International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 4, April 2014)

LSB Audio Steganography Approach

Kamred Udham Singh[1]
[1]Department of Computer Science, Faculty of Science Banaras Hindu University, Varanasi, (U.P.), INDIA

***Abstract*— The quick growth of internet made easy to send the data correct and faster from source to destination. Security of the information is one of the most important factors of information technology and communication. The requirement for secured communication acquaints the concept of "Steganography". Word Steganography itself indicates that information within information .Data hiding is a form of steganography, this technique embedded the secret information into a digital media object and thus it ensures secured data transfer. Audio steganography is concerned with hiding information in a cover audio signal in an imponderable way. Hidden information is retrieved from the data-embedded audio signal, using a key which was employed during the hiding phase of information. This paper proposes a technique of audio steganographic that gives a unique stage to hide the secret information in audio file. Least Significant Bit (LSB) data modification technique is the most easy and popular technique used for audio steganography. This proposed technique has been tested successfully on a .wav.**

***Keywords*— Cryptography, human auditory system, LSB, data hiding, Carrier**

I. INTRODUCTION

The word steganography is derived from Greek word steganos, it means "covered or protected", and graphia meaning is "writing"[1]. It is a sub-discipline of Information hiding that focuses on hiding the existence of messages [2][3].Steganography is the technique of hiding secret information inside an image, audio, and video, in such a way that others cannot distinguish the presence of the hidden information. Steganography mean hiding of information inside other information. Audio steganography is the technique of hiding Information inside audio signal. As information is embedded with the signal, it gets modified but this modification should be made imperceptible to the human ear. Other digital object like image , video can also be taken but audio steganography is more challenging because of the features of Human Auditory System (HAS) like large power, large range of audible frequency and dynamic range of hearing[4]. Cryptography takes part in encryption of message but it makes no attempt to hide the encrypted message. In steganography the original message is not modified but the existence of message is hidden in the selected medium by embedding techniques.

Audio steganography: Cover signal + message = Stego signal (Transmitted)

Cryptography in steganography: Cover signal + Encrypted message = Stego signal

Where,

Message data + Encryption Key = Encrypted message

Now we can say that audio steganography has prime importance than cryptography because it is more secret as it conceals the existence of message. We use cryptography along with steganography for providing more security.

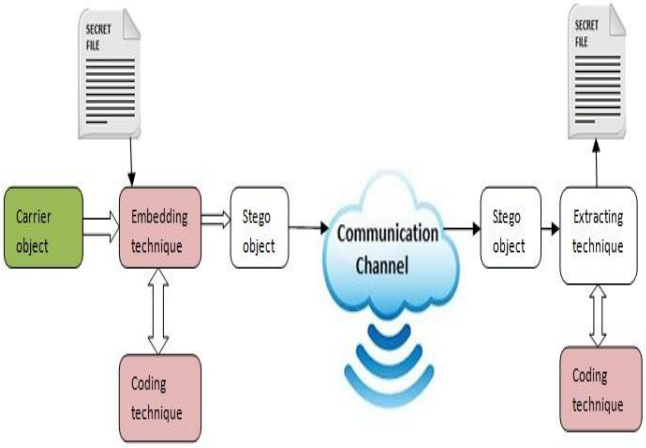
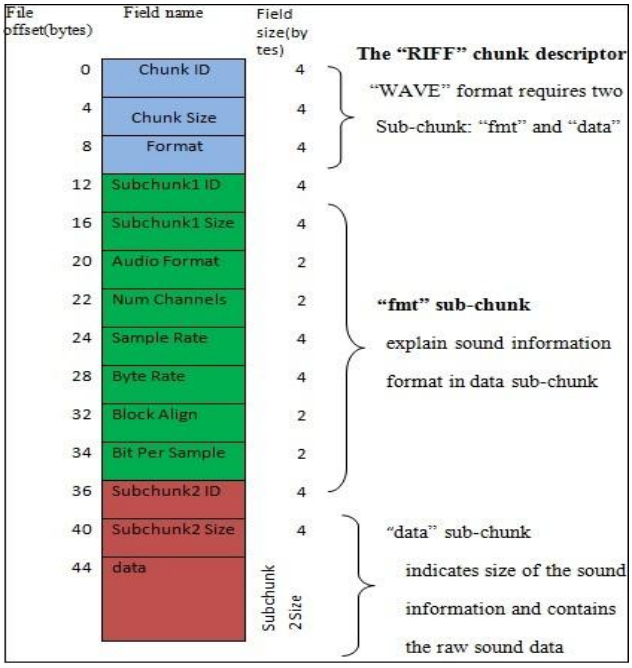


