Journal of Electronicsl and Communication Engineering (IOSR-JECE)
ISSN: 2278-2834-, ISBN: 2278-8735, PP: 12-16
www.iosrjournals.org

A Optimized and Secure Audio Steganography for Hiding Secret Information - Review

Sheetal A. Kulkarni[1], Dr. Shubhangi B. Patil[2] , Prof B.S.Patil[3]

[1]*(Assistant Professor, Instrumentation & Control Department, Cummins College of Engineering for Women/ Pune University, India)*
[2]*(Professor, Head, Electronics Engineering Department, Dr. J.J. Magdum College of Engineering, Jaysingpur/ Shivaji University, India)*
3.(Head,IT Department,P.V.P.I.T.,Budhgaon)

ABSTRACT: *In the current internet community, secure data transfer is limited due to its attack made on data communication. So more robust methods are chosen so that they ensure secured data transfer. One of the solutions which came to the rescue is the audio Steganography. Commonly used techniques for audio steganography are temporal domain and transform domain techniques, where the frequency domain techniques and wavelet domain techniques come under transform domain.. Among the techniques studied wavelet domain shows high hiding capacity and transparency. In wavelet domain different techniques are applied on the wavelet coefficients to increase the hiding capacity and perceptual transparency. Leaning towards designing a system that ensures high capacity or robustness and security of embedded data has led to great diversity in the existing steganographic techniques. In this paper, we present a current state of art literature in digital audio steganographic techniques. We explore their potentials and limitations to ensure secure communication. A comparison and an evaluation for the reviewed techniques is also presented in this paper.*

Keywords - *Digital data security, audio steganography, information hiding, ,stego signal, Embedding*

I. INTRODUCTION

Steganography, which means “covered writing” has drawn more attention in the last few years. Its primary goal is to hide the fact that a communication is taking place between two parties. The sender embeds secret data of any type using a key in a digital cover file to produce a stego file, in such a way that an observer cannot detect the existence of the hidden message. At the other end, the receiver processes the received stego-file to extract the hidden message. An obvious application is a covert communication using innocuous cover audio signal, such as telephone or video conference conversations.

To minimize the difference between the original medium and the one obtained after embedding the hidden data, recent steganography techniques benefit from the natural limitations in the auditory and visual perceptions of human in one hand, and on the other hand from the properties of digital media through utilizing them as a cover to vehicle secret communications. Image and video based steganography relies on the limited human visual system in remarking luminance variation at levels greater than 1 in 240 in uniform gray levels or 1 in 30 of random patterns [1]. However, audio-based steganography exploits the masking effect property of Human Auditory System (HAS). Various features influence the quality of audio steganographic methods. The importance and the impact of each feature depends on the application and the transmission environment.

The most important properties include robustness to noise and to signal manipulation, security and hiding-capacity of embedded data. Robustness requirement is tightly related to the application and is the most challenging to satisfy in a steganographic system. In addition, there is a tradeoff between robustness and hiding-capacity. Generally, they hardly coexist in the same steganographic system.

In this review, the use of audio files as a cover medium to vehicle secret communications is thoroughly investigated. Several works in audio steganography are discussed in this paper. The reminder of this paper is organized as follows:

Latest audio steganography techniques and their performance analysis are presented in Sections II, III, and IV respectively. Finally, conclusion are presented in Section V.

II. TEMPORAL DOMAIN

2.1 LSB Encoding

LSB (Least Significant Bit), it is one of the popular methods used for information hiding. It consists in embedding each bit from the message in the least significant bit of the cover audio in a deterministic way Fig. 1. Thus, for a 16 kHz sampled audio, 16 kbps of data is embedded [2]. The LSB method allows high embedding capacity for data and is relatively easy to implement or to combine with other hiding techniques. However, this technique is characterized by low robustness to noise addition and thus by low security as well since it is very vulnerable even to simple attacks. Filtering, amplifying, noise addition or lossy compression of the stego-audio will very likely destroy the data. An attacker can easily uncover the message by just removing the entire LSB plane. In a simple LSB strategy has been applied to embed a voice message in wireless communication.

