Volume 4, No. 9, July-August 2013

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Encoding and Advanced LSB Technique

Kamalpreet Kaur
M.tech Computer Science,
Department of CSE, Rbiebt, Kharar
Punjab Technical University, India.
Kamal.27.sandhu@gmail.com

Er. Deepankar Verma
AP,M.tech Computer Science,
Department of CSE, Rbiebt, Kharar
Punjab Technical University, India.
deepankar9819@gmail.com

Abstract: 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. The purpose of this paper is to come up with a technique hiding the presence of secret message and increase the security level. Steganography is the art of secret communication. Its purpose is to hide the presence of communication. This paper uses the Multi-Level Steganography, is a new concept for hidden communication in computer networks. It uses at least two steganographic methods are utilized either these methods are same or different type in such a way that one method serves as a carrier for the second one. Multi-Level Steganography has advantage of difficult decoding and sending two or more secret message through a single cover object. Here three different steganographic methods have been used instead of using one steganographic method. This has been done with a layering approach. This paper defines a method for audio steganography using LSB modification, parity encoding and advanced LSB technique in multi-level steganography. In this thesis I will present the review of three layered approach for audio multi-level steganography. Here three secret messages rather than one can be transmitted with a single cover file. This method provides an effective way of to achieve higher security, to increase undetectability of upper-level methods, the clarity of digital audio signal should not be harmed and to maintain the robustness during the substitution of bits.

Keywords: Information security, Information hiding, Steganography, Audio steganography, Multi-level steganography, Stego object, Decoy object

I. INTRODUCTION

A. *Steganography:*

The term Steganography is forked from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". Steganography is an art and science known for ages, whose main aim is to hide secret data (steganograms) in innocent-looking carriers [4].

Steganography can be applied to different objects like text, picture, image, audio or video. This objects called cover object or carrier object of the steganographic method. The secret message can also be of types like text, picture, image, audio or video. These objects are called message object. After application of steganographic method the produced output file is called stego-object. Dr. Al Najjar first introduced another type of object which is called intermediate object or decoy object. This decoy object is output of first level steganographic method and input of second level steganographic method. Decoy object actually nullifies the requirement of two different cover objects for sending two different secret messages [1].

B. *Audio Steganography:*

Audio steganography is the technique of hiding information inside an audio signal. Embedding secret messages into digital sound is known as audio Steganography. It is usually a more difficult process than embedding messages in other media. Audio Steganography methods can embed messages in WAV, AU, and even MP3 sound files. As data is embedded in the signal, it gets modified. This modification should be made imperceptible to the human ear. Image can also be taken as a medium but audio steganography is more challenging because of the characteristics of Human Auditory System (HAS) like large power, dynamic range of hearing and large range of audible frequency [8].

C. *Multi-Level Steganography:*

Multi-Level Steganography is a new concept of information hiding in telecommunication networks that uses features of an existing steganographic method (the upper level method) to create a new one (the lower-level method). Multi-Level Steganography (MLS) was originally proposed by Al-Najjar for picture steganography. MLS is based on combining two or more steganographic methods in such a way that one method (the upper-level) is a carrier for the other method (the lower-level) [2].

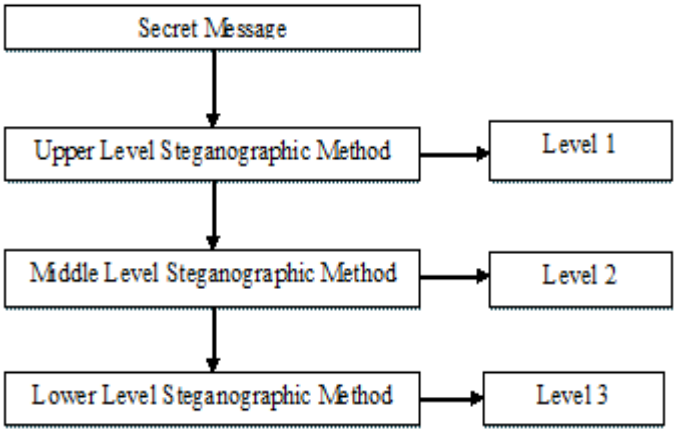

Figure 1. Overview of Proposed Multi-level Steganography System

D. Least Significant Bit (LSB):

One of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is Least Significant Bit modification coding technique. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message [1].

