Increasing the Compression Ratio using Speech Coding Techniques in Audio Steganography

Sapna Sharma
PG Student
Department of Electronics & Communication
Hasmukh Goswami College of Engineering, Vahelal, Ahmedabad

Abstract— In the day to day life, everyone is dependent upon transfer of communication, where data security is not ensured. There is different techniques available for secure transmission of data, but all techniques do not provide secure and leakage proof communication over the network. Therefore, steganography solves this purpose. Steganography allows hiding data in a great way, through which strong communication may occur. Audio steganography actually hides the secret message behind an audio cover file using various techniques to provide secure and safe transmission of message without the reach of hackers. In this paper, most powerful speech analysis technique is used called Linear Predictive Coding (LPC), which encodes speech signal at very low bit rate and provides great estimation of various speech parameters. This paper gives the knowledge about previous methods of audio steganography and how proposed algorithm gives better results and shows how LPC method is better than LSB method.

Key words: Steganography, cryptography, LSB technique, linear predictive coding (LPC)

I. INTRODUCTION

There is a high need of secure communication over the internet because digital media is used by all for its various advantages. Therefore, security of transmitted data is needed. For this purpose, cryptography is used, which secure data over the network but still does not provide any guarantee of no leakage of data during transmission. So, steganography is the solution to above problem. Firstly, one must clear their concepts about cryptography and steganography. Both are different things with the same objective, where cryptography fails to achieve secure and leakage proof communication. The idea of hiding information is very ancient trick, has a long history. In ancient Greece, A message is to be write on the wood, then cover it with wax, to transfer information secretly. People also get their head shaved and get a message tattooed over there and cover it by new grown hair, share information using again shaved head [2]. Invisible inks was also used in earlier ages, to hide a message. Pencil marks is also a form of steganography. Null ciphers (unencrypted messages) were also used. But this concept work for secure transmission, then steganography is introduced.

Steganography in simple words means "secret or cover writing". Steganography can be implemented in various formats like text, images, audio and video formats. Implementing steganography on text format is very easy task but can be detected very easily by hackers because of less space available for writing a secret message.

Image steganography is quite beneficial than text steganography, provides much redundant space, provides more imperceptibility than text steganography. Another one is Audio steganography, which actually uses audio file as cover media and hides secret data behind that audible sound file. Video steganography is also another format, which makes use of both audio sound and video images, provides much more redundant space for embedding secret message and is difficult for hackers to extract data from this format of steganography. Therfore, steganography is an utmost challenging area in data security field.

II. AUDIO STEGANOGRAPHY

When audio file is used as the carrier file and any kind of secret information is embedded in it, called audio steganography.

Steganography is the way of secure transmission of message by hiding the secret message inside the original message in such a way that only the intended user knows about it. The original message is also called as cover media.

Cover media and secret message can be any kind of digital form like text, image, audio and video. Steganography is the art and science of invisible communication of messages (2)

When a carrier file is used as audio file and a secret message is hide behind it, is called audio steganography. Hiding text with the help of audio file is a tough task than image steganography, but provides a lot of redundant space to hide data.

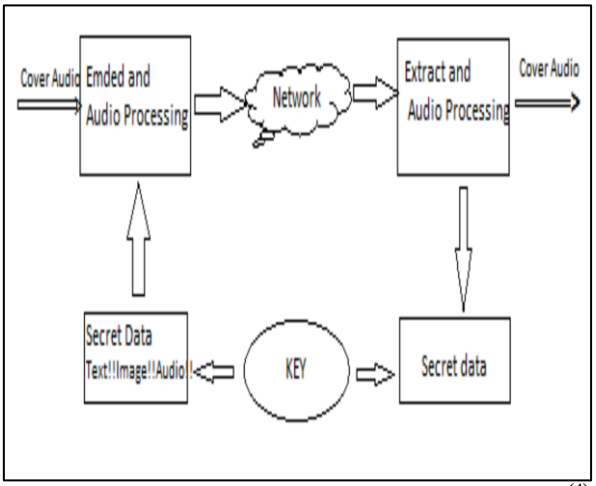

Fig. 1: Block Diagram Audio Steganography Model [4]

Here, a very basic process for audio steganography is shown, in which audio file is taken as cover media and secret message is embed into it using embedding and audio processing block, then secret message hide behind audio file is sent over network for its transmission and then on receiver side that embedded secret message and audio file is extracted. The main thing of concern is that secret message which is to be hide is kept secured using a key or a

password, and it is only known by the intended sender and intended receiver, to make this process more secure and safe.

