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

Shefali Rani[1], Yogesh Kumar[2]

[1](*M.Tech Department of Computer Science, BGIET Sangrur India)*

[2](*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

Data hiding plays an important role for security purposes like in military areas or marketing strategies. Information hiding is a type of steganography which converts the data into digital media such as image, text, audio and video. In terms of privacy, information hiding is used that provides the anonymous for content providers on the World Wide Web which is used for hiding the data into the digital media etc [1].

In information hiding, the information is embedded into digital media that is distributed and can be used. Information hiding differs from the cryptography in which only authorized user can access the information and that can be easily decrypted as compared to information hiding [1].

Information Hiding has becomes an important role in a several application such as digital audio, video and images that are hidden in other data to protect from the unauthorized user [1].

II. STEGANOGRAPHY

Steganography is the form of coverting the data into another data such as cover medium by using the various steganographic methods whereas cryptography converts the data into encrypted from i.e. cipher text. Generally, we apply the steganography method where the cryptography is not effective [2]. The aim of steganography is sending the information secretly between the sender and recipient [3].

Terms used in Steganography: -

Cover file: - is also known as carrier file or envelope which contains the hidden text such as human voice speech, music signal with different duration are gathered [4].

Stego key: - is a key which is used for embedding the data [4].

Embeddor: is a block that embeds the data into the cover file [4].

Stego signal: - after embedding the data in the cover object, it is called stego signal. It is not possible to

differentiate between the cover signal and stego signal [4].

Extractor/ Detector: - is a block that extracts the data from the cover file [4].

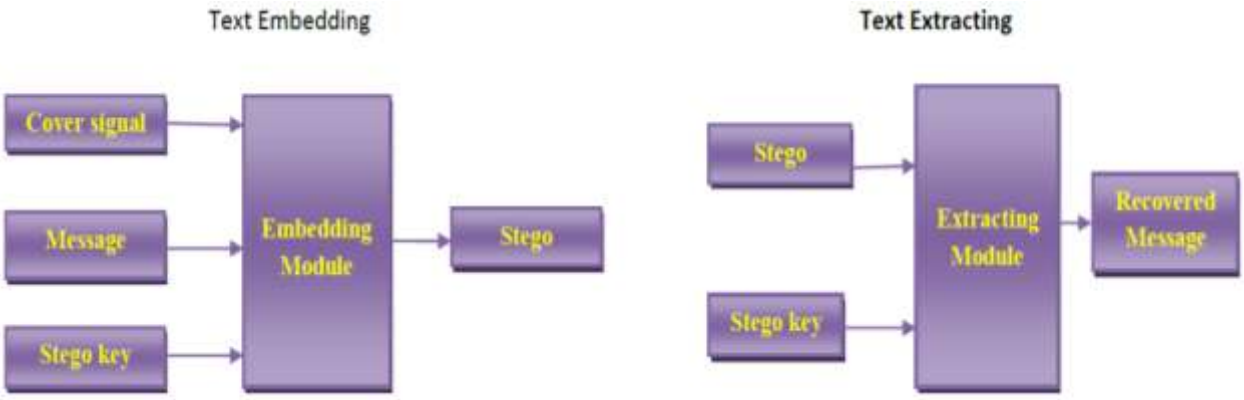

Fig 1 Terms are used in steganography

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 [5].

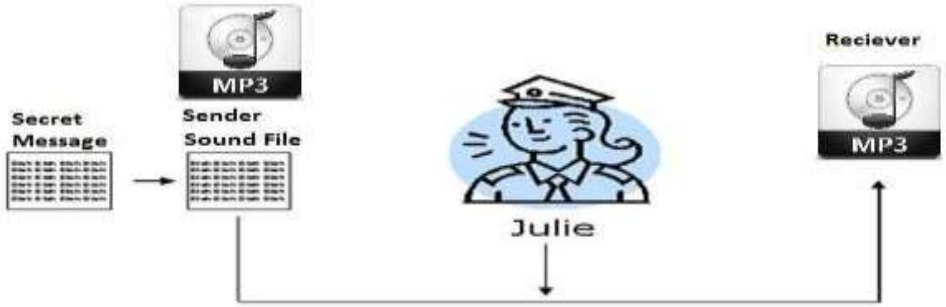

Fig 2 Secret message behind MP3

There are three main digital audio formats typically in use: -

1. Sample Quantization: - is a 16-bit linear sampling architecture which is used by most popular audio formats such as .wav [6].