The LSB technique takes advantage of the HAS which cannot hear the slight variation of audio frequencies at the high frequency side of the audible spectrum. The LSB technique allows high embedding rate without degrading the quality of the audio file. It is possible to encode messages using frequencies that are inaudible to the human ear. Using any frequencies above 20.000 Hz, messages can be hidden inside sound files and will not be detected by human checks. Furthermore, it is relatively effective and easy to implement [8].

E. Parity Encoding:

Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion [1].

F. Advanced Least Significant Bit (LSB):

An advanced LSB embedding scheme that possesses the advantages of LSB embedding technique, but it also provides an additional level of communication security. The advanced LSB scheme breaks the regular pattern of pairs of values in the histogram domain, increasing the difficulty of steganalysis and thereby raising the level of security. In advanced LSB the hidden message is undetectable by the well-known steganalysis attacks.

II. RELATED WORK

Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique (Prof. Samir Kumar Bandyopadhyay and Barnali Gupta Banik) [1]

Steganography is a very well-known method of information security through information hiding. Here two different steganographic methods have been used instead of using one steganographic method. This has been done with a layering approach. This method is named as multi-level steganography. Multi-Level Steganography has advantage of difficult decoding and sending two secret message through a single cover object.

Multi-Level Steganography: Improving Hidden Communication in Networks (Wojciech Frączek, Wojciech Mazurczyk, Krzyszt of Szczypiorski) [2]

The paper presents Multi-Level Steganography (MLS), which defines a new concept for hidden communication in telecommunication networks. In MLS, at least two steganographic methods are utilized simultaneously, in such a way that one method (called the upper-level) serves as a carrier for the second one (called the lower-level). Such a relationship between two (or more) information hiding solutions has several potential benefits. The most important is that the lower-level method steganographic bandwidth can be utilized to make the steganogram unreadable even after the detection of the upper-level method: e.g., it can carry a cryptographic key that deciphers the steganogram carried by the upper-level one. It can also be used to provide the steganogram with integrity. Another important benefit is that the lower-layer method may be used as a signaling channel in which to exchange information that affects the way that the upper-level method functions, thus possibly making the steganographic communication harder to detect.

An Integrated Synchronized Protocol for Secure Information Transmission derived from Multilevel Steganography and Dynamic Cryptography (Navneet Singh Sikarwar) [6]

In this paper a protocol is elucidated, it is based on multilevel steganography and dynamic cryptography in the secure information transmission, because the growing possibilities of modern communications require the special means of confidential and intellectual property protection against unauthorized access and use. Especially these problems are actually for computer networks, which make possible to exchange the large amount of digital information (text, audio, video, and image). The use of multilevel steganography provides more strength compare to simple steganography technique.

The Decoy: Multi-Level Digital Multimedia Steganography Model (Atef jawad Al-najjar) [3]

Define four types of objects: message-object, intermediate-object, cover-object, and stego-object. All objects are represented by a finite set of elements, where each element is in turn represented by a finite sequence of bits. The bits make the primitive components of the representation. A multimedia (MM) object can be in one of several classes: text, picture, image, audio, or video. MM objects are used for human-human, human-machine, or machine-machine communication. Hence, MM objects have storage and transmission requirements. For example, an audio object can be represented in several formats, e.g., wav and MP3. Text objects can be represented using an image, ASCII or Unicode, among other representations. MM objects can be published or hidden. The focus of this paper is twofold to develop an abstract multi-level model; and to use a published object to conceal (hide) a secret object using the proposed model. An example of hiding a text message-object, represented by a black and white (B&W) image object, into a gray-image (intermediate-object, or decoy) that is then hidden in a color image object in RGB-color format, is given.

