IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 5 Issue 12 December, 2017

Audio Steganography Techniques-An investigation

Debasish Hati
Lecturer, Technique Polytechnic Institute, Hooghly, West Bengal, India[1]
debasishhati2013@gmail.com[1]

ABSTRACT

we can communicate with each other by passing messages which is not secure, but we make a communication be kept secret by embedding the message into carrier or by special tools such as invisible ink, microdots etc. Steganography is the science that involves communicating secret data in an appropriate carrier which is used from hundreds of years. In digital age new techniques of hiding the data inside the carrier are invented which are known as digital steganography. Nowadays, the carrier of the message can be an image, audio, video or a text file. In this paper we have purposed a method to enhance the security level in audio steganography and also improve the quality by making 2-level steganography.

Keywords: Steganography, Audio steganography and its technique**,** Echo Hiding, Phase Coding, Parity Coding, Spread Spectrum, Tone insertion, LSB

1. INTRODUCTION

Steganography is the art and science of covered writing (hide in plain sight) and its techniques are in use from hundreds of years. Digital Steganography is the technique of securing digitized data by hiding it into another piece of data. Today, in digital age the easy access to any form of data such as audio, videos, images and text make it vulnerable to many threats

The data can be copied for purpose of copyright violation, tampered with or illegally accessed without the knowledge of owner. Therefore, the need of hiding secret identification inside different types of digital data is required such that owner can prove copyright ownership; identify attempts to tamper with sensitive data and to embed annotations. The main task of the field of steganography is the storing, hiding, and embedding of secret data in all types of digital data. The main goal of steganography is to communicate securely in a completely undetectable manner such that no one can suspect that it exist some secret information. Unlike cryptography, which secures data by transforming it into another unreadable format, steganography makes data invisible by hiding (or embedding) them in another piece of data. Thus cryptography is science of overt secret writing while steganography as covert secret writing. The cover, host or the carrier is the target media in which information is hidden so that other person will not notice the presence of the information. The modified cover, including the hidden data, is referred to as a *stego-object* which can be stored or transmitted as a message. The secret information can be embedded in various types of cover. If information is embedded in cover text file, the result is stego-text object. It is possible to have cover audio, video and image for embedding which result in stego-audio, stego -vedio, stego- image Nowadays, the combinations of steganography and cryptography methods are also used to ensure data confidentiality and to improve the information security.

2. TYPES OF STEGANOGRAPHY

Depending on the type of the cover object there are many suit a)e stenographic techniques which are in order to obtain security.

a) **Image Steganography:** The process of concealing the secret message in an image file is known as image steganography. It has certain limitations like you cannot embed a large amount of data in an image because it may distort which may arise suspicion that the image might contain any information.

b) **Video Steganography:** The process of concealing the secret message in an Video file is known as Video steganography. Video Steganography is far more safe and efficient as compared to that of the image steganography as you can embed large amount of data in audio and frames of the video.

c) **Network Steganography:** Network Steganography method uses modification of a single network protocol. The protocol modification may be applied to the PDU (Protocol Data Unit), time relations between exchanged PDUs, or both (hybrid methods). It is Highly secure and robust.

d) **Audio Steganography:** In Audio Steganography audio is used as the cover to hide the secret information it is also very robust in nature but with limitation of the amount of data one can hide.

e) **Text Steganography:** Secret Data is hided in a text file. This method lacks robustness and is not that much efficient in hiding the data. It can be easily detected by the eyes of intruders.

3. DATA HIDING

Various schemes are used for data hiding in audio, such as echo hiding, time domain modification, and spread spectrum technology. Data hiding in audio must satisfy at least the three constraints of security or imperceptibility, robustness, and capacity. These terms are commonly used to describe the properties of different data hiding schemes.

Security: Data hiding in audio is also called in audibility. In most cases, security, including perceptual transparency of the hidden data, is considered to be the most important issue. In other words, the noise introduced by the hidden data should be almost in audible and should not degrade the audio quality. The statistical properties of the embedded audio signal should be exactly the same as the original audio to ensure that the hidden data is imperceptible and undetectable by third parties.

Robustness: The algorithm should be robust enough to withstand unintentional or intentional attempts such as removal or alteration of the hidden data. Even with unfavourable conditions such as bad wireless channels which degrade the audio quality, the hidden data should be recovered successfully.

Capacity: Often, the capacity of the hidden data is also a very demanding aspect. Capacity refers to the number of bits per second that can be transmitted by the data hiding system. This depends on the underlying technology and the choice of parameters for the hiding scheme. At present, the data rates reach several hundred bits per second.

Security, robustness, and capacity have contradictory arguments so they cannot be adjusted independently. For instance, increases of the data hiding capacity will degrade the robustness and security. This trade-offs form the triangle shown in Fig. 2 with an appropriate operating point within the limits of the triangle chosen for different applications.

