Computer based audio steganography

Avadhut Apte
Department of Electrical Engineering,
V.J.T.I.,
Mumbai, India.
E-mail address : avadhut.apte@gmail.com

Amutha Jeyakumar
Department of Electrical Engineering,
V.J.T.I.,
Mumbai, India.
E-mail address : amuthajaykumar@vjti.org.in

***Abstract* - People use cryptography to send secret messages to one another without a third party overseeing the message. Steganography is a type of cryptography in which the secret message is hidden in another message. In this paper, a method of hiding the speech signal inside a music file using LSB coding is proposed. The speech signal can be hidden inside music file by replacing the LSBs of the samples of music file by speech signal bits. At the receiver's end, speech signal can be heard only when a pre-defined password or codeword is entered by the receiver. Otherwise, a person can only hear the music file which covers the speech signal.**

Keywords - Steganography, Stego signal, Embedding, Carrier, Data hiding.

I. Introduction

Steganography is an art and a science of communicating in a way, which hides the existence of the communication. It is also called as "covered writing", because it uses a "cover" of a message for sending any important secret message.

Steganography serves as a means for private, secure and sometimes malicious communication. Steganography is a powerful tool which increases security in data transferring and archiving. In the steganographic scenario, the secret data is first concealed within another object which is called "cover object", to form "stego object" and then this new object can be transmitted or saved. It causes the existence of the secret data and even its transmission to be hidden. A steganography system, in general, is expected to meet three key requirements, namely, imperceptibility of embedding, correct recovery of embedded information & large payload.

There are various techniques used for steganography based on the nature of the secret message & the carrier signal. Using different techniques, we can send secret data in the form of an image, a music file or even a video file by embedding it into the carrier, forming a stego signal. At the receiver's end, the secret data can be recovered from the stego signal using different algorithms. Audio steganography can be performed in time domain as well as frequency domain. Different domains have special features which make them suitable for different applications.

II. Basic Idea

The basic purpose is to send the speech signal with the help of a carrier signal which is a music file. For this to achieve, speech signal has to be embedded into the music file to form a "stego signal" which can now be sent to the destination. The embedding of the speech into the music file is done by LSB replacement method for which the total number of samples in both has to be known. Then one can decide the number of bits per sample in a music file that can be replaced with speech signal bits. Now the receiver can detect the hidden signal only if it knows the "password" or "codeword" which is pre-defined. If the password entered by the receiver is correct, then the stego signal is passed through the specially designed band pass filter which allows the speech signal to pass through it. Since its cut-off frequencies are 20Hz & 20kHz,, the signal frequency components less than 20 Hz & greater than 20 kHz are rejected & the output of the filter is the speech signal hidden inside the music file. If the password entered is wrong, the stego signal is itself heard & not the speech signal. The coding & decoding can be done in MATLAB / JAVA / C / C++, but the most important things are the bit replacement at the time of embedding & the pre-defined password for the detection.

III. LSB Coding

This technique was mainly developed for image & video steganography, but it can also be used for audio steganography. The technique uses the fact that most of the information in a sample in any audio file is contained in the MSBs rather than LSBs. If one has to hide any speech signal inside a music file which is also called as "carrier", it can be done by replacing consecutive LSBs in each sample of the carrier with the message bits. Such a bit replacement is very simple & safe. There is a very small change in the carrier & that can be observed if we compare the spectra of original carrier & the carrier after embedding. The replacement can be done in two ways viz. fixed coding & variable coding. But, with increasing number of replaced bits, the amount of noise goes on increasing, which puts some limit on embedding.

