International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol. 1 Issue 6 December 2015

A Survey on Recent Trends in Audio Steganography

Kanchan Chilhate[1], Kailash Patidar[2], Gajendra Singh Chandel[3]

M-tech scholar SSSIST, Sehore[1], HOD CSE, SSSIST Sehore[2], Asst. Prof, CSE SSSIST, Sehore[3]
chilhatekanchan@gmail.com[1], kailashpatidar123@gmail.com[2], gajendrasingh86@gmail.com[3]

ABSTRACT:- Communication of data in public requires data to be transmitted in robust and secure manner. Also, excessive use of digital data in various fields of life demands a secure system. Various techniques such as cryptography, steganography and watermarking have been established. Among these steganography provides better confidentiality as it is the practice of hiding data within data. In digital media steganography, text files, images, audio as well as video are used as carrier. We focus in this paper on digital audio as the carrier. In this paper, a survey on latest audio steganographic methods is carried out along with their strength and weakness. Also, comparison between various steganographic methods based on robustness is carried out. Another contribution of this paper is evaluation of performance of various reviewed steganography techniques.

KEYWORDS:- Steganography, audio signal, confidentiality, data hiding.

I. INTRODUCTION

Large demand of internet applications have increased the possibility of attacks. Hence, security in public communication has become a fundamental issue. Security of data can be achieved by encryption or data hiding. Encryption is related to cryptography which is defined as protecting the information by encrypting it into unrecognizable format. It doesn't hide the existence of the message from the attacker instead it renders the content of the message garbled to unauthorized people. Steganography and watermarking are related to data hiding. Watermarking hides the legal information inside the carrier for copyright protection. It embeds information into carrier in such a way that its removal becomes impossible. It can also be used for authentication and certification. Steganography is one of the best techniques employed for ensuring data security. Steganography hides the information in such a way that the existence of information is undetectable. Steganography comes from Greek words 'Stegnos' which means 'Covered' and 'Graptos' which means 'Writing' i.e. covered or concealed writing. Steganography is carried out intelligently so that it becomes difficult for the intruder to detect the existence of the hidden message in the carrier. This technique requires a cover which can hold the message that is to be transmitted. Cover may be image, audio, text file or even video. Secret message may be a text file, a cipher text, audio or image. Stego key is required for the embedding and extraction process.

Embedding a message in a cover file should be carried out in such a way that the quality of the cover file is not compromised. Once the message is embedded into carrier, the stego file is generated and transmitted over channel. To extract the message, the receiver must also have the stego key [1-2].

This paper is further organized as follows: section II details the recent advancement in audio steganography, a comparative analysis among various audio steganography in spatial and transform domain with their performance evaluation is highlighted, section III deals with proposed framework for audio steganography, and finally, section IV concludes the paper.

II. AUDIO STEGANOGRAPHY

Audio steganography is one of the steganography methods which employs audio file as the stego media. In this method, secret message can be image, audio or text. This method requires modification of audio signal in an imperceptible manner. In order to make audio steganography successful, the audio carrier signal and stego audio signal should have the same characteristics [3]. There are three parameters which define the audio steganography techniques

i. Capacity: how many bits of secret message can be embedded in the carrier.
ii. Transparency: how securely the message is embedded.
iii. Robustness: ability to resist steganalysis attacks.

Robustness and capacity rarely coexist within the same steganographic system due to tradeoff

imbalance between the two parameters where increase in robustness level decreases the data hiding capacity [3-4].

In audio steganography data embedding approaches are broadly classified into spatial domain and transform domain.

A. Spatial Domain Methods :

These methods hide information on the basis of geometric characteristics of audio signal. Majority of spatial domain methods employ LSB techniques. Other techniques falling under this domain are also presented in subsequent sections.

1) Low Bit Encoding :

Low bit encoding is also known as Least significant bit (LSB). LSB is one of earliest methods used for hiding information. This method embeds the secret information into the least significant bit of audio file. Modification in the LSB of audio file must be carried out in such a way that the quality of audio file is not compromised. This method allows high data embedding capacity and can be easily incorporated for hiding data. However, this technique is less robust to noise which inturn reduces its security performance. No doubt, this method achieves imperceptibility at high embedding rate but the security and robustness of hidden information are easily compromised [1], [3], [5].