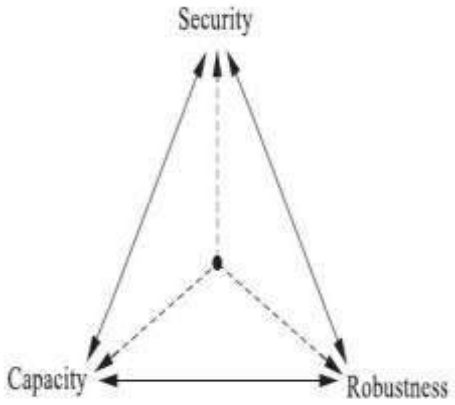

Fig. 1 Trade-off between security, robustness, and Capacity

4. METHODS OF AUDIO STEGANOGRAPHY

This section presents some common methods used in audio Sateganography

4.1 LSB Coding

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. The following diagram illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method (Fig. 3).

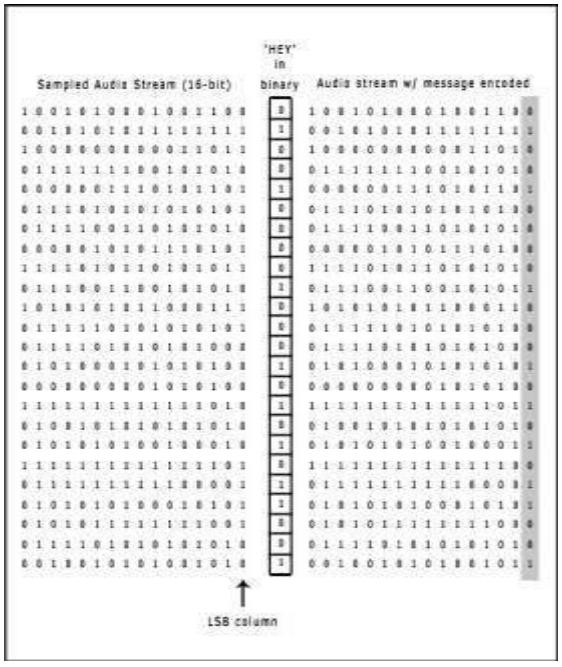

Fig. 2 LSB CODING

Standard LSB ALGORITHM:

It performs bit level manipulation to encode the message. The following steps are:-a. Receives the audio file in the form of bytes and converted in to bit pattern. b. Each character in the message is converted in bit pattern. c. Replaces the LSB bit from audio with LSB bit from character in the message.

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. Thus, one should consider the signal content before deciding on the LSB operation to use. For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise. On the other hand, the same noise would be audible in a sound file containing a piano solo.
The main advantage of the LSB coding method is low computational complexity of the algorithm while its major disadvantage : As the number of used LSBs during LSB coding increases or, equivalently, depth of the modified LSB layer becomes larger, probability of making the embedded message statistically detectable increases and perceptual transparency of stego objects is decreased.

4.2 Phase Coding

Phase coding addresses the disadvantages of the noise-inducing methods of audio Steganography. Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Rather than introducing perturbations, the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal (fig. 4) , achieving an inaudible encoding in terms of signal-to-perceived noise ratio.

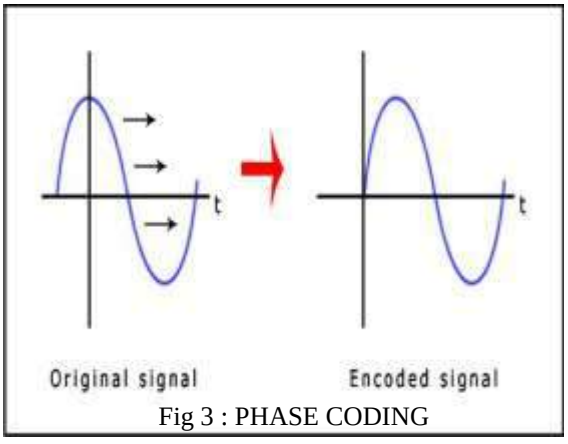

Fig 3 : PHASE CODING

The phase coding method breaks down the sound file into a series of N segments. A Discrete Fourier Transform (DFT) is applied to each segment to create a matrix of the phase and magnitude. The phase difference between each segment is calculated, the first segment (s0) has an artificial absolute phase of p0 created, and all other segments have newly created phase frames. The new phase and original magnitude are combined to get the new segment, Sn. These new segments are then concatenated to create the encoded output and the frequency remains preserved. In order to decode the hidden information the receiver must know the length of the segments and the data interval used. The first segment is detected as a 0 or a 1 and this indicates where the message starts.

