ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2, Issue 2, Ver. 2 (April - June 2014)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Audio Steganography by LSB Method and Enhanced Security with AES

[I]Gaurav Saini, [II]Parulpreet Singh
[I,II]Dept. of Computer Science, Baddi University of Emerging Sciences and Technology, Baddi, HP, India

Abstract
In this study, we will have a survey on audio steganography recent researches. Steganography techniques are used in Multimedia data transfer. The paper presents Hiding Techniques that define general technique that can be applied to every network steganography method to improve its undetectability. In this proposed method, secret message in form of audio file is embedded within another carrier audio file (.wav) .In the transmitter end the output will be similar to the carrier with secret message embedded inside. In the second level it uses a more powerful modified LSB (Least Significant Bit) Method to encode the message into audio. It performs bit level manipulation to encode the message. In the third level it uses the AES algorithm to increase the audio bit size and also to improve the security. The quality of sound depends on the size of the audio which the user selects and length of the message. This method has provided an effective way to achieve higher security, increased undetectability as compare to previous results.

Keywords
Audio Steganography, LSB Method, Cryptography, Data Hiding and AES.

I. Introduction

Steganography is the art and science of hiding the fact that communication is taking place. Using the steganography, we can embed a secret message inside a piece of unsuspicious information and send it without anyone knowing of the existence of the secret message. Information security is essential for confidential data transfer. Steganography is one of the ways used for secure transmission of confidential information. Hiding information in audio is less suspicious than communicating an encrypted file. The main purpose of steganography is to convey the information secretly by concealing the very existence of information in some other medium such as 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.

Steganographic algorithm: It can be characterized by a number of defining properties. Three of them, are most important for audio steganographic algorithms, are introduced below:

Transparency: It evaluates the audible distortion due to signal modifications like message embedding or attacking. In order to meet fidelity constraint of the embedded information, the perceptual distortion introduced due to embedding should be below the masking threshold estimated based on the HAS/HVS and the host media.

Capacity: The Capacity of an information hiding scheme refers to the amount of information that a data hiding scheme can successfully embed without introducing perceptual distortion in the marked media.

Robustness: It measures the ability of embedded data or watermark to withstand against intentional and unintentional attacks. Unintentional attacks generally include common data manipulations such as lossy compression, digital-to-analog conversion, re-sampling, requantization, etc. whereas intentional attacks cover a broad range of media degradations which include addition white and colour noise, rescaling, rotation (for image and video steganography schemes), resizing, cropping, random chopping, and filtering attacks.

Steganography Mechanism: Steganography is the technique of hiding the message in a chosen carrier such that no one except the intended recipient is aware of its existence. Block diagram of steganography mechanism is shown in Figure 1. Here a secret data is being embedded inside a cover image to produce the stego image. A key is often needed in the embedding process. The proper stego key is used by the sender for the embedding procedure. The same key is used by the recipient to extract the stego cover image in order to view the secret data. The stego image should look almost identical to the cover image.

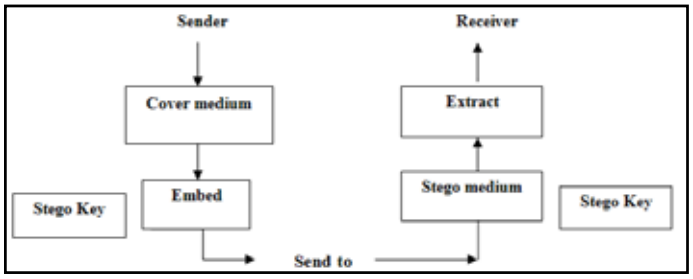

Fig. 1 : Block Diagram of Stegnography Mechanism.

Types of Steganography: In modern approach, depending on the nature of cover object, steganography can be divided into five types:

Text Steganography: Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of textual elements (e.g., characters). It includes line-shift coding, word-shift coding and feature coding.

Image Steganography: Images are the most popular cover objects used for steganography. . In the domain of digital images many different file formats exist and for these file formats different algorithms exist. These different algorithms used are least significant bit insertion, Masking and filtering, Redundant Pattern Encoding, Encrypt and Scatter, Algorithms and transformations.