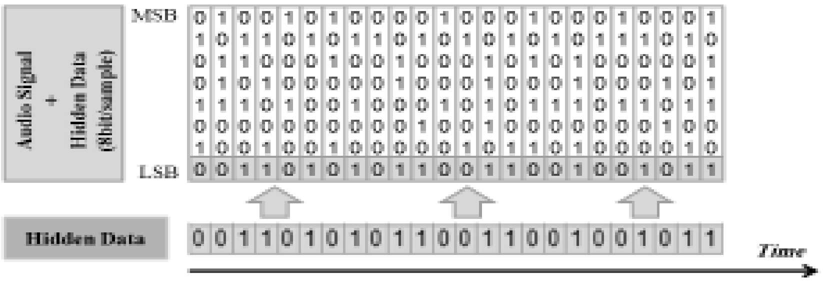


Fig. 1: LSB in 8b/sample signal is overwrote by one bit of the embedded data.

To improve robustness against distortion and noise of LSB method and have increased the depth of the embedding layer from 4th to 6th and 8th LSB layer without affecting the perceptual transparency of the stego audio signal. In [2] only bits at the sixth position of each 16 bits sample of the original host signal are replaced with bits from the message. To minimize the embedding error, the other bits can be flipped in order to have a new sample that is closer to the original one. The fact that the embedding occurs in the eighth bit will slightly increase the robustness of this method compared to the conventional LSB methods. However, the hiding capacity will decrease since some of the samples have to be left unchangeable to preserve the audio perceptual quality of the audio signal.

2.2 Parity coding

One of the prior works in audio data hiding technique is parity coding technique. Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion [3].

2.3 Echo Hiding

Echo hiding technique embeds secret information in a sound file by introducing an echo into the discrete signal. Echo hiding has advantages of providing a high data transmission rate and superior robustness when compared to other methods. Only one bit of secret information could be encoded if only one echo was produced from the original signal. Hence, before the encoding process begins the original signal is broken down into blocks. Once the encoding process is done, the blocks are concatenated back together to create the final signal [4]. To hide the data successfully, three parameters of the echo are varied: amplitude, decay rate and offset (delay time) from the original signal. All three parameters are set below the human hearing threshold so the echo is not easily resolved. In addition, offset is varied to represent the binary message to be encoded.

Due to low embedding rate and low security, no audio steganography system based on echo hiding has been presented in recent researches. Moreover, only few techniques have been proposed for audio watermarking. To improve the watermark system robustness against common signal processing, an interesting echo hiding-time spread technique has been proposed in [3]. Compared to the conventional echo-hiding system, the proposed method detects the watermark bit based on the correlation amount at the receiver not on the delay.

III. TRANSFORM DOMAIN

3.1 Frequency domain

3.1.1 Tone insertion

Frequency masking property is exploited in tone insertion method. A weak pure tone is masked in the presence of a stronger tone. This property of inaudibility is used in different ways to embed information.

By inserting tones at known frequencies and at low power level, concealed embedding and correct data extraction are achieved. The author [5] of this method acknowledges a hiding capacity of 250 bps when four tones are inserted in each speech spectrum. Any attempt to further increase the capacity must use more than four tones. Tone insertion method can resist some of the unintentional attacks such as low-pass filtering and bit truncation. Besides the low embedding capacity, embedded data can be retrieved since inserted tones are easy to detect.

3.1.2 Phase encoding

Phase coding exploits the human audio system insensitivity to relative phase of different spectral components. It is based on replacing selected phase components from the original speech spectrum with hidden data. However, to insure inaudibility, phase components modification should be kept small . It is also noted that among data hiding techniques, phase coding tolerates better signal distortion. Authors in [6] have inserted data in phase components using an independent multi-band phase modulation. In this approach, imperceptible phase modifications are achieved using controlled phase alteration of the host audio. Authors [7] the original sound signal is broken up into smaller segments whose lengths equal the size of the message to be encoded.. Disadvantages associated with phase coding are a low data transmission rate due to the fact that the secret message is encoded in the first signal segment only and to extract the secret message from the sound file, the receiver must know the segment length.