Figure 1: General Steganography Block Diagram

In this paper, we proposed a data hiding method where message is hide in audio object using (LSB least significant-bit) modification technique. The binary sequence of an audio file is changed by adding secret message in it. WAVE, AU, and MP3 audio file formats are used in least significant-bit technique. Audio steganography is a way of embedding information inside an audio signal. The WAVE file format is selected because this is the original format of other formats. It means that which audio files have other formats, either are converted from WAVE format, or can be simply converted to WAVE format. WAVE audio file format follows the specification of Microsoft for multimedia storage, as so called Resource Interchange File Format (RIFF) [5].

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 4, April 2014)

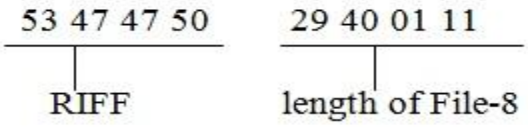
II. THE WAVE FILE FORMAT



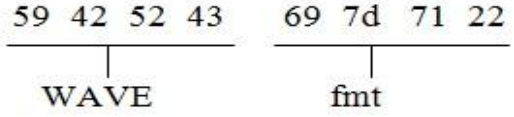
Wave file in a HEX editor it starts like that, and continues with unreadable binary data:

```
53 47 47 50 29 40 01 11  59 42 52 43 69 7d 71 22  RIFF$@ ....WAVE fmt
10 00 10 00 01 00 02 11  10 2B 01 00 55 AD 00 00  ..............+...D.....
04 00 10 00 62 61 72 59  01 45 01 00 00 00 00 00  .....data @.....
```

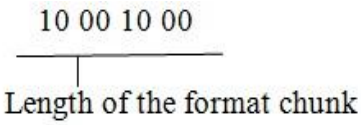
Every RIFF file starts with the text "RIFF", followed by the Int32 length of the entire file:



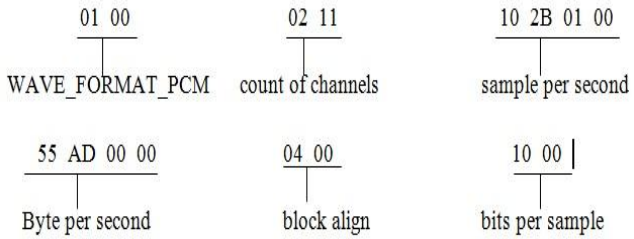
The next fields define RIFF file which contains Wave data and open the format chunk:



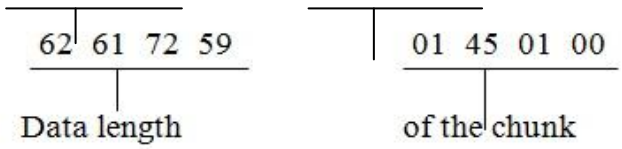
The length of the chunk must be 16 for PCM files



Now the format is being specified by a WAVEFORMATEX structure:



The format chunk can be followed by some extra information. Then the interesting parts begin with the data chunk.



The data chunk contains all the Wave samples. That means the rest of the file is pure audio data. Little changes might be hearable, but won't destroy the file.

III. LSB CODING

Least significant bit (LSB) data hiding technique is the easiest way to hide information in a digital audio object. LSB coding permits for a huge amount of data to be encoded by replacing the least significant bit (LSB) of each sampling point with a binary information [7]. Figure 3 illustrates how the message is encoded in an 8-bit sample using the LSB technique [8][9]. Data transmission rate In LSB coding is 1 kbps per kHz. In some of LSB coding implementations, two LSB of a sample are substituted with two information bits. It increases the quantity of data which can be encoded but it also increases the quantity of resulting noise in the audio file. To extract a secret information from an LSB encoded audio file (stego object), the receiver requires access to the sequence of sample which used in the embedding process.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 4, April 2014)

Usually, the length of the secret information to be encoded is slighter than the total number of samples in an audio file.