Audio Steganography: In audio steganography, secret message is

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods like LSB coding, Phase coding, spread spectrum, Echo hiding which are used for audio steganography.

Video Steganography: Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds.

Protocol Steganography: The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. There are covert channels in the layers of the OSI network model where steganography can be used.

Uses of Steganography: The three most popular and researched uses for steganography in an open systems environment are covert channels, embedded data and digital watermarking. Covert channels can be very useful for any secure communications needs over open systems such as the Internet. By embedding the hidden data into the cover message and sending it, you can gain a sense of security by the fact that no one knows you have sent more than a harmless message other than the intended recipients Digital watermarking is very important in the detection and prosecution of software pirates/digital thieves. Steganography is used by some modern printers, including HP and Xerox brand color laser printers.

II. Steganographic Methods

The following formula provides a very generic description of the pieces of the steganographic process:
cover_medium + hidden_data + stego_key = stego_medium
In this context, the *cover_medium* is the file in which we will hide the *hidden_data*, which may also be encrypted using the *stego_key*. The resultant file is the *stego_medium* (which will, of course. be the same type of file as the cover_medium). The cover_medium (and, thus, the stego_medium) are typically image or audio files. In this article, I will focus on image files and will, therefore, refer to the *cover_image* and *stego_image*.
Before discussing how information is hidden in an image file, it is worth a fast review of how images are stored in the first place. An image file is merely a binary file containing a binary representation of the color or light intensity of each picture element (pixel) comprising the image.
Images typically use either 8-bit or 24-bit color. When using 8-bit color, there is a definition of up to 256 colors forming a palette for this image, each color denoted by an 8-bit value. A 24-bit color scheme, as the term suggests, uses 24 bits per pixel and provides a much better set of colors. In this case, each pix is represented by three bytes, each byte representing the intensity of the three primary colors red, green, and blue (RGB), respectively. The Hypertext Markup Language (HTML) format for indicating colors in a Web page often uses a 24-bit format employing six hexadecimal digits, each pair representing the amount of red, blue, and green, respectively. The color orange, for example, would be displayed with red set to 100% (decimal 255, hex FF), green set to 50% (decimal 127, hex 7F), and no blue (0), so we would use "#FF7F00" in the HTML code.
The size of an image file, then, is directly related to the number of pixels and the granularity of the color definition. A typical 640x480 pix image using a palette of 256 colors would require a file about 307 KB in size (640 • 480 bytes), whereas a 1024x768 pix high-resolution 24-bit color image would result in a 2.36 MB file (1024 • 768 • 3 bytes).
To avoid sending files of this enormous size, a number of compression schemes have been developed over time, notably Bitmap (BMP), Graphic Interchange Format (GIF), and Joint Photographic Experts Group (JPEG) file types. Not all are equally suited to steganography, however.
GIF and 8-bit BMP files employ what is known as *lossless* compression, a scheme that allows the software to exactly reconstruct the original image. JPEG, on the other hand, uses *lossy* compression, which means that the expanded image is very nearly the same as the original but not an exact duplicate. While both methods allow computers to save storage space, lossless compression is much better suited to applications where the integrity of the original information must be maintained, such as steganography. While JPEG can be used for stego applications, it is more common to embed data in GIF or BMP files.
The simplest approach to hiding data within an image file is called *least significant bit (LSB) insertion*. In this method, we can take the binary representation of the hidden_data and overwrite the LSB of each byte within the cover_image. If we are using 24-bit color, the amount of change will be minimal and indiscernible to the human eye. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011

Now suppose we want to "hide" the following 9 bits of data (the hidden data is usually compressed prior to being hidden): 101101101. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in **bold** have been changed):

10010101 00001100 11001001
10010111 00001110 11001011
10011111 00010000 11001011

Note that we have successfully hidden 9 bits but at a cost of only changing 4, or roughly 50%, of the LSBs.
This description is meant only as a high-level overview. Similar methods can be applied to 8-bit color but the changes, as the reader might imagine, are more dramatic. Gray-scale images, too, are very useful for steganographic purposes. One potential problem with any of these methods is that they can be found by an adversary who is looking. In addition, there are other methods besides LSB insertion with which to insert hidden information.