3.1.3 Spread spectrum Spread spectrum technique spreads hidden signal data through the frequency spectrum. Spread Spectrum (SS) is a concept developed in communications to ensure a proper recovery of a signal sent over a noisy channel by producing redundant copies of the data signal. In [8] conventional direct sequence spread spectrum (DSSS) technique was applied to hide confidential information MP3 and WAV audio digital signals. For a better hiding rate of 20 bps, used SS technique in sub-band domain. Appropriately chosen subband coefficients were selected to address robustness problem and resolve synchronization uncertainty at the decoder.

3.1.4 Amplitude modification

The ”masking effect” phenomenon masks weaker frequency near strong resonant frequency. An original method has been proposed in [9] where the original odd magnitude frequency components are interpolated to generate the even samples that are used for embedding data bits. In the receiver, the original odd samples and the interpolated even samples are the same as in the coder. The method has a capacity of 3 kbps and provides robustness against common audio signal processing such as echo, added noise, filtering, resampling and MPEG compression [11].

3.1.5 Cepstral domain

The cover signal is transformed into cepstral domain and data is embedded in selected cepstrum coefficient by applying statistical mean manipulation. In this method, an embedding rate of 20 to 40 bps is achieved while guarantying robustness to common signal attacks. In [8], This method ensured a reliable embedding rate of approximately 54 bits/s and latter algorithm and embed data with different arbitrary frequency components at each frame to improve security.

3.2 Wavelet domain

Audio steganography based on Discrete Wavelet Transform (DWT) is described in [12]. Data is embedded in the LSBs of the wavelet coefficients achieving high capacity of 200 kbps in 44.1 kHz audio signal. To improve embedded data imperceptibility, [13] employed a hearing threshold when embedding data in the integer wavelet coefficients, while avoided data hiding in silent parts of the audio signa

Haider Ismael Shahadi and Razali Jidin,[14] proposes a high capacity and inaudibility audio steganography scheme. The algorithm is based on discrete wavelet packet transform with adaptive hiding in least significant bits. Here the input signal is segmented into G segments. The secret message is also segmented into G segments. The cover signal is decomposed into wavelet coefficients and each detail signals is scaled according to its maximum value and number of bits per sample. For each sample, the algorithm determines the number of bits that can be safely hidden. In the next step the stegano-key is embedded in lowest frequency details signal which makes the stegano-key more resistant against distortion. Then stegano signal is reconstructed. The algorithm has got high hiding capacity and excellent output quality.

Dora M. Ballesteros L and Juan M Moreno A, [15] proposes a paper in wavelet domain based on Efficient Wavelet Masking (EWM). The paper mainly concentrates on speech in speech hiding. EWM is a steganography model which adapts the secret message to the host signal. It uses two principles: the efficient adaptation and masking property of Human Auditory System (HAS). The method in the paper is best suited for speech in speech hiding. Also it uses all of the host coefficients to hide the secret message, instead of a selected group of coefficients in other methods. The method also uses a secret key which adds additional security. In the transmitter end the output will be similar to the carrier with secret message embedded inside. The hacker will be blinded by the transmitted signal [10]. At the receiver end the original message can be retrieved without any loss. The entire proposed system is simulated and their corresponding waveforms prove the effectiveness of this method.

3.3 Encoder domain

When considering data hiding for real time communications, speech codecs such as: AMR, ACELP, SILK at their respective coding rate are employed. Passing through one of the codecs, the transmitted signal is coded and compressed according to the codec rate then decompressed at the decoder end. Authors in [16], [17] have presented a lossless steganography technique for G.711-PCMU telephony speech coder. One bit is embedded in 8 bits speech data whose absolute amplitude is zero. Depending on the number of samples whose absolute amplitudes are 0, a potential hiding rate ranging from 24 to 400 bps is obtained.

