Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Audio Contents Protection Using Invisible Frequency Band Hiding Based on Mel Feature Space Detection: A Review

Shefali Rani
M.Tech Department of Computer Science,
BGIET, Sangrur, India

Yogesh Kumar
Asst Prof. of CSE Department
BGIET, Sangrur, India

Abstract - In this proposed system of audio steganography we have implemented a new scheme based on mel frequency components. The mel frequency cepstrum coefficients are used for finding the unique feature audio data in audio file. The returned features provide us with highly robust and high end features with low invariance. We have used this property of MFCC in order to detect high bandwidth free space location in the sound data and have embedded the encrypted watermark image data into these MFCC components. The proposed scheme works to increase the PSNR values and reduce the error rate of hiding the data in the image and thus improves the sound quality and makes it look original. The effect of MFCC is positive as the watermark extracted from this proposed scheme shows high correlation to the original watermark and also the resistance towards various attacks has also been improved, the attacks degrade the watermark due to high payload or bigger watermark size, the probability of extraction of watermark or steganograph data becomes higher.

Keywords— Steganography, Information hiding, Audio Steganography, MFCC

I. INTRODUCTION

Now-a-days digital communication is widely used for transmitting the information and most of the applications are based on the internet as for the communication purpose, people uses the internet and hence it also increases the risks of attack like stealing the information by an unauthorised user on the data. Hence, security plays an important role when it comes to communication purpose. Security is basis on the various factors such as encoding decoding of data, confidentiality of data and authentication. To achieve the security of the digital data, the encryption and data hiding is used [1].

II. STEGANOGRAPHY

Audio data hiding or the term steganography is derived from the "stegos" that indicates the "cover" and "grafia" that indicates "writing or drawing" which defines as "covered drawing or writing" [2]. The steganography system contains the cover file such as image, text, audio or video and the secret message which is embedded within the cover file and by this secret message is concealed and then produces the stego file which is similar to cover file that cannot be detected or changed easily [3]

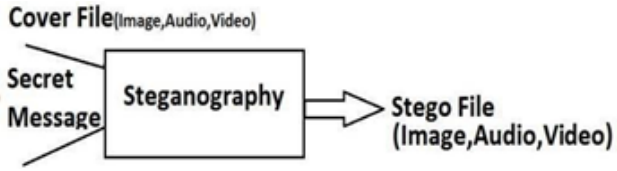

Fig 1 Process of Steganography

III. AUDIO STEGANOGRAPHY

Audio Steganography is the method of embedding the information in sound files like wav file. In computer –based audio steganography system, private messages are hidden in the digital audio file. The secret messages are embedded by replacing the binary sequence of the audio file. The formats of audio steganography are wav, au and mp3 sound [4].

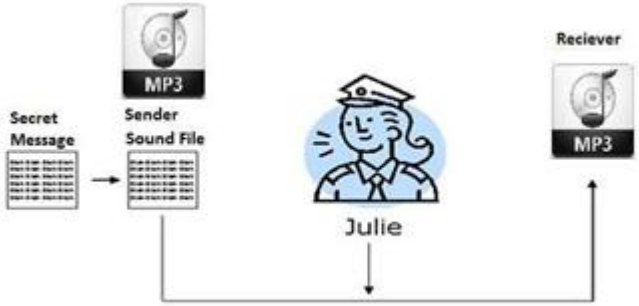

Fig 2 Secret message behind MP3

IV. TECHNIQUES of AUDIO STEGANOGRAPHY

There are various different techniques that have been used for hiding the secret data in audio signals such that an unauthorized user cannot able to detect that message. The techniques are:

LSB (Least Significant Bit) Coding: - LSB algorithm is used to replaces the least significant bit with some bytes of the cover object so as to embed the number of bytes which contains the secret message. In this figure, the 'HEY' message is embedded in a 16-bit audio file with the use of the LSB method. In this example, 'HEY' is the secret message and the sound file is used as the host file. HEY is hidden in the music file. The first step is to convert the 'HEY' and the audio file in the form of bits. The last bits of the least significant bit are replaced with the bits of the secret message 'HEY'. After hiding the secret message 'HEY', the stego-file is obtained [5].