Cryptography: Cryptography can be defined as the conversion of data into a scrambled code that can be deciphered and sent across a public or private network. Cryptography uses two main styles or forms of encrypting data; symmetrical and asymmetrical. Symmetric encryptions, or algorithms, use the same key for encryption as they do for decryption. Other names for this type of encryption are secret-key, shared-key, and private-key. The encryption key can be loosely related to the decryption key; it does not necessarily need to be an exact copy. Symmetric cryptography is susceptible to plain text attacks and linear cryptanalysis meaning that they are hack able and at times simple to decode. With careful

planning of the coding and functions of the cryptographic process these threats can be greatly reduced. Asymmetric cryptography uses different encryption keys for encryption and decryption. In this case an end user on a network, public or private, has a pair of keys; one for encryption and one for decryption. These keys are labelled or known as a public and a private key; in this instance the private key cannot be derived from the public key. The asymmetrical cryptography method has been proven to be secure against computationally limited intruders. The security is a mathematical definition based upon the application of said encryption. Essentially, asymmetric encryption is as good as its applied use; this is defined by the method in which the data is encrypted and for what use. The most common form of asymmetrical encryption is in the application of sending messages where the sender encodes and the receiving party decodes the message by using a random key generated by the public key of the sender.

III. Audio Steganography

Audio Steganography is the technique of hiding information inside an audio signal. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV, AU, and even MP3 sound files. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. 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. All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

Least Significant Bit (LSB) Coding

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. LSB hiding is a simple and fast method for embedding information in an audio signal. It consists of embedding each bit from the message in the least significant bit of the cover audio in a specific way. LSB hiding schemes provide a very high channel capacity for transmitting many kinds of data and is easy to implement and to combine with other hiding techniques. The length of the secret message to be encoded should be smaller than the total numbers of samples in a sound file. 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. Furthermore, it is relatively effective and easy to implement.

Advantage: It is the simplest way to embed information in a digital audio file. It allows large amount of data to be concealed within an audio file, use of only one LSB of the host audio sample gives a capacity equivalent to the sampling rate which could vary from 8 kbps to 44.1 kbps (all samples used). This method is more widely used as modifications to LSBs usually not create audible changes to the sounds.

Disadvantage: It has considerably low robustness against attacks.

IV. Related Work

There are many papers proposed in this audio steganography with most of the papers embed secret audio file in a carrier audio file. Some of them used cryptography for additional security. The authors are mainly concerned with the security of the embedded message. To achieve high robustness and capacity of our steganalysis various methodologies have been implemented and verified their approach.

In [1] *kaliappan gopalan* proposed a steganalysis in audio file with an encryption key for the embedded secret audio file. In [2] *M Asad,J Gilani & A Khalid* proposed a audio steganography with an encrypted audio file using Advanced Encryption Standard(AES). In [3] *Mazdak Zaman, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad, Farhang Jaryani, Hamed Taherdoost, Akram M. Zeki* proposed a genetic algorithm for the embedding secret audio files for achieving higher robustness and capacity. In [4] *kaliappan gopalan* embed the information of secret message in spectral domain of a cover audio or image files. In [5] *K.B.Raja, C.R.Chowdary, Venugopal K R,& L.M.Patnaik* proposed a work on image steganography where a LSB embedding is used and then DCT is performed followed by a compression technique to provide high security in the hidden data. In [6] *Hossein Malekmohamadi and Shahrokh Ghaemmaghami* proposed an enhancement in image steganalysis of LSB matching by reducing the complexity using gober filter co-officients. In [7] *R Balagi & G Naveen* extended their work towards video steganography by embedding the secret information in some particular frames. In [8] Data hiding technique: Audio steganography using LSB technique (Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar): 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. 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.