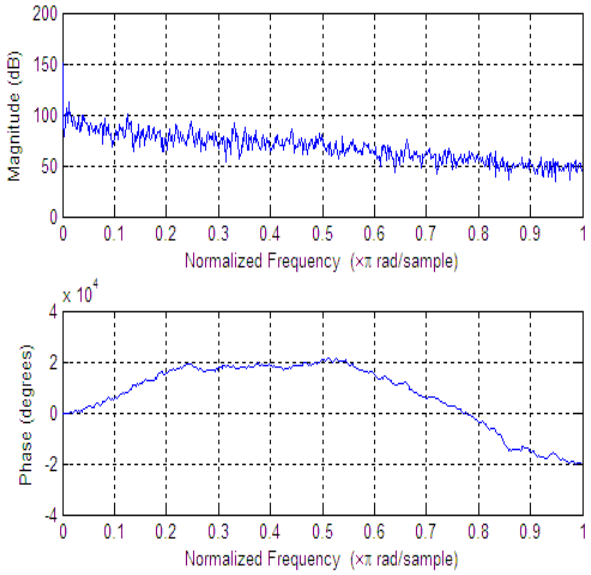

Figure 1. Original carrier spectrum

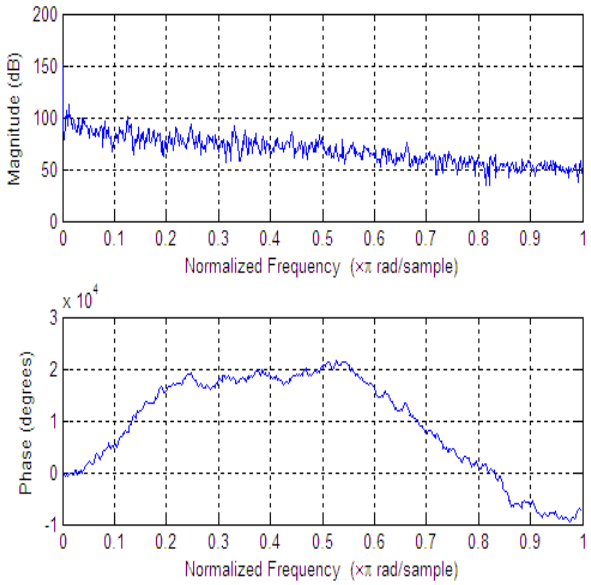

Figure 2. Modified carrier spectrum

Above figures show the obtained results of the LSB coding, in picture form. From the above spectra, one can get a clear idea of the two signals. If we compare both of them, we observe very small changes & these are so small that they cannot be detected when one hears the modified carrier signal.

IV. Algorithm

The algorithm of the proposed method contains two parts as mentioned below. First part gives the steps to embed the speech into the carrier & the next part gives the steps to detect the speech signal.

A. *Encoding*

1) *Read the speech signal.*
2) *Read the audio file or music file stored on the drive.*
3) *Embed the signal in music file using LSB coding.*
4) *Write the stego signal to the drive.*

B. *Decoding*

1) *Read the stego signal.*
2) *Enter the password.*
3) *If the password is correct, pass the stego signal through band pass filter.*
4) *Take the output of the filter as the required output.*
5) *If the password is incorrect, take the output as the stego signal itself.*

V. Box Diagram

The detection part of the algorithm can be represented diagrammatically as below.