IV. AUDIO STEGANOGRAPHY ANALYSIS

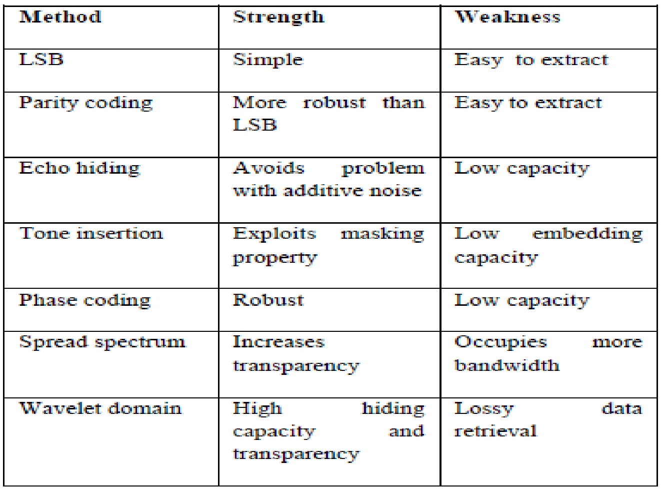
To evaluate the performance of the reviewed techniques, signal-to-noise ratio SNR is utilized [18]. SNR's value indicates the distortion amount induced by embedded data in the cover audio signal s_c (m, n). SNR value is given by the following equation.

$$SNR_{dB} = 10\log_{10}\left(\frac{\sum_{n=1}^{N}|s_c(m,n)|^2}{\sum_{n=1}^{N}|s_c(m,n)-s_s(m,n)|^2}\right) \qquad (1)$$

Where s_s (m, n) is the stego-audio signal such as: m =1…M and n = 1….N , where M is the number of frames in milliseconds (ms) and N is the number of samples in each frame.

To control the distortion induced by the embedding process, most audio steganography methods based on frequency domain use a perceptual model to determine the permissible amount of data embedding without distorting the audio signal [19]. Many audio steganography algorithms use most often frequency masking and auditory masking as the perceptual model for steganography embedding. In addition, some frequency domain approaches, i.e, phase embedding implicitly inherit the phase properties which include robustness to common linear signal manipulations such as : amplification, attenuation, filtering, resampling, etc. [20] The performance of the method is analyzed in terms of MSE (Mean Squared Error), PSNR (Peak Signal-to-Noise Ratio) and SNR (Signal-to- Noise Ratio) [21]. Subjective quality evaluation of these methods can be carried out by performing listening tests and comparing original with audio signal and corresponding stego audio signal.

Table 1. Summary of audio steganography techniques



Method	Strength	Weakness
LSB	Simple	Easy to extract
Parity coding	More robust than LSB	Easy to extract
Echo hiding	Avoids problem with additive noise	Low capacity
Tone insertion	Exploits masking property	Low embedding capacity
Phase coding	Robust	Low capacity
Spread spectrum	Increases transparency	Occupies more bandwidth
Wavelet domain	High hiding capacity and transparency	Lossy data retrieval

V. CONCLUSION

Up to the date the main challenge in digital audio steganography is that audio to audio steganography with high efficiency, lossless and with best security. This paper presents a review of the current state of art literature in digital audio steganography techniques and approaches. We discussed their potentials and limitations in ensuring secure communication. From our point of view, a comparison and an evaluation for the reviewed techniques has been also given. The advantage on using one technique over another one depends strongly on the type of the application and its exigencies such as hiding capacity or the type of attacks that might encounter the transmitted signal.

REFERENCES

[1] Kekre, H.B. , " Increasing the Capacity of the Cover Audio Signal by Using Multiple LSBs for Information Hiding" , *3rd International Conference on Emerging Trends in Engineering and Technology (ICETET)*, 2010.

