IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Enhanced Audio Steganography using RSA Cryptography and LSB algorithm

Prof. Pankaj Waghralkar[1], Ms. Durga Solanki[2], Ms. Sayali Shilamkar[3], Ms. Priyanka Belekar[4], Ms. Pooja Chandan[5]

Department of Information Technology Engineering, PadmabhooshanVasantdada Patil Institute of Technology, Pune, India[1, 2,3,4,5]

Abstract: Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. Audio steganography is a young branch of this discipline. An encoding mechanism is used for embedding the message into the audio file. In this paper we used the 4th Bit LSB method to do it. The quality of the audio file after encoding remains unaffected. A public key cryptographic algorithm, RSA is also used to ensure greater security

Keywords: Steganography, Audio Data Hiding, LSB Algorithm, Cryptography, RSA, EASS.

I. INTRODUCTION

The word "Steganography" comes from the Greek word “stegos” and it means "covered or secret writing", asdefined today, it is the technique of embedding information into something else for the sole purpose of hiding that information from the casual spectator. Audio Steganography describe methods to embed information into a carrier signal. In this technique audio file is sampled and then an appropriate bit of each alternate sample is altered to embed the textual information. Cryptography is one option to send message secretly. But when we convert plain text into cipher text then intruder comes to know something important message is there in cipher text and then he tries to break that cipher text. Intruders may leak the information to others manipulate it to misinterpret as well as to misrepresent an individual or organization. Steganography is one of the solutions to overcome this problem by making intruder believe that there is no useful information.

In this paper we described EASS for secure data transmission. It is useful in following sectors:

- Chemical companies.
- Military.
- Corporate industries.

This document is intended for description of existing system, proposed system and challenges in current Audio Steganography tools.

II. LITERATURE SURVEY

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods available for audio steganography. Some of them are as follows:

1. LSB Coding
2. Parity Coding
3. Phase Coding
4. Spread Spectrum

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. Figure 3 illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method.

In LSB coding, the ideal data transmission rate is 1 kbps per 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.

To extract a secret message from an LSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is smaller than the total number of samples in a sound file. One must decide then on how to choose the subset of samples that will contain the secret message and communicate that decision to the receiver. One trivial technique is to start at the beginning of the sound file and perform LSB coding until the message has been completely embedded, leaving

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

the remaining samples unchanged. This creates a security problem, however in that the first part of the sound file will have different statistical properties than the second part of the sound file that was not modified. One solution to this problem is to pad the secret message with random bits so that the length of the message is equal to the total number of samples. Yet now the embedding process ends up changing far more samples than the transmission of the secret required. This increases the probability that a would-be attacker will suspect secret communication.

III. EXISTING SYSTEM

LSB algorithm is one of the most easiest and secured algorithm in audio Steganography. By modifying the least significant of several bytes of an audio file, only minor changes occur in the original sound, most of which cannot be distinguished by the human auditory system. We make use wav files to hide the message since it can be edited and manipulated with ease relatively.

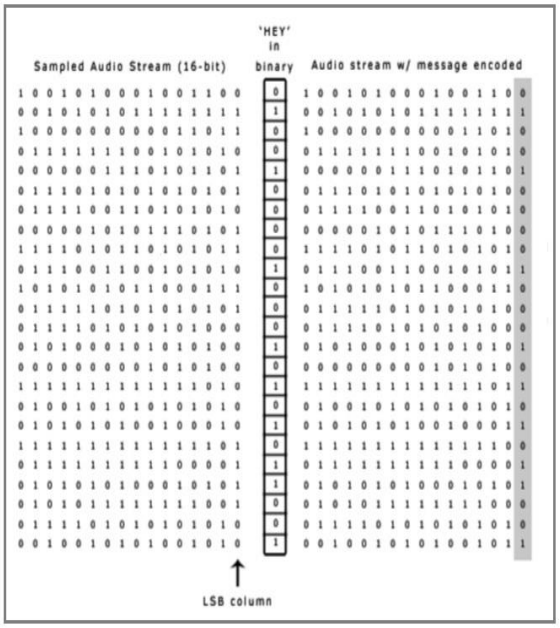

Fig.1 : Message 'Hey' Is Encoded In A 16-Bit CD Quality Sample Using The LSB Method

Wav files make use of either 8 or 16 bits to store sound information. 8 bit files allow values of sound in the range between 0 and 255 and the 16 bit files will have values from 0 to 65535. By changing the values of bytes slightly, we can store our secret data. If for example, we have 8 byte sample of wav audio: 200 234 157 141 these values would be represented in binary as:
11001000 11101010 10011101 10001101

Suppose we want to hide the binary file 1110 (14) inside this sequence. We replace the least significant bit in each byte of wave sample (the least significant bit because it will cause the least amount of change in the value) by bits of the binary form that makes up 14. The sequence of binary after modifying wav by stuffing 14 is shown below:
11001001 11101011 10011101 10001100

To increase the storage capacity another approach is to add message bits in higher LSB layers (4th and 5th LSB layer). It is shown as below,

A. Before Embedding:
Sample bits are: 00101111
Target layers are 4th and 5th and message bits are 0 and 1.
B. After Embedding:
Sample bits are: 00110111