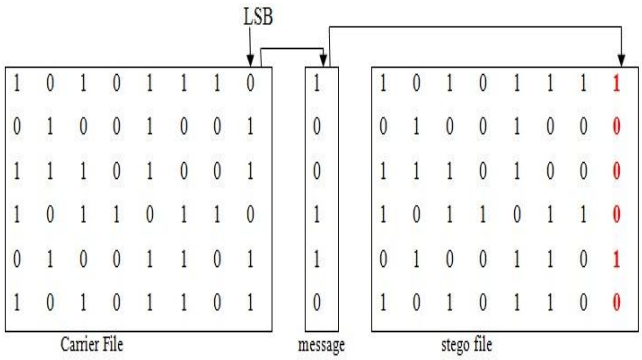


Figure 3: LSB modification procedure for Audio Steganography

A. LSB Insertion method

1. Convert audio file into the data samples.
2. Skip first 40 byte of carrier file because these are address part of wave file.
3. Converted the text message in binary.
4. Convert the length of text message is also in binary.
5. The identifier is selected to hide the text message.
6. An identifier helps in the recovery of text.
7. If there is no identifier in audio file, audio file no hidden text message.
8. The identifier's binary is 10101010.
9. Identifier can be hidden in 8 data samples.
10. The next 10 data samples will serve as the length of text message.
11. The next 10 data samples will be as the width of text message.
12. The text message in the remaining data samples lsb is to be hidden.

B. Data Extraction Process

1. Text can be recovered in a reverse way of how the text is hidden.
2. Now check the received audio file whether identifier present or not.
3. Without identifier, there can be no hidden text in data samples.
4. Both the length and width of the text message from the data samples lsb are to be measured.
5. The lsb bit of data samples should be taken until the length of the message is received
6. Then the message in the lsb bit is to be converted into text.

C. Advantages:

It is the easiest way to hide information in a audio file. It allows huge amount of data to be hided within an audio file, use of only one least significant bit of the host audio file sample gives a capacity equivalent to the sampling rate that could vary from 8 kbps to 44.1 kbps [10]. This technique is more generally used as changes to LSBs usually not create audible change in the sounds.

Disadvantage: This technique has considerably low robustness against attacks.

IV. Conclusion

The proposed technique is considered to be an efficient method for concealing text in audio files such that information can reach the destination in a safe way without being modified. Audio steganography is a technique of sending secret information by concealing it in a carrier file. Only the receiver of this file has acquaintance of the existence of the information. If any other is known about the existence of the information in carrier then the purpose of Steganography is failed. LSB technique of Steganography is very easy to apply. The substitution of LSB of the audio bytes with the message bits will create a small change in audio but that change will not be noticeable by HAS (Human Audio System).

REFERENCES

[1] Nedeljko Cvejic , "Algorithms for audio watermarking andsteganography",http://herkules.oulu.fi/isbn9514273842/isbn9514273842.pdf

[2] "audio steg: overview", Internet publication on www.snotmonkey.com http://www.snotmonkey.com/work/school/405/overview.html.

[3] W Bender, D Gruhl, N Morimoto, A Lu, Techniques for Data Hiding. IBMSyst. J.35(3 and 4), 313–336 (1996)

[4] Shahreza S.S. and Shalmani M.T.M., "Adaptive wavelet domain audio steganography with high capacity and low error rate", in Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, pp: 1729 – 1732, 2008.

[5] RIFF Format http://netghost.narod.ru/gff/graphics/summary/micriff.htm

[6] WAVE PCM SOUNDFILE FORMAT HTTPS://CCRMA.STANFORD.EDU/COURSES/422/PROJECTS/WAVEFORMAT/

[7] N Cvejic, T Seppanen, Increasing Robustness of, LSB Audio Steganography Using a Novel Embedding Method, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC04). vol. 2, (Washington, DC, USA, 2004), pp. 533

[8] N Cvejic, T Seppanen, Reduced distortion bit-modification for LSB audio steganography. J. Universal Comput. Sci.11 (1), 56–65 (2005)

[9] MA Ahmed, LM Kiah, BB Zaidan, AA Zaidan, A Novel Embedding Method to Increase Capacity and Robustness of Low-bit Encoding Audio Steganography Technique Using Noise Gate Software Logic Algorithm.J. Appl. Sci.10, 59–64 (2010)

[10] N. Cvejic, T. Seppanen, "Increasing Robustness of LSB Audio Steganography using a novel embedding method", in Proc. IEEE Int. Conf Info. tech.: Coding and Computing, Vol. 2, pp.533-537, April 2004.