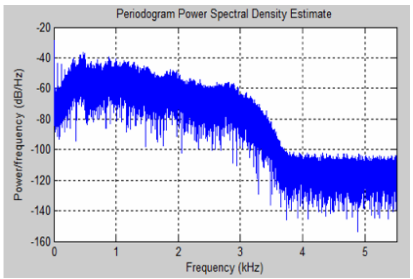
Table 1. PSNR and MSE Values

Measures	Value
PSNR	119.5043
MSE	1.2801e-13

5. Conclusion

In the view of enhancing the protection of digital data content, new and enhanced steganography methods were evolved by the researchers. In this kind audio steganography address the issues concerning the protection of data hidden over the audio. The data hidden may be related to audio (which includes artist name, specifications, etc.) or

Table 2. Comparison of several features between Original Audio Signal and Stegnographed Audio Signal

Features	Original Audio Signal	Stegnographed Audio Signal
Timing Diagram		
PowerSpectral Density		
Pitch	388.3061	388.3048
RMS	0.11471	0.11479
RollOff	2036.9064	2036.9004
In-Harmonicity	0.47734	0.47700
Flatness	0.10701	0.10710

any other secret messages. The main intent is to protect the data and also only very less distortion to the original audio so that the secret embedding will not be over-hauled[14]. Our proposed method addresses these security issues by adding only at specified bit positions which is only known to the sender and receiver. Our experimental results show that audio features (Pitch, RMS, Rolloff, Flatness, etc.,) of the original audio signal and stegno audio signal has no difference in values, which means there is no distortion of the audio signal. And also the size of the stegno audio remains the same as original that is our method shows higher PSNR value. The proposed method of using LSB addresses the enhancement of information security using specified bit positions, the using of LSB, which also addresses the hiding capacity this paper only addresses the increasing information security, and hence the capacity of hiding text can also be extended to the future works. In future work the above mentioned LSB specific location embedding can be further extended with the DWT transform domain embedding at various levels.

6. References

1. Cvejic N, Seppanen T. Increasing the capacity of LSB-based audio steganography. IEEE Workshop Multimedia Signal Processing. 2002 Dec. 336, 338:9–11.
2. Dora M, Ballesteros L, Juan M, Moreno A. Real-time, speech-in-speech hiding scheme based on least significant bit substitution and adaptive key. Journal on Computers and Electrical Engineering. 2013; 39:1192–203.
3. Adhiya KP, Patil SA. iding text in audio using LSB based steganography. Journal of Information and Knowledge Management. 2012; 2(3).
4. Anuradha, Kriti, Harish. Audio steganography step toward the secure data transmission: an overview. National Conference on Emerging Computing Technology (NCECT); 2010.
5. Kekre HB, Athawale A, Rao BS, Athawale U. Increasing the capacity of the cover audio signal by using multiple LSBs for information hiding. IEEE International Conference on Emerging Trends in Engineering and Technology; 2010.
6. Saurabhi J, Ambhaikar A. Audio steganography using RPrime RSA and GA based LSB algorithm to enhance security. International Journal of Science and Research. 2012 Nov; 1(2).
7. Bhowal K, Pal AJ, Tomar GS, Sarkar P. Audio steganography using GA. International Conference on Computational Intelligence and Communication Networks; 2010.
8. Kumar H, Anuradha. Enhanced LSB technique for Audio Steganography. Proceedings of International Conference on Computing, Communications and Networking Technologies; 2012 Jul.
9. Cvejic N, Seppiinen T. Increasing the capacity of, LSB-based audio steganography. IEEE Workshop on Multimedia Signal Processing; 2002. p. 336–38.
10. Bender W, Gruhl D, Morimoto N, Lu A. Techniques for data hiding. IBM System Journal. 1996. 35(3 and 4):313–36.
11. Gopalan K. Audio steganography using bit modification. Proceedings of the IEEE 2003 International Conference on Acoustics, Speech, and Signal Processing; 2003 Apr; Hong Kong.
12. Cvejic N, Seppanen T. Increasing robustness of LSB audio steganography using a novel embedding method. Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC04). 2004; Washington, DC, USA. p. 533.
13. Cvejic N, Seppanen T. Reduced distortion bit-modification for LSB audio steganography. Journal of Universal Computer Science. 2005; 11(1):56–65.
14. Ahmed MA, Kiah LM, Zaidan BB, Zaidan AA. 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. 2010; 10:59–64.
15. Li T, Ogihara M. Music generic classification with taxonomy. Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing. 2005 Mar; 5: 197–200.
16. Liu M, Wan C. A study on content based classification and retrieval of audio database. Proceedings of International Symposium on Database Engineering and Applications; 2001 Jul:339–45.
17. Agostine G, Longari M, Pollastri E. Musical instrument timbres classification with spectral features. EURASIP JASP. 2003 May:5–14.
18. Ramalingam A, Krishanan S. Gaussian mixture modelling using short time fourier transform features for audio finger printing. Proceedings of IEEE International Conference on Multimedia and Expo; 2005 Jul. p. 1146–149.