2) Echo Hiding:

This method introduces a short echo to the host signal and then embeds data in it. After addition of echo in the carrier file, the stego signal must retain the same statistical characteristics. Three parameters of echo signal are manipulated for hiding data : initial amplitude, the offset (delay) and the decay rate (for the inaudible echo). The effect is indistinguishable for delay upto 1ms between original signal and echo. Data could be hidden imperceptibly as amplitudes and decay rates can be set to values which are under audible threshold of human ear. The drawbacks of this method are low embedding rate and security [2-3], [6].

a) Strength & Weakness Of Spatial Domain :

Conventional LSB technique and its variant provide an easy way to hide information. Also, tolerance to noise addition at low levels have been achieved through LSB variant methods but with a low hiding capacity. Robustness and security are not the main characteristics of spatial domain methods[3], [6].

B. Transform Domain Methods :

These methods hide information along the frequency distribution of the carrier signal. Human auditory system has several characteristics which can be exploited by various methods of transform domain to hide data. Various methods falling under transform domain are briefly described below.

1) Spread Spectrum :

Spread spectrum technique is mainly used for properly recovering the signal transmitted over the noisy channel. In spread spectrum technique, the hidden information is distributed over a frequency spectrum of audio signal. This technique produces redundant copies of the data signal. Actually, multiple copies of data are produced using M-sequence code which is known to both sender as well as receiver. Once multiple copies are produced they are embedded in audio carrier. Hence, if some values get corrupted, there will still be copies of the values which would be used to recover the hidden information[2], [3], [6].

2) Discrete Wavelet Transform (DWT) :

Wavelet usually refers to small waves. The technique is used to hide data in transform coefficients of the audio signal. DWT was developed as an alternative to short time fourier transform. Fourier transform is used for analyzing components of stationary signal. A stationary signal can be defined as the signal with no change in the properties of the signal. We can say, Fourier Transform [10] is the powerful tool for processing signal that are composed of some sine or cosine signals or combination of the two signals. In case of non stationary signals, Fourier Transform is not so useful. Non stationary signal is the signal where there is change in the properties of the signal. For non stationary signals, wavelet transform is applied. Discrete wavelet transform is the special case of wavelet transform. DWT actually decomposes the audio signal into many multiresolution sub-bands, which inturn helps to locate the most appropriate sub-bands for embedding bits of secret message. Since, energy of host signal wavelet sub-bands shows that the first and second sub-band have more than 95% of signal energy, therefore, these two sub-bands can't be used in steganography for embedding purpose. Any change in these two sub-bands will cause drastic change in energy level of audio host signal. Implementation of this technique makes the signal much more robust to attacks occurring in the noisy channel. Data hiding in wavelet domain attempts to obtain high embedding rate but the extraction of

data at the receiver might be inaccurate [7],[10].

Juli and Sathish have applied a technique of digital audio watermarking using wavelet transform to watermark Indian classical songs [9]. They have mathematically represented watermarking problem as:

$$xw = x + w \qquad (1)$$

where xw is the watermarked audio signal, x is the host audio signal, w is the watermark and is the watermark intensity. Algorithm for audio steganography using DWT technique is shown in Fig 1. Procedure used for embedding watermark [9] is described as :

i. Watermark image is expressed as 2-Dimensional matrix which is converted into 1-Dimensional watermark vector W.

ii. Watermark intensity is multiplied to each element of W to get new watermark vector, Wf.

iii. Audio signal is decomposed to n levels using DWT.

iv. Wf is embedded into wavelet coefficients of selected sub band.

v. Inverse DWT (IDWT) is applied to obtain the watermark audio signal.

3) Tone Insertion :

It is the indirect exploitation of the psychoacoustic masking phenomenon. Psychoacoustical or auditory masking is actually the characteristic of human auditory system HAS where the presence of stronger tone renders the weaker tone in its spectral domain. The masked sound becomes inaudible in presence of another louder sound. However, the masked signal is still present. The method is resistant to attacks of low- pass filtering and bit truncation. Tone insertion method has low embedding capacity. Also, the embedded data can be easily extracted since inserted tones are easy to detect [2], [6].