[2] Muhammad Asad, Junaid Gilani, Adnan Khalid , " An enhanced least significant bit modification technique for audio steganography ", *International Conference on Computer Networks and Information Technology (ICCNIT)*, 2011.

[3] Fatiha Djebbar, Beghdad Ayady, Habib Hamamzand Karim Abed-Meraim, "A view on latest audio stegnography", *International Conference on Innovations in Information Technology*, 2011, pages 409-414.

[4] Jayaram P. , Ranganatha H R. , Anupama H S, " Information hiding using audio steganography – a survey" , *International Journal of Multimedia & its applications* ,Vol.3, No.3, August 2011.

[5] K. Gopalan and S. Wenndt, "Audio steganography for covert data transmission by imperceptible tone insertion", *Proceedings of Communications Systems and Applications*, IEEE, 2004.

[6] M. Nutzinger and J. Wurzer, "A novel phase coding technique for steganography in auditive media", 2011 *Sixth International Conference on Availability, Reliability and Security (ARES)*, IEEE, 2011.

[7] Prof. Samir Kumar, BandyopadhyayBarnali, Gupta Banik, "Lsb modification and phase encoding technique of audio teganography revisited", *International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2012*

[8] Kaliappan Gopalan, "A Unified Audio and Image Steganography by Spectrum Modification", *International Conference on Industrial Technology*, 2009, Page(s):1,5

[9] F. Djebbar, H. Hamam, K. Abed-Maraim, D. Guerchi, "Controlled Distortion for High Capacity Data-in-speech Spectrum Steganography", *6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06),* Germany, Oct 2010.

[10] K. Saktisudan, P. Prabhu, "Secure audio stegnography for hiding secret information", *International Journal of Computer Applications*, 2012.

[11] Masmoudi Salma, ,Charfeddine Maha , Ben Amar Chokri, "A Robust Audio Watermarking Technique based on the Perceptual Evaluation of Audio Quality Algorithm in the Multiresolution Domain", IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), 2010

[12] Jisna Antony, Sobin C.C., Sherly A.P. , "Audio steganography in wavelet domain-A survey", *International Journal of Computer Applications*, volume 52-no. 13, Aug 2012.

[13] S. Nehete, S. Sawarkar, and M. Sohani, "Digital audio steganography using DWT with reduced embedding error and better extraction compared to DCT", *Proceedings of the International Conference & Workshop on Emerging Trends in Technology*, ACM, 2011

[14] Haider Ismael Shahadi and Razali Jidin, "High capacity and inaudibility audio steganography scheme", *7th International Conference n Information Assurance and Security* (*IAS*), IEEE, 2011

[15] D. Ballesteros L and J. Moreno A, "Highly transparent steganography model of speech signals using efficient wavelet masking", *Expert Systems with Applications, Elsevier, 2012*

[16] Naofumi Aoki, "A Technique of Lossless Steganography for G.711 Telephony Speech", International *Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2008)*, pp. 608-611, 2008.

[17] Naofumi Aoki, "A Semi-Lossless Steganography Technique for G.711 Telephony Speech", *International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2010),* pp. 534-537, 2010.

[18] Y. Hu, P. Loizou, "Evaluation of objective quality measures for speech enhancement", *IEEE Transactions on Speech and Audio Processing*, 16(1), 229-238, 2008.

[19] B. Santhi, G. Radhika and S. Ruthra Reka. "Information Security using Audio Steganography -A Survey", *Research Journal of Applied Sciences, Engineering and Technology 4(14)*: 2255-2258, 2012

[20] R Sridevi, Dr. A Damodaram, Dr. SVL. Narasimham , "Efficient method of audio steganography by modified LSB algorithm and strong encryption key with enhanced security," *Journal of Theoretical and Applied Information Technology*, 2009.

[21] Mazdak Zamani, Azizah BT Abdul Manaf, Shahidan M. Abdullah , " Efficient Embedding for Audio Steganography ", *International Journal of models and methods in applied sciences*, 2012