World Applied Programming, Vol (2), No (3), March 2012. 202-205
ISSN: 2222-2510

Audio Steganography: A Survey on Recent Approaches

Masoud Nosrati
Kermanshah University of Medical Sciences, Kermanshah, Iran
minibigs_m@yahoo.co.uk

Ronak Karimi
Kermanshah University of Medical Sciences, Kermanshah, Iran
rk_respina_67@yahoo.com

Mehdi Hariri *
Kermanshah University of Medical Sciences, Kermanshah, Iran
mehdi.hariri@yahoo.com

Abstract: In this study, we will have a survey on audio steganography recent researches. Due to it, some basic concepts of audio steganography and HAS including Least Significant Bit (LSB) Coding, Parity Coding, Phase Coding, Spread Spectrum (SS) and Echo data hiding are covered. In follow, a brief introduction and abstract of 7 recent methods for audio steganography is presented.

Keywords: Steganography, audio, data hiding, coding.

I. INTRODUCTION

The term Steganography is forked from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing” [1]. Steganography is the practice of hiding information “in plain sight”. This technique relies on a message being encoded and hidden in a transport layer in such a way as to make the existence of the message unknown to an observer [2]. The notion of data hiding or steganography was first introduced with the example of prisoners' secret message by Simmons in 1983 [3].
One of Steganography types is using audio files as stego-media [4]. In this study, we are going to have a survey on some published algorithms and methods in this field.
In second section of this study, we will get into HAS features and steganography basic concepts and techniques. In follow, some recent studies in the field of audio Steganography will be introduced. It includes:

- Modifying Quantized Spectrum Values of MPEG/Audio Layer III
- Embedding data between frames in MP3 file
- Quantized frequency domain embedding and reversible integer transforms
- Information hiding in audio signals using Considering Parity and XORing of LSB’s
- Genetic-Algorithm-Based audio steganography
- Increasing robustness of LSB audio steganography
- Audio Wave Steganography

II. AUDIO STEGANOGRAPHY

Watermarking of audio signals is more challenging compared to the watermarking of images or video sequences, due to wider dynamic range of the HAS in comparison with human visual system (HVS) [5]. The HAS perceives sounds over a range of power greater than 109:1 and a range of frequencies greater than 103:1. The sensitivity of the HAS to the additive white Gaussian noise (AWGN) is high as well; this noise in a sound file can be detected as low as 70 dB below ambient level [6].
Some commonly used methods of audio steganography are listed and discussed below in brief [7].

Least Significant Bit (LSB) Coding [8]**:** One of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is LSB coding. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message.

Parity Coding [9]: 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. Advantage: The sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive manner. Disadvantage: This method like LSB coding is not robust in nature.

Phase Coding [9]: Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. It "works by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is then adjusted in order to preserve the relative phase between segments". Disadvantage: It is a complex method and has low data transmission rate.

Spread Spectrum (SS) [8]: It attempts to spread out the encoded data across the available frequencies as much as possible. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. However, unlike LSB coding, the SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission. Advantage: It offers moderate data transmission rate while maintaining a high level of robustness. Disadvantage: It can introduce noise into a sound file.

Echo data hiding [8]: Text can be embedded in audio data by introducing an echo to the original signal. The data is then hidden by varying three parameters of the echo: initial amplitude, decay rate, and offset. If only one echo is produced from the original signal, then only one bit of information could be encoded.

In this part, we will introduce some recent methods for audio Steganography.

Modifying Quantized Spectrum Values of MPEG/Audio Layer III

Proposed method by Beixing Deng *et al.* is able to simultaneously accomplish the information embedding procedure when performing compression of MP3. In this method, modification of some quantized spectrum values of audio layer III to embed secret information into audios is done. The capacity of proposed method is six times as large as that of mp3stego. At the same time, the difference between original audio and audio with secret information is imperceptible. In the experimental results, they hide more characters into audios and extract them correctly. The audios with secret information are indiscernible to human ears.
Beixing Deng *et al.* proposed an audio information-hiding system based on modifying special spectrum lines of MPEG layer III. This scheme has the following characteristics [10].