2. Temporal Sampling: - uses only few selectable frequencies e.g. 8 kHz, 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz and 44.1 kHz. to sample the audio. In this selected part of the frequency range, sampling rate puts an upper bound. So the higher sampling rate, higher will be the usable data space [6].

3. Perceptual Sampling: - it changes the properties of the audio carefully by encoding only the parts the user views. It maintains the sound but the signal is changed. Today, this format is used on the internet [6].

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:

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 [7].

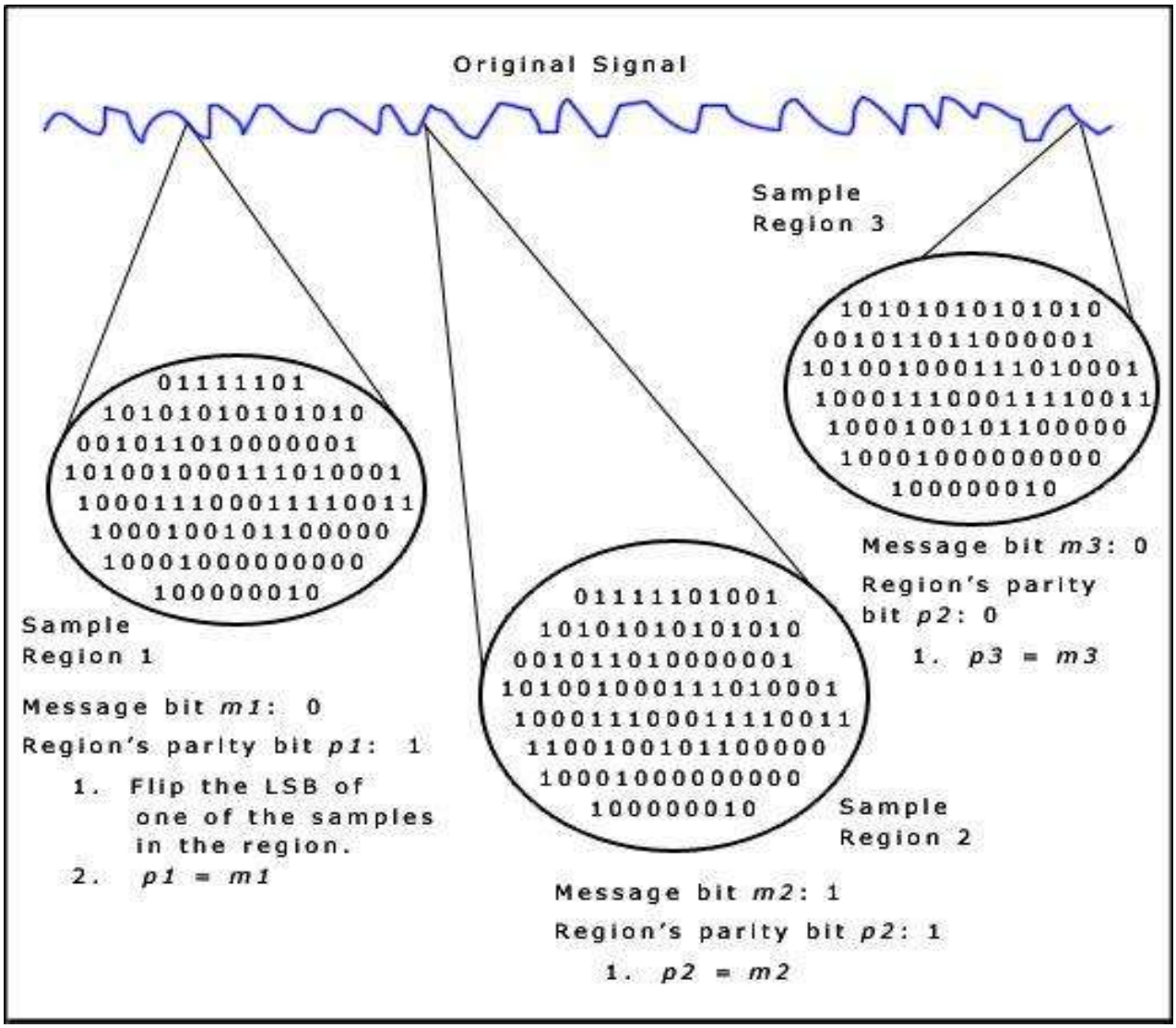

Fig 3 Parity coding

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 [7].