III. VARIOUS TECHNIQUES OF AUDIO STEGANOGRAPHY

There are very commonly used techniques are available which hides secret message using audio file as cover media. These techniques are:

- Low bit encoding
- Parity Coding
- Phase Coding
- Echo Hiding
- Spread Spectrum

A. Low Bit Encoding

Low bit encoding method is also called Least Significant Bit (LSB) method. Here, the least significant bits of the original message is replaced with the bits of secret message. This method is very to implement. This method provides large space to embed secret information behind it.

- Advantages:

(1) Very high watermark channel bit rate
(2) Low computational complexity of the algorithm

- Disadvantage

(1) Low robustness against signal processing.

B. Parity Coding

This is one of most commonly used technique in audio steganography. In this method, a signal is divided into various individual samples and then encodes each bit from the secret message in a sample region's parity bit [3]. 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.(3)

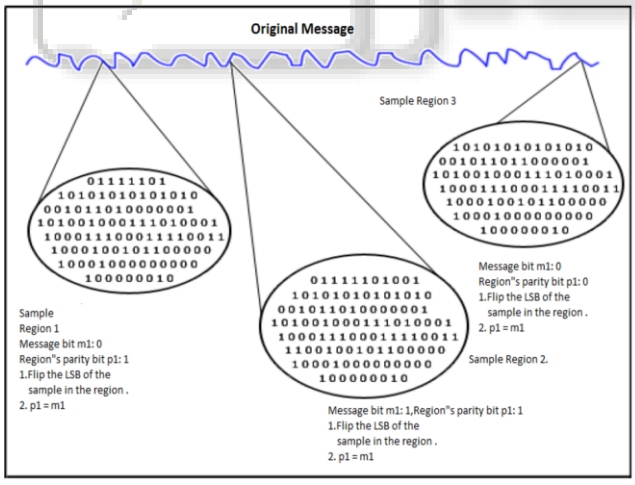

Fig. 2: Parity Coding Process (3)

- Advantages

(1) Very high watermark channel bit rate
(2) Low computational complexity of the algorithm.

- Disadvantage

(1) Low robustness against signal processing

C. Phase Coding

In Phase coding, the phase of carrier file is replaced with reference phase which represents hidden data [5] .this method 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 [9]. As it is known that phase components of audio signal is not perceptible to human ears.

- Advantage

(1) Does not introduce noise.

- Disadvantage

(1) Low data transmission rate because the secret message is encoded only in the first signal segment.

D. Spread Spectrum Technique

In spread spectrum method, secret information is spread over the audio signal's frequency spectrum as much as redundant space available over there (5), this method offers moderate data transmission rate and great robustness than other methods, but introduces noise to the signal.

- Advantages

(1) Provides high data transmission rate
(2) Great robustness than other methods

- Disadvantage

(1) Introduces noise to the signal.

E. Echo Hiding

An echo sound is added with the information message to the carrier file, which can be image, text, audio or video file. Echo signals represent information to be encoded (4)

IV. PREVIOUS METHODS

Rupanshi , Preeti , Vandana has used Direct Sequence Spread Spectrum for hiding secret message on an audio file. Here, A key is used so that secret message can be embed into noise signal, further this key is used to generate pseudo-noise wave signal. The information to be embedded must first modulated using the pseudo-noise. (6)

Kirti Gandhi, Gaurav Garg suggested a method in which LSB technique is used, where as LSB technique provide low robustness and is not highly preferred method. Instead two bits (2nd and 3rd LSB's) are used for hiding message, which further increases the data hiding capacity. A filter can be designed to reduce or minimize the changes occurred in stego file. The stego and filtered filed is used to generate a unique key. The filtered file and the generated key will be transmitted to receiver. The key will derive to extract the correct message at receiver's end.(7)

Bankar Priyanka R., Katariya Vrushabh R., Patil Komal K. proposed a method which uses genetic algorithm in which message bits are embedded into multiple and higher LSB layer values, further helps in increased robustness (8)

Lovey Rana, Saikat Banerjee implemented a method in which dual layer randomization approach is used. First layer of randomization is achieved by the selection of random byte number or samples. An additional layer of security is provided by randomly selecting the bit position at which embedding is done in the selected samples. After

using this algorithm, transparency and robustness is increased and provides improved security (9).