- In imperceptibility, most people cannot distinguish between the original music and the one with secret information.
- In indefectibility, one cannot extract the correct information without the secret key.
- In hiding capacity, this method has a capacity six times as large as that of mp3stego.
- In extracting procedure, secret information can be extracted without original audio.

Embedding data between frames in MP3 file

Alaa Ismat Al-Attili *et al.* propose a method using the space between frames of mp3 file. Limitation of this method is that the MP3 file must be of CBR type only. But the suggested method satisfies the capacity and complexity of steganography properties. In addition, the suggested method for hiding is robust against noise. It is also considered highly secure since data is encrypted using RSA algorithm before embedding data which makes the system secure especially against passive attack [11].

Quantized frequency domain embedding and reversible integer transforms

Sos S. Agaian *et al.* present two algorithms for secure digital audio steganography. In the first algorithm that is called Quantized-frequency Secure Audio Steganography algorithm (QSAS), they use classical unitary transforms with quantization in the transform domain to embed the secure data. The secure data is embedded in the transform domain coefficients. In the second algorithm that is called Integer Transform based Secure Audio Steganography (ITSAS), they use a reversible integer transform to obtain the transform domain coefficients. In the integer domain they look at the binary representation of the integer coefficients and embed the secure information as an extra bit. Also a capacity measure to select audio carriers that will introduce minimum distortion after embedding is introduced. Experimental results for both methods indicate that the changes in the embedded audio section are inaudible. The QSAS algorithm has lower embedding capacity but has much better SNR values. The ITSAS algorithm is preferred as it is reversible, simple, and efficient with acceptable SNR values [7].

Information hiding in audio signals using Considering Parity and XORing of LSB's

Two novel methods have been proposed by H.B.Kekre *et al.*, one is considering parity of the digitized samples of cover audio and the other is considering the XOR operation.

Considering Parity method uses LSB coding technique for data hiding in audio. However, instead of directly replacing LSBs of digitized samples with the message bits, it first checks the parity of the samples and then carries out data embedding.
Using XORing of LSB's method performs XOR operation on the LSBs and then depending on the result of XOR operation and the message bit to be embedded, the LSB of the sample is modified or kept unchanged. The method described below performs XOR operation on first 2 LSBs. The XORing can be further expanded to 3 LSBs, 4 LSBs upto 16 LSBs so as to increase the level of encryption.
From experimental results, it is seen that the proposed methods are effective. From listening tests, no difference is found between the original audio signal and the stego audio signal. The hidden information is recovered without any error. Also, this approach increases the capacity of the cover audio by as much as 8 times and provides robust encryption [12].

Genetic-Algorithm-Based audio steganography

Mazdak Zamani *et al.* propose the GA for optimizing the steganography using LSB. A new approach is proposed to resolve two problems of substitution technique of audio steganography. First problem is having low robustness against attacks which try to reveal the hidden message and second one is having low robustness against distortions with high average power. Proposed solution is using GA. An intelligent algorithm will try to embed the message bits in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. Using the proposed genetic algorithm, message bits could be embedded into multiple, vague and deeper layers to achieve higher capacity and robustness. Presented solutions are as follow [13]:

1. The solution for first problem: Making more difficult discovering which bites are embedded by modifying the bits else than LSBs in samples, and selecting the samples to modify privately-not all samples.
2. The solution for second problem: Embedding the message bits in deeper layers and other bits alteration to decrease the amount of the error.

Increasing robustness of LSB audio steganography

Nedeljko Cvejic *et al.* present another high bit rate LSB audio watermarking and steganography method. The basic idea of the proposed LSB algorithm is watermark embedding that causes minimal embedding distortion of the host audio. Using the proposed two-step algorithm, watermark bits are embedded into higher LSB layers, resulting in increased robustness against noise addition or MPEG compression. Listening tests showed that the perceptual quality of watermarked audio is higher in the case of the proposed method than in the standard LSB method. The results of subjective tests showed that perceptual quality of watermarked audio, if embedding is done using the novel algorithm, is higher in comparison to standard LSB embedding method. Discrimination values and mean opinion scores in the case of the proposed algorithm embedding in the 6th LSB layer are practically the same as in the case of the standard algorithm embedding in the 4th LSB layer. This confirms that the described algorithm succeeds in increasing the depth of the embedding layer from 4th to 6th LSB layer without affecting the perceptual transparency of the watermarked audio signal [14].