Data hiding technique: Audio steganography using LSB technique (Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar) [5]

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. The objective of this paper is to come up with a technique

hiding the presence of secret message. Steganography is 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 information in a cover (host) audio signal in an imperceptible way. Hidden information from the stego, or data-embedded audio signal, is retrieved 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 has been tested successfully on a .wav file at a sampling frequency of 3000 samples/second with each sample containing 8 bits.

Audio Steganography: A Survey on Recent Approaches (Masoud Nosrati Ronak Karimi Mehdi Hariri) [4]

In this study, we will have a survey on audio steganography recent researches. Due to it, some basic concepts of audio steganography and HAS including Least Significant Bit (LSB) Coding, Parity Coding, Phase Coding, Spread Spectrum (SS) and Echo data hiding are covered. In follow, a brief introduction and abstract of 7 recent methods for audio steganography is presented.

III. PROPOSED METHOD

Here three secret messages rather than one can be transmitted with a single cover file. Layering approach gives opportunity to do so. In this paper three layered approach has been presented. At the first level, cover file (C) can be embedded with the first secret message S1. Assuming the decoy file as C1 which is cover file for next middle level where secret message can be denoted as S2. Assuming the decoy file as C12 which is cover file for next lower level where secret message can be denoted as S3. Now the final stego file created as C123. So C123 holds three secret messages S1, S2 and S3.

Three levels of steganography can be identified as layer 1, layer 2 and layer 3. At layer 1 LSB technique and at layer 2 parity encoding technique and at layer 3 Advanced LSB technique has been used.

To achieve the set objectives, our proposal will focus on developing a better technique for audio multi-level steganography that will maintain the higher security, undetectability, increased bandwidth, clarity of digital audio signal and integrity. We will propose the technique using LSB, parity encoding and advanced LSB technique in multi-level steganography and implement it in MATLAB.

The proposed work will be based on mainly three steps:

a. In the level 1, an audio file will be selected whose audio samples are selected, using LSB technique and will be used to conceal the secret data. Firstly secret data is converted into encoded form using parity encoder and then hiden into audio file. In this level first secret message hided under cover object using LSB technique.
b. In the level 2, the output of the level 1 is the input for level 2. In this level second secret message hided under decoy object using parity encoding technique.
c. In the level 3, the output of the level 2 is the input for level 3. In this level third secret message hided under decoy object using advanced LSB technique. Output of this level is called stego object.
d. Now, stego object is transmitted to the receiver.