IV. PROPOSED SYSTEM

In Proposed system, the data to be transferred is initially encrypted followed by transferring of the embedded file in audio format thus increasing security of the system. The system allows embedding large amount of data with reduction in glitches. System allows transferring of data when connected to LAN. Also system provides with secured and more efficient database storage which consists of encrypted audio files. The system architecture is as follows,

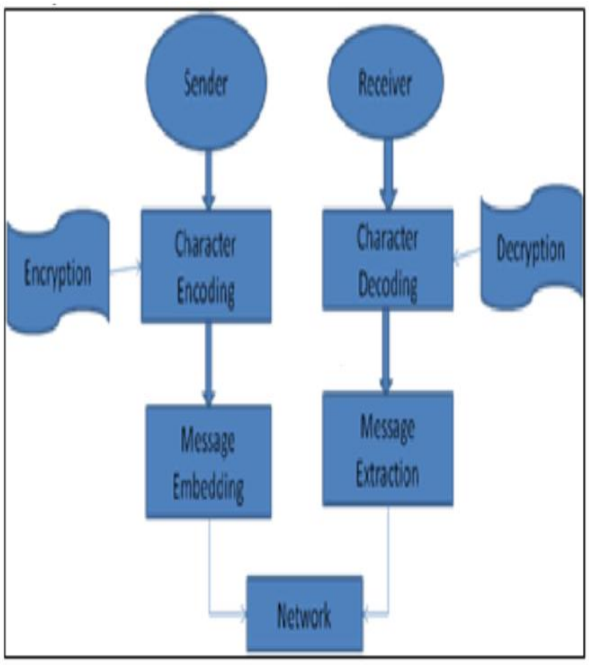

FIG. 2: System Architecture

A wav audio file is first of all divided into segments of 8 bits. Then a particular pattern is selected.
For E.g.Consider an audio segment
11001000 11101010 10011101 10001101
200 234 157 141
Message bits: 1100
And pattern is 1324

That means,
1st bit of message is stored in 1st LSB layer of 1st segment
Then first segment becomes, 11001001=201

2nd bit of message is stored in 3rd LSB layer of 2nd segment

Then second segment becomes, 11101110=238

3rd bit of message is stored in 2nd LSB layer of 3rd segment

Then third segment becomes, 10011101=157

4th bit of message is stored in 4th LSB layer of 4th segment

Then forth segment becomes, 10000101=133

As we can see that there is large difference between values of 2nd and 3rd segments before embedding and values of 2nd and 3rd segments after embedding. So to minimize this difference we have introduced an adjustment step for 3rd and 4th LSB layer.

It is shown as below, 2nd segment is, 11101110=238Now adjust remaining LSB layers in such a way that difference will get minimized after adjustment, 11101100=236 236 is more closer to 234 hence we can say that noise is reduced. Similarly, for 4th segment, 10000101=133 after adjustment, 10000111=135

V. APPLICATION

The System can be used whenever an individual wants to hide data to prevent unauthorized person from becoming aware of the existence of secret data. In the business world Audio data hiding can be used to hide a secret chemical formula or plan for a new invention. Audio data hiding can also be used in the non-commercial sector to hide information that someone wants to keep private. It can also be used in forensic applications for inserting hidden data into audio files for the authentication of spoken words and other sounds, and in the music business for the monitoring of the songs over broadcast radio.

VI. CONCLUSION

We can say that the existing system is less secured as information is not encrypted and directly embedded into audio file. While new system is more secured as we are encrypting data before embedding. As we are developing more robust and secured system it can be used in chemical companies to send chemical formulas secretly as well as in military communication. A method of embedding information in the cepstral domain of a cover audio signal is described for audio steganography applications. The proposed technique combines the commonly employed psycho acoustical masking property of the human auditory system with the decor relation property of the speech cepstrum, and achieves imperceptible embedding, large payload, and accurate data retrieval. Results of embedding using a clean and a noisy hot utterance show the embedded information is robust to additive noise and band pass filtering.

ACKNOWLEDGMENT

We would like to express our gratitude towards the professor **Prof. Pankaj Waghralkar** for his guidance, help and constant encouragement through the various difficult stages while making this paper. We are also thankful to **Prof. S.B. Madankar**, our H.O.D **Prof. N.D. Kale** and all those who directly or indirectly helped us in making this paper a reality.

REFERENCES

[1]. Padmashree G, Venugopala P S "Audio Steganography and Cryptography: Using LSB algorithm at 4th and 5th LSB Layers"IJEIT Volume 2, Issue 4,October 2012
[2]. AnuBinny, Maddulety Koilakuntla " Hiding Secret Information Using LSB Based Audio Steganography" IEEE 2014
[3]. BankarPriyanka , KatariyaVrushabh, PattiKomal "Audio Steganography using LSB" IJECSCSE ,March 2012
[4]. Varsha,DrRajendra Singh Chillar "Data Hiding using Steganography and Cryptography" IJCSMC ,April 2015
[5]. Harish Kumar, Anuradha "Enhanced LSB technique for Audio Steganography" IEEE July 2012
[6]. NedeljkoCvejic, TapioSeppänen "Increasing Robustness of LSB Audio Steganography Using a NovelEmbedding Method"IEEE
[7]. SeptimiuFabian Mare, MirceaVladutiu and Lucian Prodan "Secret data communication system using Steganography, AES and RSA." IEEE 2011.

DOI 10.17148/IJARCCE.2016.5502