V. AES

In early 1997 NIST announced that they were looking for a successor to DES and they solicited input from the cryptographic community. Because of the amount of interest this sparked, NIST decided to issue a call for new algorithms in the fall of 1997 and to hold a competition to decide on the best candidate for the standard. Submissions ran well into 1998 and in all 15 algorithms were entered into the competition. After a public debate and two conferences organised by NIST in which the competing algorithms were analysed both for security as well as for performance a shortlist of 5 candidates was selected. Another round of cryptanalysis followed which ended with another conference in April 2000. On October 2nd 2000 NIST announced that the Rijndael algorithm – designed by Belgian cryptographers Joan Daemen and Vincent Rijmen – had won the competition and would become AES. The AES algorithm is a block cipher with a block size of 128 bits (16 bytes). It supports key lengths of 128, 192 and 256 bits. AES has been thoroughly screened by the cryptographic community and no significant attacks have been found to date. NIST currently believes AES to be secure beyond 2030. Contrary to its predecessor

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

DES – which was specifically designed for sensitive but not for secret information – AES has been approved for use in encrypting official material marked 'SECRET' with 128-, 192- and 256-bit keys and for use in encrypting official material marked 'TOP SECRET' with 192- and 256-bit keys by the United States' Committee on National Security Systems (CNSS).
A number of AES parameters depend on the key length. E.g., if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. The present the most common key size likely to be used is the 128 bit key.

VI. Conclusion

The steganography is one of the safest forms of data transmissions in this digital world. In our proposed method, audio steganography is enhanced more by means of cryptographic key algorithms. The message signal is transmitted with utmost security and can be retrieved without any loss in transmission in this method. This proposed system will not change the size of the file even after encoding and also suitable for any type of audio file format. It was found that LSB were not used and only uses two bit positions data that will be hidden and occurs only from a frame. It has considerably low robustness against the attacks. Therefore maintain the robustness during the substitutions of bits.The heading of the Acknowledgment section and the References section must not be numbered.

VII. Acknowledgment

Thanks to my Guide and family member who always support, help and guide me during my dissertation. Special thanks to my father who always support my innovative ideas.

References

[1] *Gopalan., "Audio steganography using bit modification", 2003 IEEE International conference on Acoustic, Speech and Signal Processing.*
[2] *Muhammad Asad, Junaid Gilani, Adnan Khalid "An Enhanced Least Significant Bit Modification Technique for Audio Steganography", 2011 international conference on Computer Networks and Information Technology (ICCNIT).*
[3] *Zamani, M., Manaf, A, Ahmad, R.B., Jaryani, F., Taherdoost H., Zeki, AM.,"A secure audio steganography approach", International Conference for Internet Technology and Secured Transactions 2009.*
[4] *Kaliappan Gopalan, "A Unified Audio and Image Steganography by Spectrum Modification", International Conference on Industrial Technology, 2009.*
[5] *Raja K B, Chowdary C R, Venugopal K R, Patnaik L M "A Secure Image Steganography using LSB DCT and Compression Techniques on Raw Images" 2005 IEEE International conference on session B-image signal processing.*
[6] *Hossein Malekmohamadi and Shahrokh Ghaemmaghami Reduced Complexity Enhancement Of Steganalysis Of LSB-matching Image Steganography" 2009 IEEE/ ACS International conference on computer system and applications.*
[7] *Balagi R, Naveen G "Secure Data Transmission Using Video Steganography", 2011 IEEE International conference on electro/information technology (EIT).*
[8] *Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar: "Data hiding technique: Audio steganography using LSB technique", Vol. 2, Issue 3, May-Jun 2012, pp.1123-1125*
[9] *Increasing robustness of LSB audio steganography using a novel embedding method. Cvejic, N. Seppanen, T. Media Team Oulu Group, Oulu Univ., Finland.*
[10] *Arvind Kumar, Km. Pooja, Steganography- A Data Hiding Technique, Research paper , International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.*
[11] *H. B. Kekre, Archana Athawale, Swarnalata Rao, Swarnalata Rao, "Information Hiding in Audio Signals", International Journal of Computer Applications (0975 – 8887) Volume 7– No.9, October 2010*
[12] *Krishna Bhowal, Debnath Bhattacharyya, Anindya Jyoti Pal, Tai-Hoon Kim, "A GA based audio steganography with enhanced security", Springer Science, Business Media, LLC 2011.*