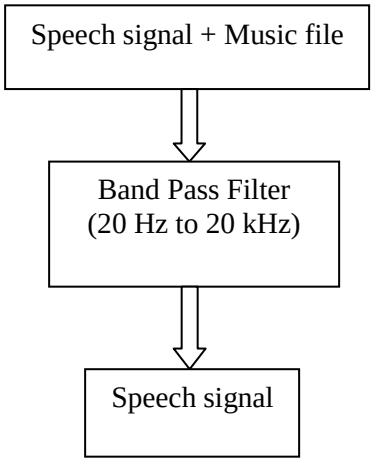

Figure 3. Detection method

VI. Flow Chart

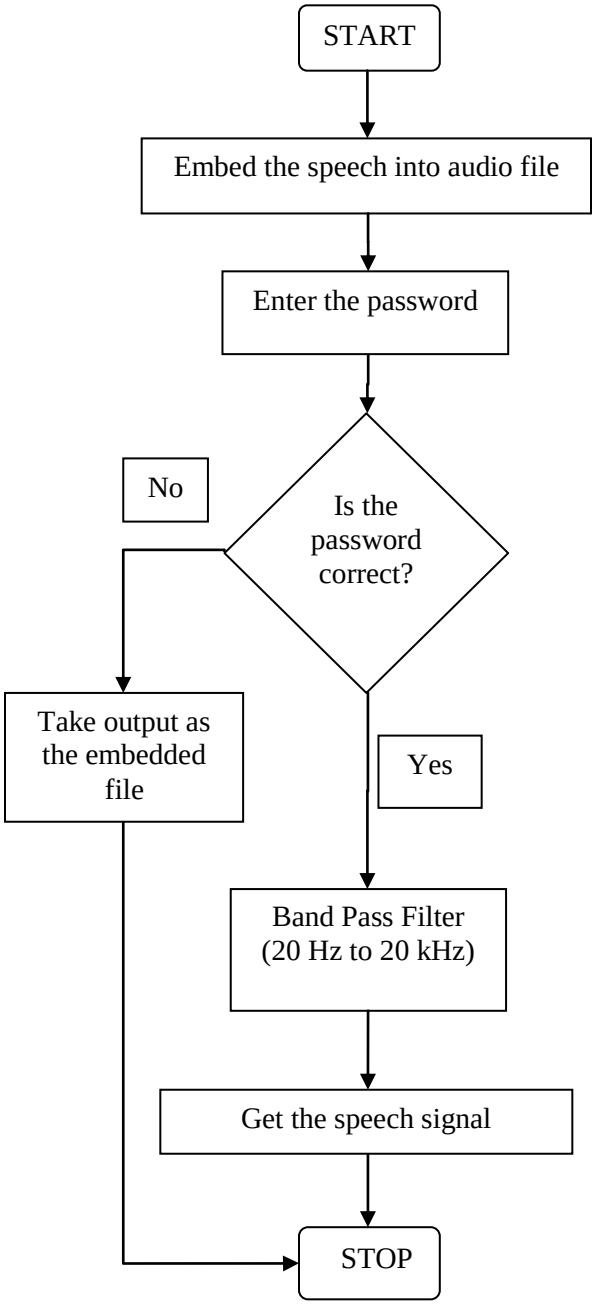

Figure 4. Flow chart

VII. Conclusion

Thus, we have proposed a new technique of audio steganography by hiding a speech signal inside a music file by bit replacement. The figures also show the closeness of the spectra of original carrier signal & the carrier signal after embedding the speech inside it. The advantage of the encoding method is its simplicity. Further, the decoding method seems to be very safe because of the requirement of the password at the receiver's end, in order to know the hidden speech signal. Hence a very high level of data security is maintained during the transmission of any valuable data. Although the method has low robustness & possibility of errors with increasing number of replaced bits, it is still intended to become more important day by day & finds innumerable applications requiring secure data transmission like military communication, INTERPOL messaging & so on.

Acknowledgment

We would like to express our gratitude towards the professors of VJTI for their able guidance while making this paper. We are also thankful to all those who directly or indirectly helped us in making this paper a reality.

References

[1] K. Gopalan, "Audio steganography by cepstrum although the algorithm is applicable to other resolution modification," In Proc. IEEE Int. Conf. Acoustics, Speech, levels of wavelet and Signal Processing, Vol. 5, pp. 481-484, March 2005.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, vol. 35, issue 3-4, September 1996, pp.313-336

[3] S. Wang, X. Zhang, and K. Zhang, "Data Hiding in Digital Audio by Frequency Domain Dithering," MMMACNS, Springer-Verlag, Berlin Heidelberg, 2003, pp.383-394.

[4] Tian, Jun, "High Capacity Reversible Data Embedding and Content Authentication," IEEE Conference on Acoustics, Speech and Signal Processing, vol. 3, pp. 517-520, 2003

[5] J. M. Pickett. "Acoustics of Speech Communication, The: Fundamentals, Speech Perception Theory, and Technology" Allyn & Bacon 1999, ISBN-10: 0205198872