4) Phase Coding :

Phase coding exploits the fact that Human Auditory System can't recognize the change in phase as easily as it can recognize the noise in the signal. It is based on the fact that phase components of sound are not as perceptible to human ear as noise is. This technique encodes the secret message as phase shifts in the spectrum of a digital signal. The disadvantage of phase coding is low transmission rate because the secret message is embedded only in the first signal segment. We can increase the transmission rate by increasing the length of the signal segment but this would also change phase relations between each frequency component of a segment more drastically, which will make embedding easier to detect.

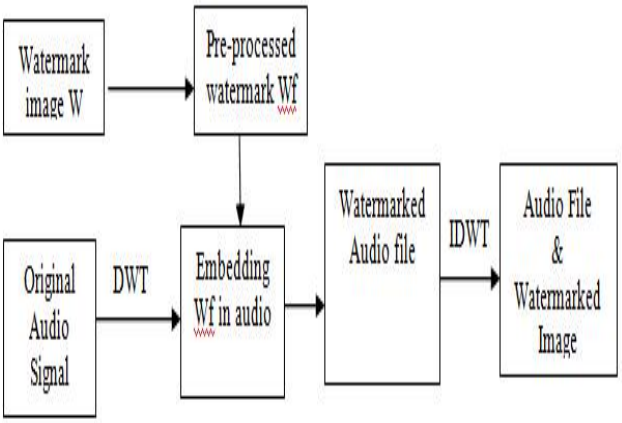

Fig. 1. Algorithm for audio steganography using DWT.

Procedure of phase coding is explained below :-

- The audio signal is broken up into many smaller segments whose length is equal to the size of secret message.
- Discrete Fourier Transform is applied to each segment. As a result, a matrix of phases and Fourier transform magnitude are formed.
- Phase differences between adjacent segments are calculated.
- Relative phase differences between adjacent segments can't be modified. But we can change the absolute phases of the segment. Hence, secret message can be inserted in the first phase of the signal segment.
- New phase matrix is created having phase of first segment and original phase differences [2], [8].

a) Strength & Weakness Of Transform Domain :

It has been proven that hiding data in transform domain gives much better results than hiding data in spatial domain. Many transform domain techniques are robust against several audio signal manipulations such as amplification, filteration etc. Robustness in the hidden data is the main characteristic of transform domain methods. However, the embedded hidden data unlikely survives data compression induced by one of the encoding processes such as ACELP [3], [6].

The detailed comparison of various steganography techniques are shown in Table I.

TABLE I. COMPARISON OF VARIOUS AUDIO STEGANOGRAPHY TECHNIQUES

Domain	Methods	Advantage	Disadvantage	Hiding Rate
Spatial domain	Low bit encoding [1][6]	High embedding rate, simple and easy	Noticeable to human ear, less robust to human ear	16kbps [6]
	Echo hiding [1][2][6]	Recovers easily from lossy data compression algorithms	Low capacity and low security	50bps [6]
Transform domain	Spread spectrum [1][6]	More robust	More vulnerable to time scale modifications	20bps [6]
	Discrete Wavelet Transform [1][6][7]	High embedding capacity	Inaccurate data retrieval	70kbps [6]
	Tone Insertion [1][2][6]	Imperceptibility of embedded data	Poor Transparency	250bps [6]
	Phase Coding [2][6][8]	Robust against signal distortion	Low capacity	333bps [6]

III. PROPOSED WORK

The maximum data hiding capacity of existing system is 70kbps [11-13]. In order to enhance the data hiding capacity, the steganographic technique using QR [11] and SVD [7] transform has been proposed as shown in Fig. 2. Following are the sequence of steps that are followed :

IV.

step 1: Input audio file and a secret message are read.

step 2: Steganography techniques QR and SVD are applied.

Step 3: Stego audio file is generated and transmitted over the channel.

V.

Step 4:- Secret message and the audio file are extracted from the stego audio file on the receiver side.

