**Audio Steganography by Least Significant Bit Method**

**By:**

**Farrah Aslam**

**Ammarah Shakeel**

**Department of Computer Engineering,**

**Faculty of Telecommunication and Information Engineering,**

**University of Engineering and Technology, Taxila**

Abstract:- ***Increased use of electronic communication has given birth to new ways of transmitting information securely. Audio steganography is the science of hiding some secret text or audio information in a host message. The host message before steganography and stego message after steganography have the same characteristics. Least Significant Bit (LSB) technique is the most simple and efficient technique used for the audio steganography. This report describes method to do audio steganography by using LSB technique.***

1. Introduction

In this era of emerging technologies, electronic communication has become an integral and significant part of everyone’s life because it is simpler, faster and more secure. With adoption of electronic communication on such a large scale, it has become necessary to devise ways to transmit information secretly. Steganography is the branch of science which deals with the embedding secret message on the transmitter side and retrieving it successfully on the receiver side. Whether it is about copyright protection for piracy prevention or private personal communication, steganography is the emerging technique which would be the solution to such issues. Strictly speaking, steganography is not only authentication provider through watermarking but a door to confidential communication as well.

Steganography is an art of hiding secret message in another message without letting anyone know about presence of secret message except the intended receiver. The massage used to hide secret message is called host message or cover message. Once the contents of the host message or cover message are modified, the resultant message is known as stego message. In other words, stego message is combination of host message and secret message.

Steganography is often mixed up with cryptography. Cryptography changes representation of secret message being transmitted while steganography hides presence of secret message.

Steganography can be applied to different type of media including text, audio and video. Audio and video files are considered to be excellent carriers for the purpose of steganography due to presence of redundancy. Audio steganography requires a text or audio secret message to be embedded within a cover audio message. Due to availability of redundancy, the cover audio message before steganography and stego message after steganography remains same. However, audio steganography is considered more difficult than video steganography because the Human Auditory System (HAS) is more sensitive than Human Visual System (HVS).

LSB technique is briefed in section II. Description and Experimental results of LSB methodology are presented in section III and IV. Code is in section V. Section VI presents conclusion.

1. LEAST SIGNIFICANT BIT METHOD

The LSB technique is one of the simplest audio steganography techniques. In this technique, data is being hidden in least significant bit of audio samples. The weightage of LSB in comparison with the combined weightage of whole sample is very small. However, changing the LSB will induce some noise but as long as noise induced is below detectable threshold, audio steganography is possible.

Fig. 1 shows block diagram of LSB technique encoder. The host message in analog form is converted to digital form. The LSB(s) of host message samples are being modified to embed the secret message. The modified host message or stego message is then converted to analog form to produce analog stego message.

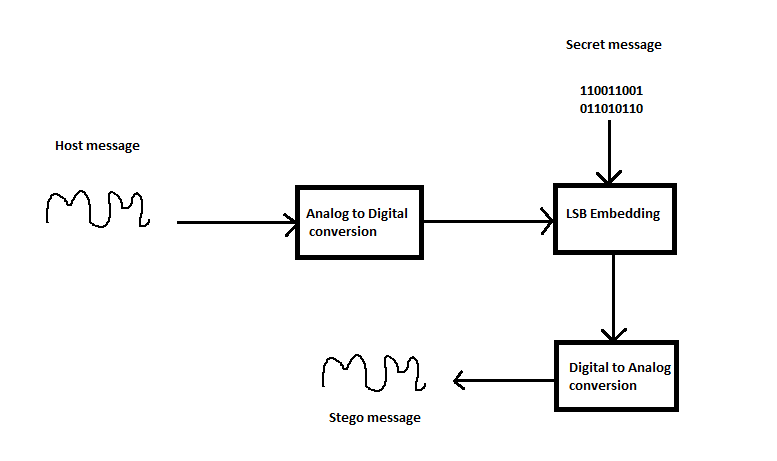


Fig. 1 LSB technique encoder

Fig.2 shows block diagram of a decoder. In decoder analog stego message is converted into digital form to obtain samples of the stego message. On the basis of encoding, decoding is performed where the bits from samples are extracted to retrieve complete secret message.