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 [7].

Spread Spectrum: - In audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the frequency spectrum of the audio signal. This is similar to a system which uses an implementation of the LSB that spreads the message bits randomly over the entire sound file. However, unlike LSB coding, the Spread Spectrum method spreads the secret information over the frequency spectrum of the sound file using a code which is independent of the actual signal. As a result, the final signal occupies a bandwidth which is more than what is actually required for transmission [7].

V. LITERATURE REVIEW

Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim and Habib Hamam [8] 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, Kyung-Hyune Rhee and Kouichi Sakurai [9] 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.

Jisna Antony , Sobin c.c and Sherly A.P, [10] in 2012 proposes the various techniques for hiding the information. In audio steganography, audio is used as a cover media. The most common method are used for the audio steganography are temporal domain and transform domain techniques. The main focus on this paper is to review the audio steganography in wavelet domain. For the effective wavelet masking scheme, lifting scheme can also be used in a future work. The major drawback of the wavelet domain is to generate the high data quality at the receiver end. The extraction process can also be affected by even making a little change in the values of the host coefficients. So, the wavelet domain should also aim on better data quality at the receiver end.

R.Valarmathi , M.Sc., M.Phil and G.M. Kadhar Nawaz M.C.A., Ph.D, [11] in Jan 2014 describes the reviews of both the techniques i.e. cryptography and steganography. By combination of both techniques, the information is converted into encrypted form by using a software and then covert the encrypted information within an image or any kind of media with the use of the stego key. To increases the security of the embedded information, both the techniques are used. The various characteristics of the steganographic algorithms are defined in this paper. The most widely characteristics used for audio steganographic algorithms are transparency, capacity and robustness.

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] Ravi Saini and Rajkumar Yadav, A New Data Hiding Method Using Pixel Position and Logical and Operation, *International Journal of Computer and Electronics Research, Volume 1, Issue 1, June 2012*

[2] Vipula Madhukar Wajgade and Dr. Suresh Kumar, Enhancing Data Security Using Video Steganography, *International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 4, April 2013*

[3] Krupali V. Deshmukh and Prof. Gyankamal J. Chhajed, A Steganographic Method for Data Hiding in Binary Image using Edge based Grids, *Int.J.Computer Technology & Applications,Vol 5 (4),1369-1374, July 2014*

[4] Burate D.J. and M. R. Dixit, Performance Improving LSB Audio Steganography Technique, *International Journal of Advance Research in Computer Science and Management Studies, Volume 1, Issue 4, ISSN: 2321-7782, Sep 2013*

[5] Nishu Gupta and Mrs. Shailja, 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*

[6] Neha Gupta and Nidhi Sharma, Hiding Image in Audio using DWT and LSB, *International Journal of Computer Applications, Volume 81, No2, November 2013*

[7] Jaya ram P, Ranganatha H R and Anupama HS, Information Hiding Using Audio Steganography– A Survey, *The International Journal of Multimedia & Its Applications (IJMA), Volume 3, No.3, August 2011*

[8] Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim and Habib Hamam, Comparative study of digital audio steganography techniques, *EURASIP Journal on Audio, Speech and Music Processing, 2012, 2012:25*

[9] Rimba Whidiana Ciptasari, Kyung-Hyune Rhee and Kouichi Sakurai, An enhanced audio ownership protection scheme based on visual cryptography, *EURASIP Journal on Information Security, 2014:2, 2014*

[10] Jisna Antony, Sobin c.c and Sherly A.P, Audio Steganography in Wavelet Domain – A Survey, *International Journal of Computer Applications, Volume 52– No.13, August 2012*

[11] R.Valarmathi, M.Sc., M.Phil and G.M. Kadhar Nawaz M.C.A., Ph.D, Information Hiding Using Audio Steganography with Encrypted Data, *International Journal of Advanced Research in Computer and Communication Engineering, Volume 3, Issue 1, January 2014*