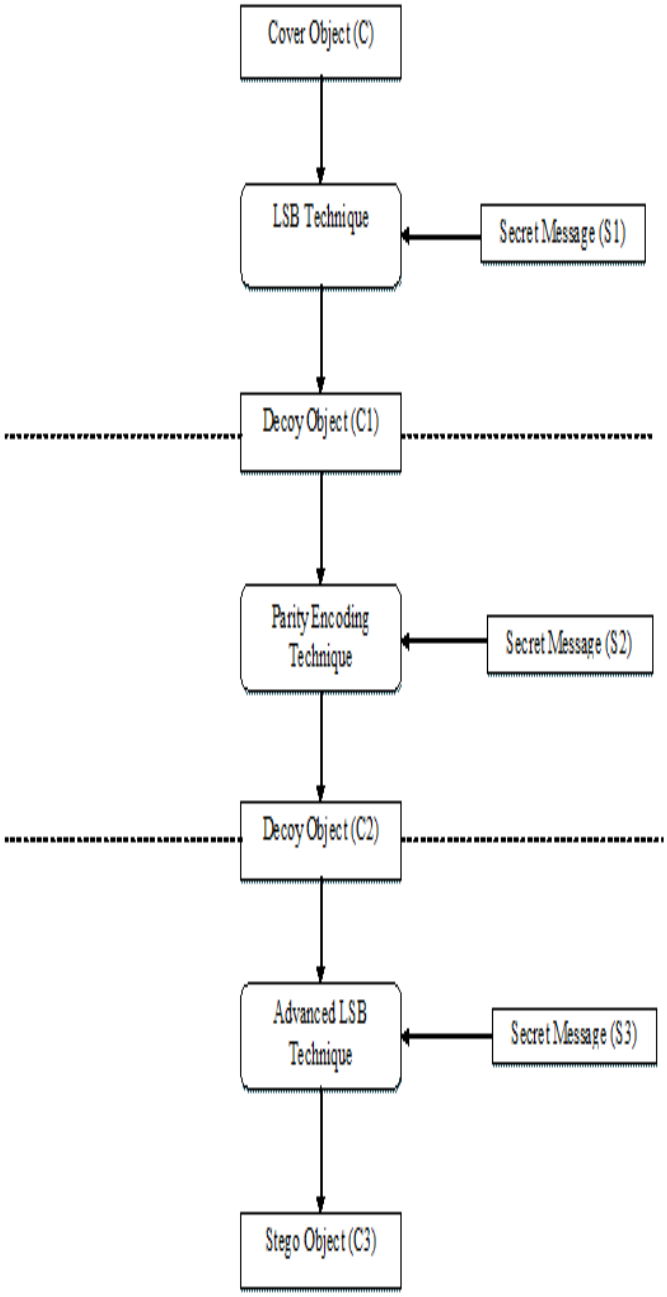

Figure 2. Proposed Multi-Level Audio Steganography System

IV. CONCLUSTION

This paper proposed an audio steganography technique for hiding text data into digital audio files based on three different techniques to select the carrier audio samples into which bits of the secret data are to be hidden. In this paper three secret messages can be hidden. Three traditional method of steganography blended in a level based approach to reach the

goal. The output stego object is very difficult to decode which makes this method successful in the world of audio steganography.

V. REFERENCES

[1] Prof. Samir Kumar Bandyopadhyay and Barnali Gupta Banik: "Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique", Volume 1, Issue 2, July – August 2012.

[2] Wojciech Fraczek, Wojciech Mazurczyk, Krzysztof Szczypiorski: "Multi-Level Steganography: Improving Hidden Communication in Networks", Cornell University Library, Jan 2011, http://arxiv.org/ftp/arxiv/papers/1101/1101.4789.pdf

[3] Al-Najjar AJ: "The Decoy: Multi-Level Digital Multimedia Steganography Model", In Proc. Of 12th WSEAS International Conference on COMMUNICATIONS, Heraklion, Greece, July 23-25, 2008.

[4] Masoud Nosrati, Ronak Karimi, Mehdi Hariri: "Audio Steganography: A Survey on Recent Approaches", World Applied Programming, Vol (2), No (3), March 2012.

[5] Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar:"Data hiding technique: Audio steganography using LSB technique", Vol. 2, Issue 3, May-Jun 2012, pp.1123-1125

[6] Navneet Singh Sikarwar:"An Integrated Synchronized Protocol for Secure Information Transmission derived from Multilevel Steganography and Dynamic Cryptography", Volume 3, Issue 4, April 2012.

[7] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das: "A Tutorial Review on Steganography", IC3–2008.

[8] Youssef Bassil: "A Two Intermediates Audio Steganography Technique", VOL. 3, NO.11 Nov, 2012

[9] K. Gopalan, "Audio steganography using bit modification", Proceedings of International Conference on Multimedia, vol.1, pp.629-632, 2003.

[10] B. Santhi, G. Radhika and S. Ruthra Reka: "Information Security using Audio Steganography -A Survey", Research Journal of Applied Sciences, Engineering and Technology 4(14): July 15, 2012.