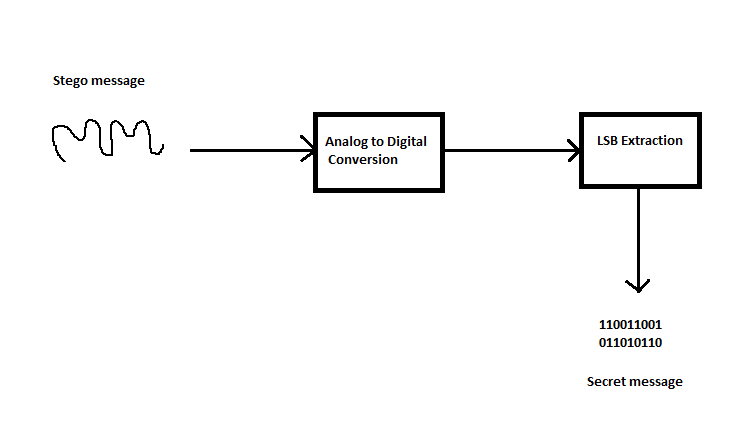


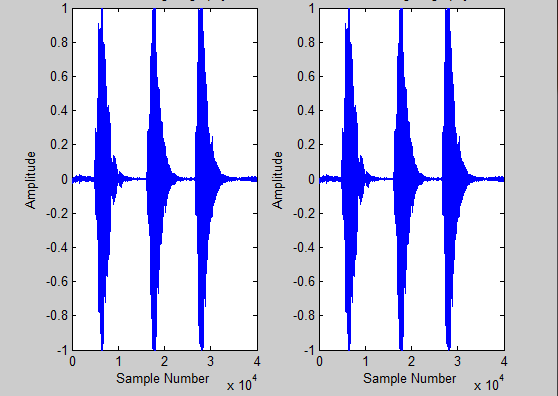
Fig. 2 LSB technique decoder

1. DESCRIPTION

**Encoder:** We recorded the sound through some recorder and read that on MATLAB by waveread function. There are two channels in .wav file here we just worked with one channel. The range of audio samples lies between -1 to +1. We have to convert it into binary for this we first converted it into decimal by multiplying each sample by 2nbits-1.

Negative numbers cannot be converted into binary. So we have made them positive. For that purpose we used most significant bit (z). If number is negative z=1 otherwise z=0. After this we converted it into binary. Then we took secret message and changed it into 8 bit binary. This was the matrix of nx8 order. We changed it into row vector for convenience. We checked length of message and compared it with number of samples. If length of message is greater than number of samples then we displayed ‘error’. On the other hand if length of message is smaller than number of samples we converted length of message into 16 bit binary. Then we embedded it into first 16 samples by using LSB embedding technique. From 17th we started to embed our secret message by LSB embedding technique.

After embedding we changed this digital form into analog form. For this purpose we changed the binary into decimal. Then from most significant bit we checked the sign of each sample. After this we divided each sample by 2nbits-1 to make the range of samples between -1 to +1. Then we saved the sound which contained our secret message with new name by using wavewrite function. Then we compared the sound and graph of host message and stego message which showed the same results.

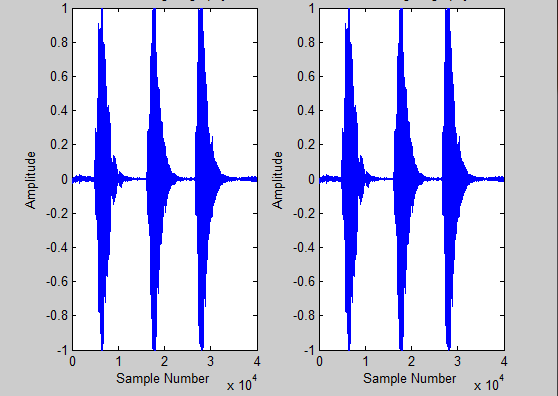


Before Steganography After Steganography

**Decoder:** We read the .wav file and changed it into binary. We checked first 16 samples by LSB extraction technique. Which told us how many next samples contained our secret message. Then by LSB extraction technique we retrieved our secret message from those samples.

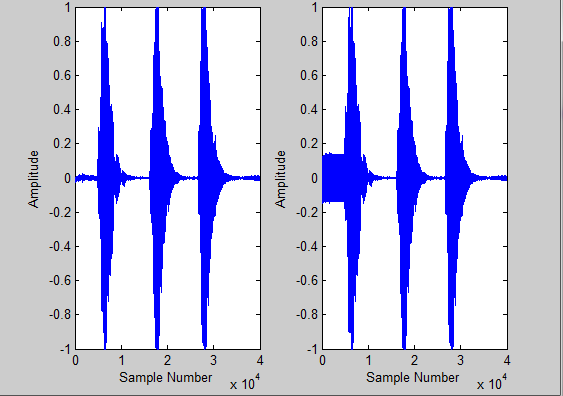
1. Experimental results

First we embedded our secret message in least significant bits and compared the sound and graph with original one. We observed no change in sound and graph.



Before Steganography After Steganography

As we started embedding our secret message in significant bits we observed the change in sound and graph in comparison with original sound and graph.



Before Steganography After steganography