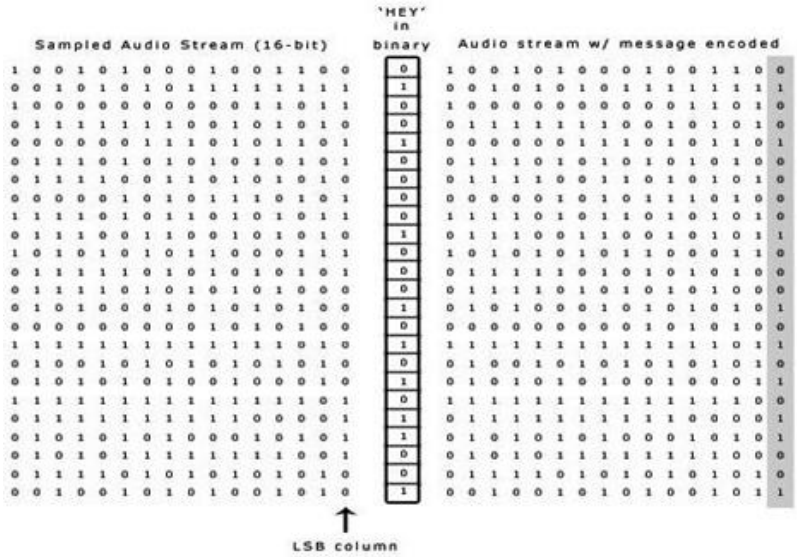

Fig 3 LSB coding example

Parity Coding: - Parity coding is used as a robust audio steganographic method. In this method, splits the signal into the different samples instead of the decomposing the signal into the discrete samples and then hides each bit of private data within the parity bit. When the parity bit of the given areas does not match with the data bit to be embedded, they it flips one of the bit of the LSB. So the sender can choose more than choice to embed the secret data. Figure illustrates the parity coding process [5].

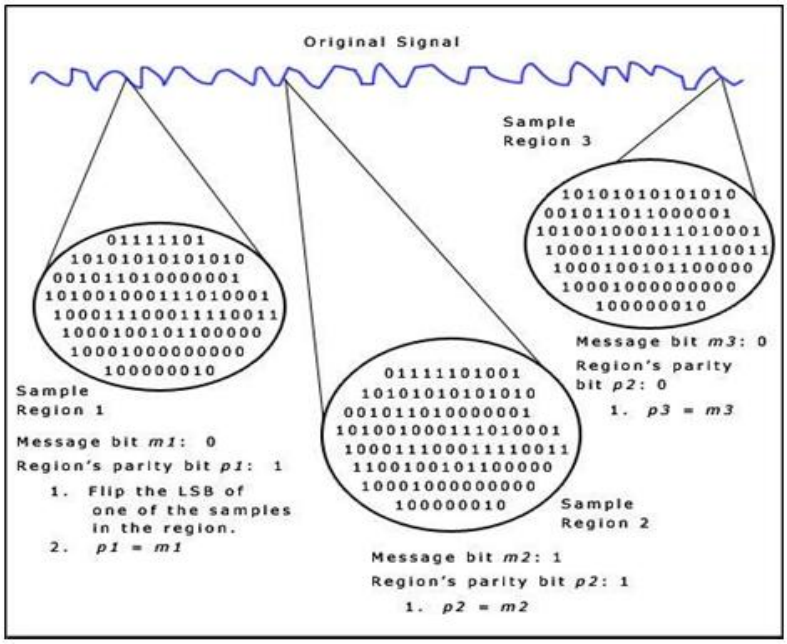

Fig 4 Parity coding

Phase Coding: - In the phase coding technique, the phase of the initial audio segment is replaced by the reference phase that shows the secret data and the remaining phase segments is arranged to store the relative phase within the segments. It is the most efficient technique for the signal to noise ratio. If there is sudden modification in the phase relation within any frequency component, then the dispersion will occurs in the noticeable phase. But when there is only small change in the phase, then we achieve the inaudible coding. This method based on the phase components of audio are imperceptible to the human auditory system [5].

IV. LITERATURE REVIEW

Fatiha Djebbar et. al. [6] in 2012 describes the review of comparative study of digital audio steganography technology. In this proposed scheme, the author describes the current digital audio steganographic techniques and can be calculate their performance depends on robustness, security and hiding capacity indicators. Another contribution of this paper is to provide the classification of steganographic techniques when embedding process occurs. The technique of digital audio steganography is also implemented in this paper. In this proposed system, digital audio steganography techniques and approaches are compared. Advantages and disadvantages of the digital audio steganography techniques are also discussed in this paper to show their capabilities to ensure the secure communications. Also, comparisons between the different techniques are shown in this paper.

Rimba Whidiana Ciptasari et. al. [7] in 2014 describes the combination of encryption and secret sharing technology which provides the various ownership protection schemes. In ownership protection area, author describes the audio watermarking depends on the visual cryptography. In this proposed system, we just focus on constructing an audio ownership protection scheme to increase the security by using the discrete wavelet transform and discrete cosine transform, visual cryptography, and digital timestamps. This method is providing the better robustness of the proposed scheme. In this paper, it can mostly used for the audio ownership protection scheme for superior robustness against both intentional and incidental distortions. The trade-off can be reduced between the data payload and two other properties such as imperceptibility and robustness while maintains the quality of the audio signal.