R. Sridevi, Dr. A Damodaram and Dr. SVL. Narasimham proposed an efficient method of audio steganography by modified LSB algorithm and strong encryption key with enhanced security is proposed (10). Enhanced Audio Steganography (EAS) is a combination of audio Steganography and cryptography. EAS proceeds in two steps: it uses most powerful encryption algorithm in the first level and in the second level it uses a modified LSB (Least Significant Bit) algorithm to embed the message into audio (10).

V. LINEAR PREDICTIVE CODING (LPC)

Speech coding or speech processing is actually used to reduce the amount of memory required to transmit any speech signal.

- Many speech compression schemes are available which are:
- Channel vocoder
- Linear predictive coder (LPC)
- Code excited linear prediction (CELP)
- Sinusoidal coders
- Mixed excitation linear prediction (MELP)

LPC is actually a speech compression or speech coding method which is used in proposed algorithm. LPC is the most accurate method of speech coding. Linear predictive coding method is a kind of digital method which actually predicts the future value on the basis of linear prediction of past values of that speech signal. [1] Generally, speech signal is sampled at 8000 samples/second in which 8 bits are used to represent each sample and it rate of 64000 bits/second, where as if LPC method is used to compress the speech signal, it reduces this value up to 2400 bits/second.[1] The frequency of human speech ranges from 300Hz to 3400Hz. LPC is a lossy method of speech compression, means input and output speech are different, but it is not detected by Human Auditory System (HAS).

LPC voice coder has four main attributes: bit rate, delay, complexity and quality.

Bit rate, the first attribute, it decides the degree of compression that a voice coder achieves (1). Linear predictive coder transmits speech at a bit rate of 2.4 kb/s (1)

Delay is the second attribute; this is related to transmission of speech signal. The signal delay is considered unacceptable if the delay is more than 300ms.

Complexity, another attribute, as the compression rate of LPC technique is quite high, so the method is more complex, means high cost. For more complex system, linear predictive coder requires more than one processor to run in real time applications.

Quality, last attribute, this defines that how the output speech sounds to a listener after compression. Basically, compression is done, but it is undetectable to human ear. The speech quality can be tested using different methods. The most common test is Absolute Category Rating (ACR), measures the speech signal quality and rate them as good, bad, excellent and so on.

The proposed algorithm uses LPC-10 means linear predictive coder of order 10. The main feature of LPC is that it is modelled as a single linear filter and provides compression rate of 2.4 kbps.

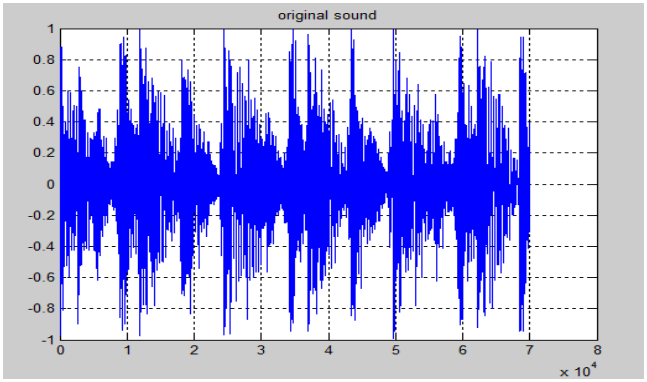

Fig. 3: Original Sound File (Amplitude Versus Number of Samples)