Audio Wave Steganography

Ajay.B.Gadicha1 explores another 4^{th} bit rate LSB audio steganography method that reduces embedding distortion of the host audio. Using the proposed algorithm, Message bits are embedded into 4^{th} LSB layers, resulting in increased robustness against noise addition.
Proposed algorithm: developed a novel method that is able to shift the limit for transparent data hiding in audio from the first LSB layer to the fourth LSB layer, using a two-step approach. In the first step, a watermark bit is embedded into the 4th LSB layer of the host audio using a novel LSB coding method. In the second step, the impulse noise caused by watermark embedding is shaped in order to change its white noise properties.
Proposed method introduces smaller error during watermark embedding. If the 4^{th} LSB layer is used, the absolute error value ranges from 1 to 4 QS, while the standard method in the same conditions causes constant absolute error of 8 QS. The average power of introduced noise is therefore 9.31 dB smaller if the proposed LSB coding method is used. In addition to decreasing objective quality measure, expressed as signal to noise ratio (SNR) value, proposed method introduces, in the second step of embedding, noise shaping in order to increase perceptual transparency of the method [15].

III. CONCLUSION

This review paper got into audio steganography. Basic concepts of audio steganography were mentioned and some recent approaches were investigated. They were: Modifying Quantized Spectrum Values of MPEG/Audio Layer III, Embedding data between frames in MP3 file, Quantized frequency domain embedding and reversible integer

transforms, Information hiding in audio signals using Considering Parity and XORing of LSB's, Genetic-Algorithm-Based audio steganography, Increasing robustness of LSB audio steganography, Audio Wave Steganography..

REFERENCES

[1] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[2] Sridevi R., Damodaram A., 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.

[3] G. J. Simmons, "The prisoners' problem and the subliminal channel" in Proc. Advances in Cryptology (CRYPTO '83), pp. 51-67.Berglund, J.F. and K.H. Hofmann, 1967. Compact semitopological semigroups and weakly almost periodic functions. Lecture Notes in Mathematics, No. 42, Springer-Verlag, Berlin-New York.

[4] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, An introduction to steganography methods, World Applied Programming, Vol (1), No (3), August 2011. 191-195.

[5] Bender W, Gruhl D & Morimoto N (1996) Techniques for data hiding. IBM Systems Journal 35(3): p 313–336.

[6] Nedeljko Cvej, Algorithms for audio watermarking and steganography, Oulu 2004, ISBN: 9514273842.

[7] Sos S. Agaian, David Akopian, Sunil A. D'Souza1, Two algorithms in digital audio steganography using quantized frequency domain embedding and reversible integer transforms, USA.

[8] "audio steg: methods", Internet publication on www.snotmonkey.com http://www.snotmonkey.com/work/school/405/methods.html

[9] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, "A Tutorial Review on Steganography".

[10] Beixing Deng, Jie Tan, Bo Yang, Xing Li, A Novel Steganography Method Based on Modifying Quantized Spectrum Values of MPEG/Audio Layer III, Proceedings of the 7th WSEAS International Conference on Applied Informatics and Communications, Athens, Greece, August 24-26, 2007.

[11] Alaa Ismat Al-Attili, Osamah Abdulgader Al-Rababah, New technique for hiding data in audio file, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.7, July 2010.

[12] H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale, Information Hiding in Audio Signals, International Journal of Computer Applications (0975 – 8887) Volume 7– No.9, October 2010.

[13] Mazdak Zamani, Azizah A. Manaf, Rabiah B. Ahmad, Akram M. Zeki, and Shahidan Abdullah, A Genetic-Algorithm-Based Approach for Audio Steganography World Academy of Science, Engineering and Technology 54 2009.

[14] Nedeljko Cvejic, Tapio Seppänen, Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04).

[15] Ajay.B.Gadicha1, Audio Wave Steganography, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-5, November 2011.