International Journal of Recent Engineering Science (IJRES),
ISSN: 2349-7157, *Volume 2 Issue 6 November to December 2015*

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

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 steganographic data becomes higher.

Keywords— *Steganography, Information hiding, Audio Steganography, MFCC*

I. INTRODUCTION

In modern communication system data hiding is the most fundamental issue for the network security. As every user wants to keep their information secret but as transmitting the data via internet is highly unsecured way. So for this steganography technique is used to protect our data. In steganography technique, embedding the secret messages in audio file is the most difficult to use [1]. 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 [2].

II. STEGANOGRAPHY

Steganography is the art of embedding a file into another file, message, text or image [3]. 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 [4].

The aim of steganography is sending the information secretly between the sender and recipient. The data should be covert in such a manner that cannot be easily detectable by the unauthorized user and that can be extremely difficult task to hide the information inside another digital media. Mostly steganography method is preferred in military areas, corporate and private areas to keep the information secret [5].

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 [6].

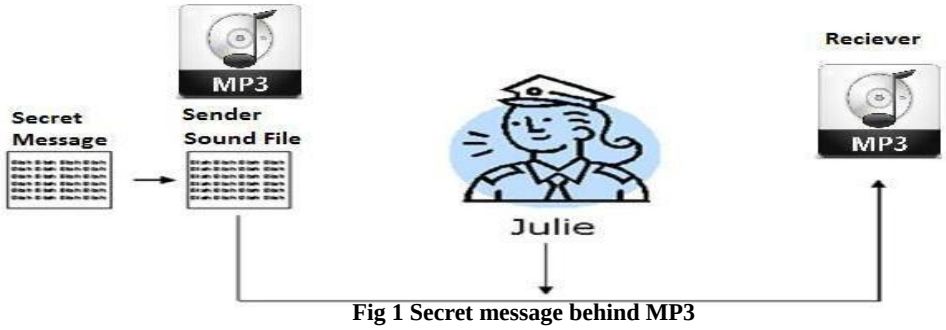

Fig 1 Secret message behind MP3

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 [7].

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 [7].

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 [7].

IV. APPLICATIONS OF THE AUDIO STEGANOGRAPHY

Several audio steganography applications have been successfully developed. Three main application audio steganography are: -

1. **Secret communication: -** is used in military areas, medical science, multimedia messaging etc. For e.g. in medical science to maintain the medical reports, images are embedded in sound file and transmitted to different recipients. Only authorised user retrieves the media images that have the knowledge about the key. Another way of the secret communication can be used in audio MMS (multimedia messaging service) which uses the excessive amount of audio sounds in mobile devices. Since the text is hidden in MMS in real-time applications and then spreads over the network. In MMS application, 4 last bits of the audio message is replaced with the secret message and then the audio MMS transmit over the network to the receiver which open the audio MMS and then check the message [8].
2. **Improved communication: -** To make more effective the quality of audio over the telephone network is to increase the bandwidth of telephone network channel. In this audio signal is embedded at the sender side and retrieved at the receiver side. In this audio signal is embedded into the wideband signal and then transmit over the channel. The sender uses the speaker and the receiver uses the microphone [8].
3. **Data storage: -** In audio steganography methods, the data is effectively stored. The application for data storage can be seen in subtitled movies. E.g. person's speech, movie music, background music can be used to hide the data which is required for translation. In this case, bandwidth is reduced [8].

V. LITERATURE REVIEW

Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim and Habib Hamam [8] in 2012 describe 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 describe 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.

Jayaram, Ranganatha H R and Anupama HS [10] in Aug 2011 proposes the different methods of audio steganographic techniques and its strengthens and weaknesses. Now-a-days, internet applications are more likely to be used for transmitting the data in a secured way. In public communication system, data transmission is not secure as unauthorized user uses the inappropriate methods or the improper use or improper knowledge. To resolve this problem, the steganography techniques are used. 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. In this paper, this system gives the better security over the hidden messages from the unauthorised user and sent to the receiver in a secured and efficient manner. Even after the encoding process, the file size remains unchanged in this system and also more reliable for any other type of the audio file format. Author proposes a robust method of

imperceptible data hiding in the sound file in an audio steganography.

Gunjan Nehru and Puja Dhar [11] in 2012 describes about the data hiding which is most important issue of the network security purposes. One of the most efficient ways to preserve the privacy is by using the technique of audio data hiding. In this paper author proposes an imperceptible method of the data concealing in the audio file. This proposed system provides the robust method, a good and effective method for concealing the data to protect from an unauthorized user and sent it to the receiver in a secured way. This proposed scheme does not affect the file size after embedding process and can also used for more suitable to any other kinds of the format of the audio file. Author proposes a number of the methods of audio steganography with the use of the various algorithms such as genetic algorithm approach and LSB technique.

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. RESULTS AND DISCUSSION

The result shows the evaluation of audio embedding and extraction result using peak signal to noise ratio and mean square error. Correlation of the extracted watermark and original watermark. The watermark size of the based methodology is 27 X 27 and for proposed methodology is 128 X 128.