4.3 Echo Hiding

Echo hiding embeds its data by creating an echo to the source audio. Three parameters of this artificial echo are used to hide the embedded data, the delay, the decay rate and the initial amplitude. As the delay between the original source audio and the echo decrease it becomes harder for the human ear to distinguish between the two signals until eventually a created carrier sound's echo is just heard as extra resonance.

In addition, offset is varied to represent the binary message to be encoded. One offset value represents a binary one, and a second offset value represents a binary zero. If only one echo was produced from the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal as shown in fig. 5.

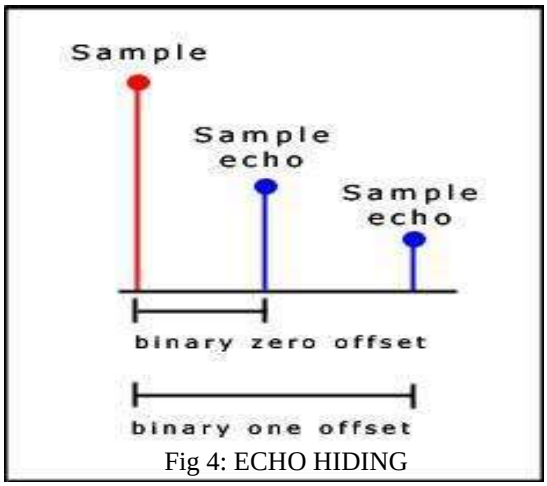

Fig 4: ECHO HIDING

The blocks are recombined to produce the final signal. The "one" echo signal is then multiplied by the "one" mixer signal and the "zero" echo signal is multiplied by the "zero" mixer signal. Then the two results are added together to get the final signal as shown in fig. 6. The final signal is less abrupt than the one obtained using the first echo hiding implementation. This is because the two mixer echoes are complements of each other and that ramp transitions are used within each signal .

These two characteristics of the mixer signals produce smoother transitions between echoes.
The following diagram summarizes the second implementation of the echo hiding process.

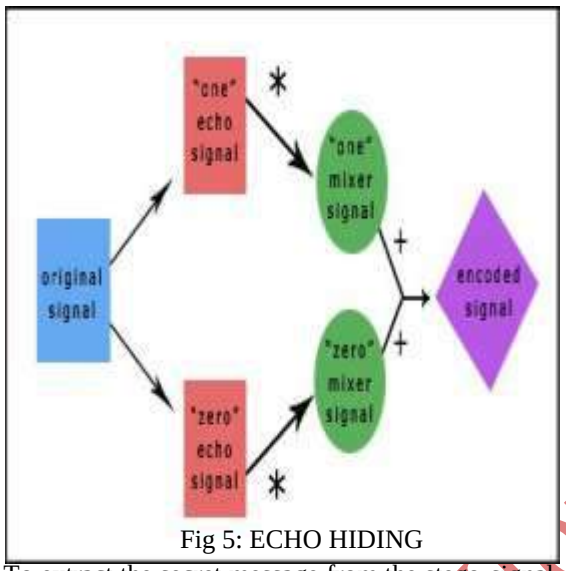

Fig 5: ECHO HIDING

To extract the secret message from the stego-signal, the receiver must be able to break up the signal into the same block sequence used during the encoding process. Then the autocorrelation function of the signal's spectrum (the spectrum is the Forward Fourier Transform of the signal's frequency spectrum) can be used to decode the message because it reveals a spike at each echo time offset, allowing the message to be reconstructed .

4.4 Spread Spectrum

Spread spectrum systems encode data as a binary sequence which sounds like noise but which can be recognised by a receiver with the correct key. The technique has been used by the military since the 1940s because the signals are hard to jam or intercept as they are lost in the background noise. Spread spectrum techniques can be used for watermarking by matching the narrow bandwidth of the embedded data to the large bandwidth of the medium.
Two versions of SS can be used in audio Steganography: the direct-sequence and frequency-hopping schemes. In direct-sequence SS, the secret message is spread out by a constant called the chip rate and then modulated with a pseudorandom signal. It is then interleaved with the cover-signal. In frequency-hopping SS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies.
Spread Spectrum Steganography has significant potential in secure communications – commercial and military. Audio Steganography in conjunction with Spread Spectrum may provide added layers of security.
Spread spectrum encoding techniques are the most secure means by which to send hidden messages in audio, but it can introduce random noise to the audio thus creating the chance of data loss. They have the potential to perform better in some areas than LSB coding, parity coding, and phase coding techniques in that it offers a moderate data transmission rate while also maintaining a high level of robustness against removal techniques.

