ISSN 2395-1621

Efficient Data Hiding Scheme Using Audio Steganography

[#1]Ankita Navagire, [#2]Ashwini Navghare, [#3]Ayush Porwal, [#4]Jhalak Swami
[#5]Prof. Santosh Darade

[1]ankitanavagire7@gmail.com
[2]ashunavghare@gmail.com
[3]ayushporwal994@yahoo.in
[4]jhalakswami@yahoo.in
[5]darade.santosh@gmail.com

[#1234]Department of Computer Engineering
[#5]Department of Computer Engineering
SITS, Narhe, Pune.

ABSTRACT

In past few decades the data transmission is not secure because of attacks by intruder or attacker. In public communication system Data transmission is not secure because of interception and improper manipulation by eavesdropper. So Steganography is the attractive solution for this problem, which is a method of writing hidden, messages apart from the sender and receiver in such a way that no one, , suspects the existence of the message, a form of security through obscurity. Audio steganography is the scheme of hiding the data in form of secret information by concealing it into another medium such as audio file. In this paper we are dealing different types of audio stenographic methods, its future work.

Keywords: **Steganography, Audio Steganography, DES Algorithm, stego key, Bitwise operator**

ARTICLE INFO

Article History

Received: 26th October 2015

Received in revised form :

28th October 2015

Accepted: 2nd November, 2015

Published online :

3rd November 2015

I. INTRODUCTION

Steganography is the technique of encrypting a file, message, image, or video within another file, message, image, or video. The word steganography is a Greek words steganos, meaning "covered, concealed, or protected", and graphene meaning "writing". Steganography is the method of covering and hiding messages in a medium called a cipher text. Steganography is related to cryptography. The basic idea behind cryptography is that you can keep a message a secret by encoding it so that no one can read it. If a good cipher is used, it is likely that no one, not even a government entity, will be able to read it. This is where steganography comes in. The purpose of steganography is to embed a message. All steganography requires is a cipher text, which is where data will be hidden, a message that is made up of data, an algorithm that decides steps to hide the data, and a key that will be used to encrypt the file. First the data that is being passed from one person to another is encrypted (not always, but this is highly suggested). Then the information is embedded into a cipher text. This is done according to the embedding algorithm and a secret key that performs the actions of the embedding process. This process outputs a steganogram that has the information hidden inside.

Audio Steganography

Hiding the messages into digital sound is called as audio Steganography. It is a more difficult process than embedding messages in other media. Using audio steganography uses can hide the message in MP3 like sound files. The Human auditory system (HAS) has the feature to get exploited in the process of audio Steganography. Auditory perception uses critical band analysis in the inner ear where a frequency to location transformation takes place along the basilar membrane. Received sound's power spectra is not represented on a linear frequency scale but on limited frequency bands called critical bands.

II. LITERATURE SURVEY

To hide data secretly in the audio file there are few techniques introduced earlier. The lists of methods are:

- LSB Coding
- Phase Coding
- Parity Coding
- Spread Spectrum

LSB coding:

In dealing with LSB coding methodologies (LSB) least significant bit is modified to embed data. In terms of phase encoding scheme the part of carrier file is to be replaced with the reference phase which represents hidden data. The signals are divided into regions in parity coding, then parity

bit of each region calculated and compared with secret message bit. Depending on the result encoding is done.

Phase coding

The source sound signal (C) is segmented to get the header. The remaining part is to be broken up into smaller segments which have lengths equal to the size of the message to be encoded. A (DFT) Discrete Fourier Transform is used for each segment to create a matrix of the phases. The embedded message is inserted in the phase vector of the initial signal segment as follows:

$$phase\_new = \begin{cases} \pi/2 & if \quad message \quad bit = 0 \\ -\pi/2 & if \quad message \quad bit = 1 \end{cases}$$

Cons with this phase coding are a low data transmission rate because of which the secret message is encoded in the first signal segment only and to get the secret message from the sound file, the receiver must know the segment length.