The experimental results have shown that the host message before steganography and stego message after steganography almost have the same characteristics. Also, the new steganography technique has comparatively better data hiding capacity than the existing ones.

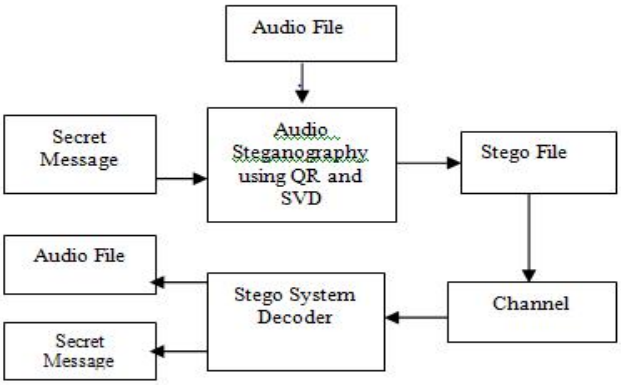

Fig. 2. Proposed audio steganography technique (WT:Wavelet transform)

IV. CONCLUSION

Recent research works have investigated many new steganography techniques which provide much better protection to digital data. Audio steganography techniques preserve the integrity of hidden data. In this work, a survey on latest digital audio steganography techniques and approaches have been presented. Also, their strengths and weaknesses is revealed. From the survey it is clear that the spatial domain maximizes the data hiding capacity whereas the transform domain focusses on masking properties to make the noise generated by embedding data imperceptible. Also, it can be concluded that the transform domain is preferred over the spatial domain in terms of imperceptibility, undetectibility and capacity. The existing audio steganography techniques lack a stable system. In this research, new audio steganography technique has been proposed with an enhanced data hiding capacity.

REFERENCES

[1] Ashima Wadhwa, “A survey on audio steganography techniques for digital data security”, International journal of advanced research in computer science and software engineering, vol. 4, issue 4, April 2014.

[2] Masoud Nosrati, Ronak Karimi, Mehdi Harari, “Audio steganography: A survey on recent approaches”, world applied programming, vol. (2), No. (3), pp. 202-205, March 2012.

[3] Jayaram P, Ranganatha HR, Anupama HS, “Information hiding using audio steganography---A survey”, The International

journal of multimedia and its applications IJMA, vol. 3, No. 3, August 2011.

[4] XU Shuzheng, Zhang Peng, Wang Pengjun, Yang Huazhong, "Performance analysis of data hiding in MPEG-4 AAC audio", Tsingua Science and Technology, vol. 14, No.1, pp.55-61, February 2009.

[5] Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade, " An efficient method for image and audio steganography using least significant bit substitution", International journal of computer applications, vol. 77, September 2013.

[6] Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim, Habib Hamam, "Comparative study of digital audio steganography techniques", Springer open journal, January 2012.

[7] Nidhi Bisla, Prachi Chaudhary, "Comparative study of DWT and DWT-SVD image watermarking techniques", International journal of advanced research in computer science and software engineering, vol. 3, issue 6, June 2013.

[8] Gunjan Nehru, Puja Dhar, "A detailed look of audio steganography techniques using LSB and genetic algorithm approach", IJCSI International journal of computer science issues, vol.9, No.2, issue 1, January 2012.

[9] C.M Juli Janardhanan, C. Sathish Kumar, "Performance analysis of discrete wavelet transform based audio watermarking on Indian classical songs", International journal of computer applications, vol. 73, No. 6, July 2013.

[10] R. Kumar, K K Ravulalollu, "Handwritten devnagari digit recognition: Bechmarking on new dataset", Journal of theoretical & applied information technology, vol. 60, No. 3, 2014.

[11] Md. Wahedul Islam, Saif al Zahir, " A novel QR code guided image steganographic technique", IEEE International Conference on consumer electronics (ICCE), 2013.

[12] Ahmad Delforouzi, mohammad Pooyan, "Adaptive digital audio steganography based on integer wavelet transform", Springer , vol. 27, pp. 247-259, April 2008.

[13] Mengyu Qiao, Andrew H. Sung, Qingzhong Liu, "MP3 audio Steganalysis", Information sciences, vol. 231, pp. 123-134, May 2013.