The following procedural figure illustrates the design (fig. 7):

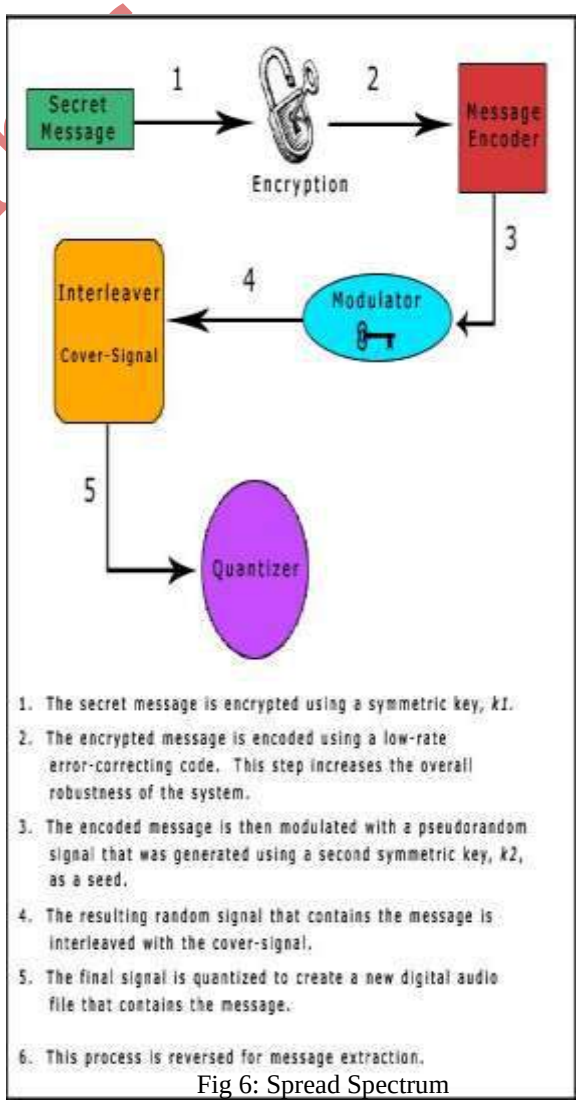

Fig 6: Spread Spectrum

5. CONCLUSION

This paper has looked in detail at the major techniques used for data hiding in audio files. Section I gave an overview of Steganography and in particular the concept of Audio Steganography. Section II described in detail, various Audio Steganography algorithms namely LSB Coding, Phase Coding, Spread Spectrum and Echo Hiding. At the end,Audio encoding process was discussed with the help of its block diagram. It can be concluded that, steganography does in fact have a number of disadvantages i.e. it has high overhead for hiding a few bits of information. This disadvantage can be overcome relatively easily. Another problem is that a steganographic system is rendered useless once it has been discovered. This also can be overcome by utilizing a key for the insertion and extraction of the hidden data. Also, Spread Spectrum method is known to be very robust, but as a consequence the cost is very large, the implementation is relatively complex, less secure and the information capacity is very limited. Current spread spectrum stegano-graphic applications with audio media are primarily limited to providing proof of copyright and assurance of content integrity. There is the potential to expand the applications to include the embedding of covert communications. Above mentioned problems related to spread spectrum can be overcome by using Direct Sequence Spread Spectrum (DSSS).DSSS used to increase the security and robustness of the system. Improvement can be achieved in robustness on the expense of reducing the capacity of hiding.

6. REFRENCES

[1] Sara Khosravi, MashallahAbbasiDezfoli, Mohammad HosseinYektaie, " A new steganography method based HIOP (Higher Intensity Of Pixel)algorithm and Strassen's matrix multiplication" , Journal of Global Research in Computer Science, Vol. 2, No. 1, 2011.

[2] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA,2000.

[3] G. J. Simmons, "The prisoners' problem and the subliminal channel" in Proc. Advances in Cryptology (CRYPTO '83), pp. 51-67.

[4] Robert Krenn, Steganography and steganalysis, Internet Publication, March 2004. Available at:http://www.krenn.nl/univ/cry/steg/article.pdf

[5] Christian Cachin, Digital Steganography, Encyclopedia of Cryptography and Security, 2005.

[6] ShashikalaChannalli et al ," Steganography An Art of Hiding Data "International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.

[7] Gruhl D, Lu A, Bender W. Echo hiding. *Lecture Notes inComputer Science*, 1996, 1174: 295-315.

[8] Xu Chansheng, Wu Jiankang, Sun Quibin, et al. Applications of digital watermarking technology in audio signals. *Journal of Audio Engineering Society*, 1999, 47(10): 805-812.

[9] Garcia R A. Digital watermarking of audio signals using a psychoacoustic auditory model and spread spectrum theory. In: 107th AES Convention. New York, USA, 1999:2713-2720.

[10] XU Shuzheng, ZHANG Peng, WANG Pengjun, YANG Huazhong, "Performance Analysis of Data Hiding in MPEG-4 AAC Audio" TSINGHUA SCIENCE AND TECHNOLOGY Volume 14, Number 1, February 2009