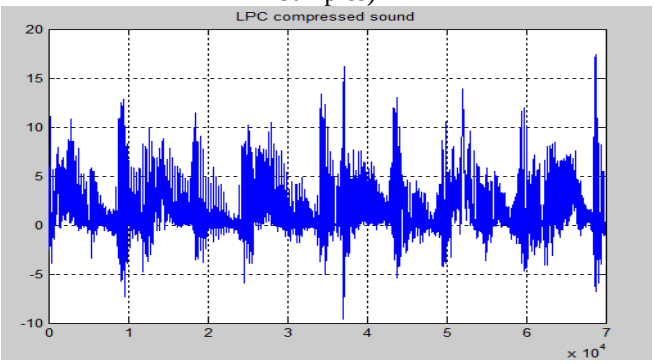

Fig. 4: LPC Compressed Sound File

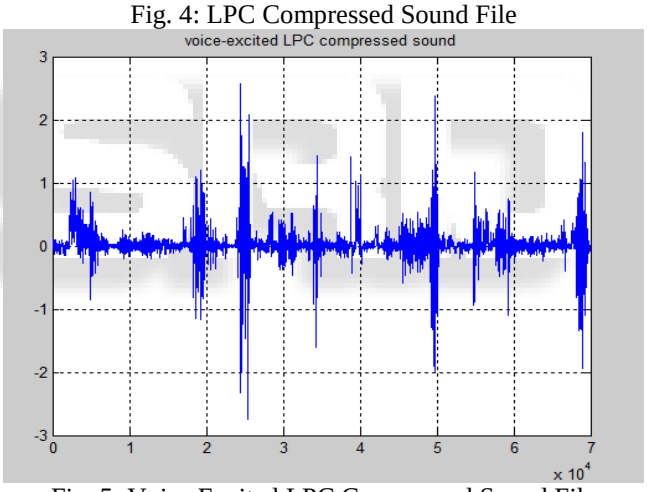

Fig. 5: Voice Excited LPC Compressed Sound File

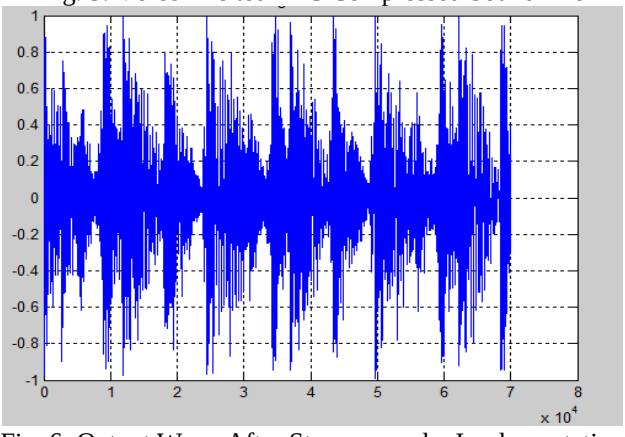

Fig. 6: Output Wave After Steganography Implementation

VI. RESULT

Here, the speech signal is compressed using plain LPC and voice excited LPC. Both methods are implemented and if both are compared in terms of compression, then voice

excited LPC method provides high compression rate than plain LPC method.

Speech compression is a great way to save limited bandwidth; therefore one can use speech coding method according to the requirement of bit rate, communication distance and privacy.

It is concluded that voice excited LPC scheme provides efficient speech compression rate with high quality being a lossy method.

VII. APPLICATIONS

The main application of LPC coder is used for speech compression in cellular telephony, where long distance communication occurs and requires speech compression for good communication. Another application is text to speech synthesis, in which a speech signal has been generated by the synthesis of text. Other applications are: voice mail systems in which speech signal needs to be compressed and then transmitted, Telephone answering machines, and multimedia applications (1)

VIII. CONCLUSION

The proposed work shows that how audio secret information is embedded into an audio carrier file. Both sound files were taken as .wav files. LPC speech processing method helps in reducing the size of file and provides almost same output results as input, also shows that voice excited LPC method provides better compression as compared to plain LPC. Therefore, if secret message file is larger in size then it is better to firstly compress the file using any speech compression technique then hide it using any cover media, this will give better results.

REFERENCE

[1] Arpana Mishra , Javed Ashraf "Speech Compression with Voice Excited Linear Predictive Coding" International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 6, June 2012
[2] Rucha Bahirat ,Amit Kolhe , "Overview of secure data transmission using Steganography" International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 3, March 2014
[3] Masoud Nosrati, Ronak Karimi, Mehdi Hariri "Audio Steganography: A Survey on Recent Approaches" World Applied Programming, Vol (2), No (3), March 2012
[4] Swati Malviya, Manish Saxena, Dr. Anubhuti hare "Audio Steganography by Different Methods" International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 7, July 2012
[5] Prof. Samir Kumar, Bandy opadhyay Barnali, Gupta Banik "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited" International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 4, June 2012
[6] Rupanshi , Preeti , Vandana "Audio Steganography by Direct Sequence Spread Spectrum" International Journal of Computer Trends and Technology (IJCTT) – volume 13 number 2 – Jul 2014
[7] Kirti Gandhi, Gaurav Garg, " Modified LSB Audio Steganography Approach" International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 6, June 2012
[8] Bankar Priyanka R., Katariya Vrushabh R, Patil Komal K, "Audio Steganography using LSB'', International Journal of Electronics, Communication and Soft Computing Science and Engineering, March 2012
[9] Lovey Rana, Saikat Banerjee, "Dual Layer Randomization in Audio Steganography Using Random Byte Position Encoding", International Journal of Engineering and Innovative Technology, Volume 2, Issue 8, February 2013
[10] R Sridevi, Dr. A Damodaram and Dr.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, pp. 771-778, 2009.