Spread spectrum

The formal (SS) spread spectrum is a technique to spread secret message across the frequency spectrum of the audio signal. The (SS) Spread Spectrum technique expands the secret message over the frequency spectrum of the audio file. As the outcome, the final signal takes a bandwidth which is more than what is actually required for transmission. Anyhow, the (SS) Spread Spectrum technique has one main con that it can introduce noise into a audio file. In (SS) spread spectrum technique secret message is expand over the audio signal's frequency spectrum as much as possible.

Name	Content	Advantage	Disadvantage
A survey on performance analysis of DES, AES and RSA Algorithm along with LSB techniques.	Merging of cryptography and steganography to secure data while transmitting in network.	AES algorithm is more secure than others and less time consuming.	Sometimes the audio files may get corrupted.
Review of an Improved Audio Steganographic methods over LSB through Random Based Approach.	Basic concepts of audio steganography and how to improve it.	System will not alter the size of the file even after encoding and also suitable for any type of audio file format.	Algorithms used in LSB insertion method are easily decrypted.

III. FIGURES

Consider Steganography is the method of embedding the fact that communication is taking place, by hiding information in other file.

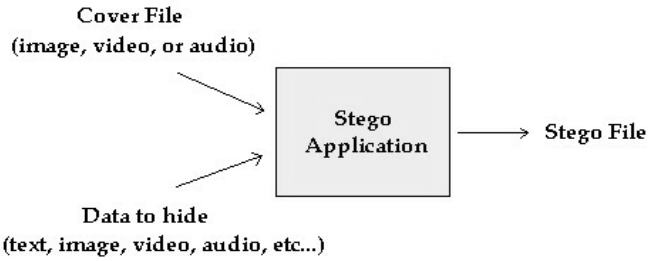

Fig 1. Steganography Application Scenario

The use of steganography application is to hide the different types of data within a cover file. The resulting stego applications do contain the hidden information, although it is virtually identical to the cover file.

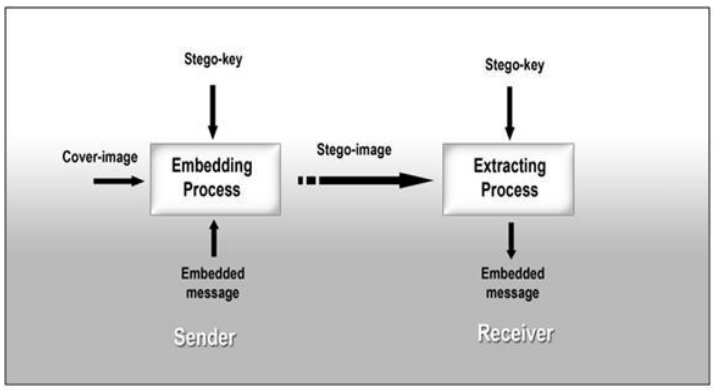

Fig 2. Block diagram for audio Steganography

This figure shows the block diagram of audio steganography. The objective is to send messages from sender toward the receiver. The sender sends the data in encrypted format. And at the receiver side receiver do the decryption of that message to achieve the original message. That message is embedded in audio. For that we had used DES (Data Encryption System) algorithm. Considering the privacy issues we are provided one public key. To the sender side and the receiver side that key is STEGO KEY. Fig. 2 represents the block diagram of a secure steganographic system. Source messages can be images, texts, video, etc. The parts of steganography system are:

Emb: The data to be embedded.

Cover: The file in which data will be embedded.

Stego: A renewed version of cover that contains the embedded message.

Key: Secret data which is required for the embedding and getting the original data and must be known to both, the sender and the receiver.

fE: A stenographic function which contains cover, emb and key as parameters and produces stego as output

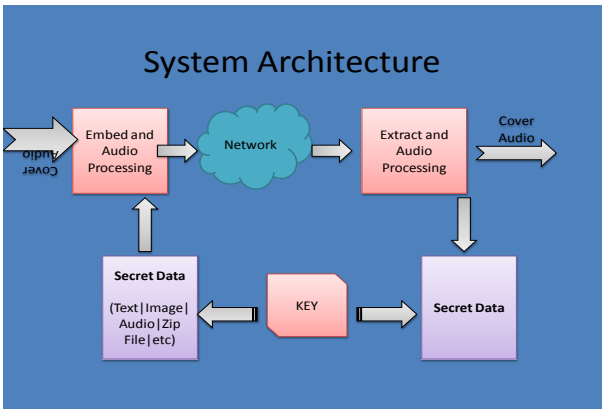

Fig 3: System Architecture of audio steganography

Working Flow of the System:

1) Firstly take an audio file and perform sampling on it.

