Ashwini Mane., Gajanan Galshetwar., Amutha Jeyakumar/ International Journal of Engineering Research and Applications (IJERA)
ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.1123-1125

DATA HIDING TECHNIQUE: AUDIO STEGANOGRAPHYUSING LSB TECHNIQUE

Ashwini Mane.*Gajanan Galshetwar.Amutha Jeyakumar*****
*Department of Electrical Engineering,
V.J.T.I.,Mumbai, India.
**Department of Electrical Engineering,
V.J.T.I., Mumbai,India
Associate Professor
Department of Electrical Engineering,
V.J.T.I., Mumbai, India.

Abstract - In this era of emerging technologies, electroniccommunication has become an integral and significantpart of everyone's life because it is simpler, faster and more secure.The objective of this paper is to come up with atechnique hiding the presence of secret message. Steganographyis the art of secret communication.Its purpose is to hide the presence of communication, as opposed to cryptography, which aims to make communication unintelligible to those who don't possess the right keys. Audio steganography is concerned with hiding informationin a cover (host) audio signal in an imperceptible way. Hidden information from the stego, or data-embedded audio signal, isretrieved using a key similar to the one that was employed during the hiding phase.Least Significant Bit (LSB) modification technique is the most simple and efficient technique used for audio steganography.Proposed technique hasbeen tested successfully on a .wav file at a samplingfrequency of 3000 samples/second with each samplecontaining 8 bits.

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 the art to hide the very presence of communication by embedding the secret message into the innocuous-looking cover media objects, such as images using the human's visual, aural redundance or media objects' statistical redundance. 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. 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.Existing audio steganography software can embed messages in WAV, AU,and even MP3 sound files.

II. Least Significant Bit insertion

In audio steganography, 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.. 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. It consists in embedding each bit from the message in the least significant bit of the cover audio. In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well.