Masoud Nosrati et. al., [8] in March 2012 reviews the various audio steganography techniques. The audio steganography and human auditory system involves the least significant bit (LSB) coding, parity coding, phase coding, spread spectrum (SS) and echo data hiding are introduced. In this paper, the basic concepts of an audio steganography technique are introduced.

Jasleen Kour et. al., [9] in May 2014 proposes the steganography and various types of steganography. In this paper, author also discusses about the various techniques of steganography methods and which have their drawbacks and its advantage. In this paper, to implement the steganography, to describe the various types of the data hiding techniques such as least significant bit coding, spread spectrum technique etc. have been reviewed in the paper. In this paper, least significant bit steganography technique is mostly preferred.

Jayaram P et. al.[10] in 2011 proposes the different methods of audio steganographic techniques and its strengthens and weaknesses. Author proposes a paper depends on the information hiding with the use of the audio steganography techniques. In this paper, author discuss about the methods of audio steganographic techniques and also discuss about strengthens and weaknesses of the different techniques and tells how they differs from the another methods. Author proposes a robust method of imperceptible data hiding in the sound file in an audio steganography.

VI. PROBLEM FORMULATION

The system used a high data embedding without considering the overall change in bit rate due to change in pitch of the sound file for the parameters of an embedding, bpm of the sound file, compression format. Also the length of the sound file is not considered as a parameter.

VII. OBJECTIVES

To hide the data securely without affecting the speech/sound quality to the perception level. The change occurring in the signal is reduced with the embedding of another data into the original data. Noise is reduced due to change in volume of bit rate in the audio file. The structural quality of the sound file is increased with the reference to the original file and also increases the correlation of the sound file. To improve the robustness against attacks, bit error rate and also improves the peak signal-to-noise ratio which is used to determine the quality of the stego image after embedding the secret data.

VIII. PROPOSED METHODOLOGY

- Reading all the given sound files into a data set.
- Divide it into the blocks
- Extracting the features of the sound or speech file by performing the Mel Feature Space Based spectrum decomposition .
- Perform the data encryption by using fuzzy based coding in fuzzy logic generator that is a MATLAB tool Using block by block embedding of the data
- Calculating mean of the sound file
- Extract the embedded data bits from the sound file by using Mel frequency based data-bit extraction
- Calculate the different parameters like SNR, PSNR, MSE values
- Calculate total correlation of the extracted data-bits.
- Find robustness against attacks

IX. CONCLUSION

As steganography is an important issue as it deals with encryption and data security we need a scheme which covers our audio data in such a way as to increase the encryption capability and decrease the destruction of the original data. We have a proposed system for dealing with steganography in audio files with DCT infused data embedding or data hiding so as to improve the fidelity of the hidden data into ensure the complete transparency of the original data and not letting the users know about the secret hidden data.

REFERENCES

[1] Ashima Wadhwa et.al., "A Survey on Audio Steganography Techniques for Digital Data Security", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 4, Issue 4, April 2014

[2] Masoud Nosrati et. al., "Audio Steganography: A Survey on Recent Approaches", *World Applied Programming*, Vol (2), No (3), March 2012. 202-205 ISSN: 2222-2510

[3] Vipula Madhukar Wajgade et. al., "Enhancing Data Security Using Video Steganography" *International Journal of Emerging Technology and Advanced Engineering*, Volume 3, Issue 4, April 2013\

[4] Nishu Gupta et. al., "A Practical Three Layered Approach of Data Hiding Using Audio Steganography" *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 3, Issue 7, July 2014

[5] Jaya ram P et. al., "Information Hiding Using Audio Steganography– A Survey", *The International Journal of Multimedia & Its Applications (IJMA)*, Volume 3, No.3, August 2011

[6] Fatiha Djebbar et. al., "Comparative study of digital audio steganography techniques", *EURASIP Journal on Audio, Speech and Music Processing*, 2012, 2012:25

[7] Rimba Whidiana Ciptasari et. al., "An enhanced audio ownership protection scheme based on visual cryptography", *EURASIP Journal on Information Security*, 2014:2, 2014\

[8] Masoud Nosrati et. al., "Audio Steganography: A Survey on Recent Approaches", *World Applied Programming journal*, Volume 2, No 3, March 2012

[9] Jasleen Kour et. al., "Steganography Techniques –A Review Paper", *International Journal of Emerging Research in Management &Technology*, ISSN: 2278-9359, Volume-3, Issue-5, May 2014

[10] Jayaram P et. al., "information hiding using audio steganography: A survey", *The International Journal of Multimedia & Its Applications (IJMA)*, Vol.3, No.3, August 2011