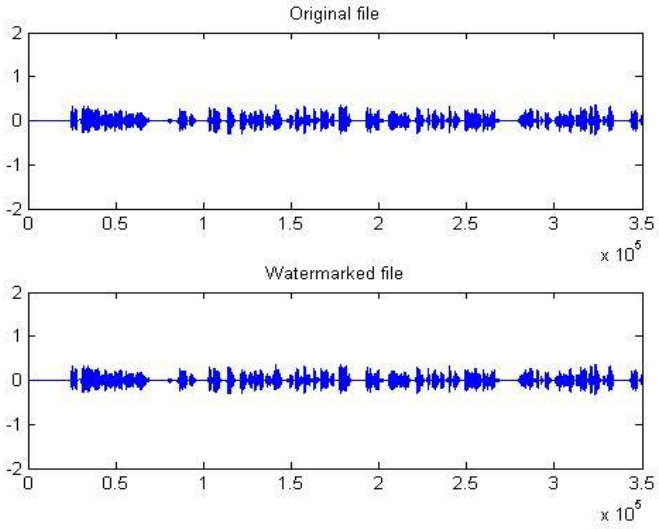

Fig 2 shows the original file of sound to be embedded and the watermarked file after embedding the watermark for based methodology.

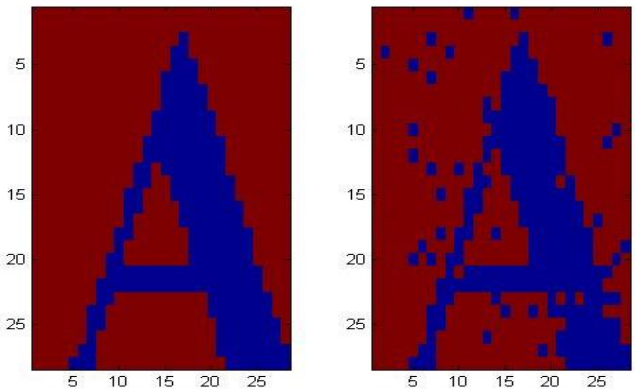

Fig 3 (a) shows the original file of image to be embedded and the fig (b) shows the extracted watermark from the file for based methodology

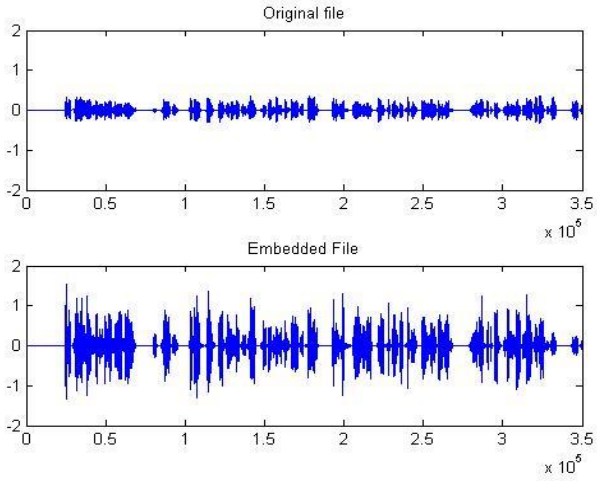

Fig 4 shows the original file of sound to be embedded and the watermarked file after embedding the watermark for proposed methodology

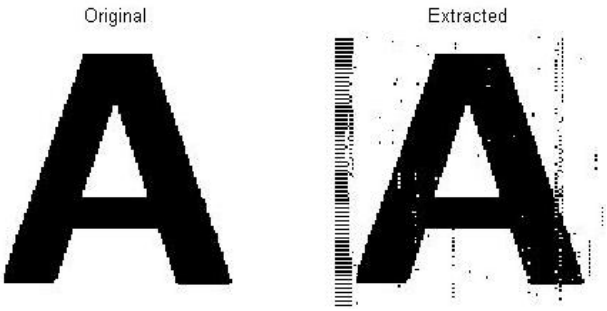

Fig 5 (a) shows the original file of image to be embedded and the fig (b) shows the extracted watermark from the file for proposed methodology

Parameters	Base Methodology	Proposed Methodology
MSE	1.5	0.01
PSNR	14.5	47
Correlation	0.89	0.92

Table 1 shows the values of parameters of the based or proposed methodology for no attack

Parameters	Base Methodology	Proposed Methodology
MSE	1.15	0.1
PSNR	8	48
Correlation	0.499	0.59

Table 2 shows the values of parameters of the based or proposed methodology for noise attack

Parameters	Base Methodology	Proposed Methodology
MSE	2.25	0.01
PSNR	14.9	47
Correlation	0.75	0.95

Table 3 shows the values of parameters of the based or proposed methodology for bass boosting attack

Parameters	Base Methodology	Proposed Methodology
MSE	1.5	0.1
PSNR	15	48
Correlation	0.89	0.92

Table 4 shows the values of parameters of the based or proposed methodology for smoothing attack

X. 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.

X. FUTURE WORK

In future our technique can be enhanced by utilizing both frequency and spatial domain and our scheme merged in hibernate system which can improve the steganography performance by utilizing both the features and giving an advantage to the user by helping them embed higher data with resistance to attacks.

REFERENCES

[1] Poulami Dutta, Debnath Bhattacharyya and Tai-hoon Kim, Data Hiding in Audio Signal: A Review, International Journal of Database Theory and Application, Vol. 2, No. 2, June 2009

[2] 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

[3] Shivani Khosla and Paramjeet Kaur, Secure Data Hiding Technique Using Video Steganography and Watermarking - A Review, IJCSIT, Volume 1, Spl. Issue 1, E-ISSN: 1694-2329, P-ISSN: 1694-2345, March 2014

[4] 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

[5] 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

[6] 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

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

[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] 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

[11] Gunjan Nehru and Puja Dhar, A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012