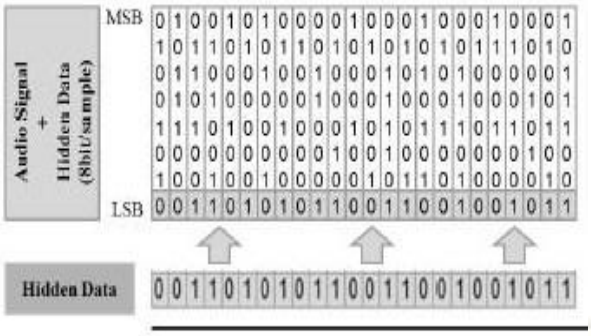


Figure 1: LSB coding technique

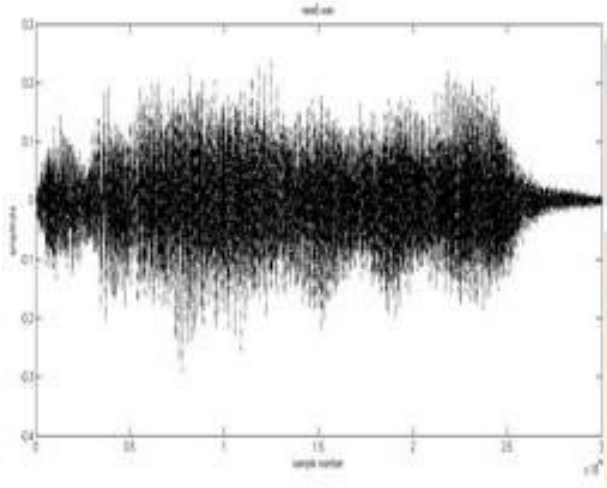


Figure 2: Original audio file

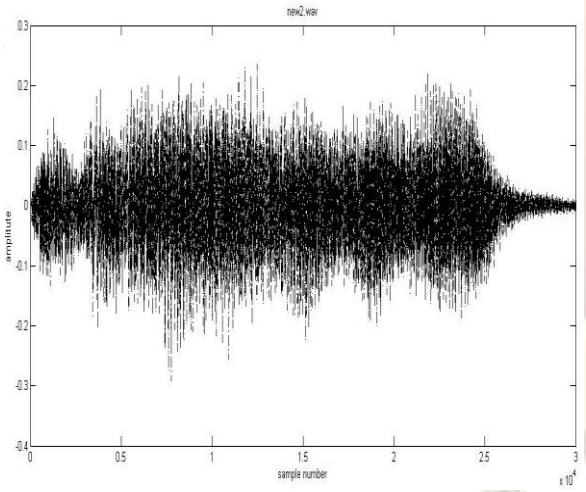


Figure 3: Stego audio file

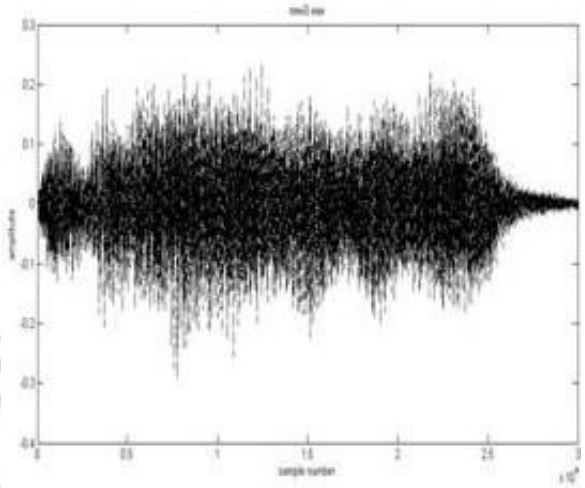


Figure 4:Third bit modified stego audio file

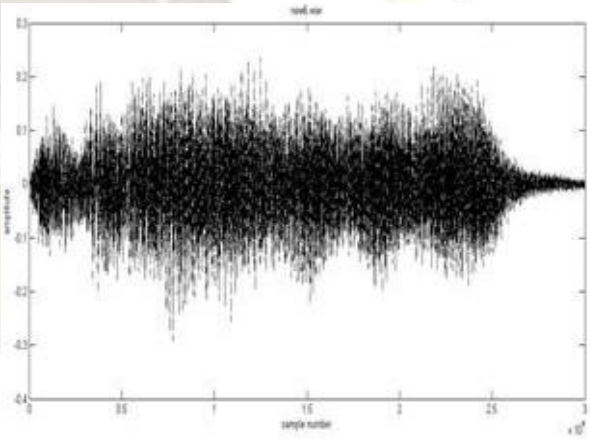


Figure 5: Eighth bit lsb modified stego audio file

Audio steganography on fixed LSB's is done. The original host message is shown in fig.2 The resulting stego audio after embedding secrete message in first LSB, third LSB and eighth LSB are shown in fig.3, fig.4 and fig 5 respectively. Above figures show the obtained results of the LSB coding,. From the above spectra, one can get a clear idea of the two signals. If we compare them, we observe very small changes & these are so small that they cannot be detected when one hears the modified carrier signal.

III. 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.

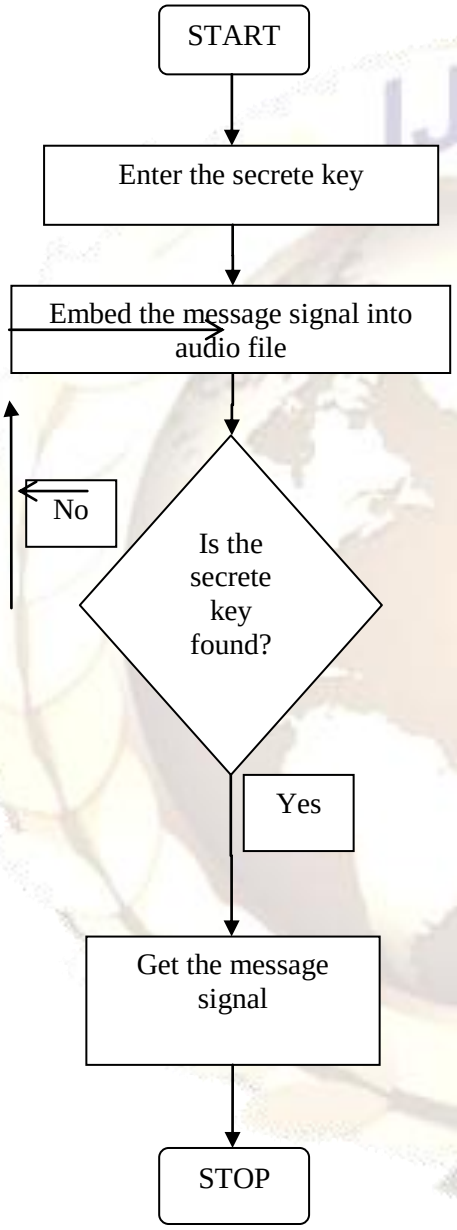
A. Encoding

1) Read the message signal.
2) Read the audio file or music file stored on the drive.
3) Enter the secrete key.

4) Embed the signal in music file using LSB coding.
5) Write the stego signal to the drive.

B. **Decoding**

1) Read the stego signal.
2) Search for the secrete key.
3) If the secrete key is found, take the next data as the required output.



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.

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] N. Cvejic, T. Seppiinen, "Increasing the capacity ofLSB-based audio steganography", IEEE Workshop on Multimedia Signal processing, pp. 336 -338, 2002.
[2] K. Gopalan, "Audio steganography using bitmodification",ProceedingsofInternational Conference on Multimedia and Expo, Vol. 1, pp.629-632, 6-9 July 2003
[3] N. Cvejic, T. Seppanen, "Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method", Proceedings of the International Conference onInformation Technology: Coding and Computing (ITCC04), vol.2, pp.533, 2004.
[4] H. Matsuka, "Spread spectrum audio steganography using sub-band phase shifting", In IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP06), pp. 36, Pasadena, CA, USA, December 2006.

.