2) Input will be the message file which we want to send. Then encrypt it using the DES (Digital Encryption Standard) algorithm by the use of public key.

3) After the encryption we will embed the encrypted data in an audio file with the help of DES algorithm.

4) After this a stego audio file is transmitted to the receiver. Here we provide stego key used for the privacy and security of data.

5) Stego key will lead the decryption which will be performed by the receiver to get the original message.

DES (Digital Encryption Standard):

1) DES is used to do Encryption and decryption of data in 64-bit block of cipher text.
2) DES has 16 rounds, means the algorithm is repeated 16 times to get the cipher text
3) It has been observed that the number of rounds is proportionally exponential to the amount of time required to find a key.
4) If the number of rounds increases, the security of the algorithm will increase exponentially
5) This project "DES (Digital Encryption Standard)" is based on client server technology
6) The sender will send the encrypted file using internet connection. On the other side the receiver will receive the file and decrypts the file by using the same private key used by the sender.

More security = **Bitwise operator:**
1) Shift the bits slightly (>> and << bitwise operators) as determined by characters in the key

2) Sorts out the problem of having an odd or even number of bits

3) Takes the byte[] array as encrypted message, and divide it in two halves around i.e. a b c d e f would become d e f a b c

4) If a long key is to be used then only some of the Key is right, then first part of cipher text will still be decrypted.

5) Shuffles the file Bytes in the blocks of key.length(). This method is powerful and good for encryption. The problem is contradiction with the fact, that sometimes, when a short text-file is encrypted, some of the 'central' text is still partially scrambled.

6) The keyStream() function accepts the user key and Make it large up to (key.length()*key.length() + key.length())*128,This will surely improve the security issues.

IV. EXISTING SYSTEM

1. In present system, the user sends data from one system to the desired system in Local Area Network.

2. Because of the security issues not only authorized persons but also unauthorized persons can view the data. Here we will discuss the cons of the previous techniques and in what way they are different with present method. There are mainly two cons associated of methods like parity coding. The human ear is very delicate and may detect the small noise which is introduced in an audio file, though the parity coding method is somewhat closer to make the introduced noise inaudible. Another con is robustness. One issue which is associated with phase coding is a low data transmission rate because of the fact that the hidden message is encoded in the first segment of signal. Phase coding method is often used when small amount of data needs to be transmitted.

Least significant bit (LSB) coding is the simplest technique to hide the data in an audio file. By substituting the LSB of each sampling point with a binary message, LSB coding ensures for a large amount of data to be encoded and to be transmitted.

V. PROPOSED SYSTEM

This system will do the analysis and encrypt the secret message in cover media with the help of efficient algorithm.

System we will be using input and output buffer for encrypting and decrypting our information.

This system will provide a good and a efficient method for embedding the data from attackers and sent safely to its destination. This proposed system will not make the change in the size of the file after encoding of data in an audio file. Encryption and Decryption techniques are used to make the security in data transmission.

VI. CONCLUSION

In this paper we have are providing a method of impossible to see an audio data hiding. This system is supposed to provide an efficient method for embedding and hiding the data from attackers and send safely to its destination. This system will not alter the size of the file even after encoding of data in an audio file. Thus we infer that audio data hiding techniques can be utilized for a number of tasks other than communication data and its storage.. Human is now pushing away its own boundaries to make every condition possible. Similarly these techniques described above can be further altered as it is in the world of Information Technology.

VII. FUTURE SCOPE

The future work of this project is to restrict the unauthorised access and provide better privacy as well as security during data transmission. The formal approach of DES (Digital Encryption Standard) is to send the scrambled data in encrypted from via internet connection. The proposed approach finds the suitable algorithm for embedding the data in audio or video file using steganography which provides the better security pattern for sending messages through a network.

REFERENCE

[1] Michel Kulhandjian, Dimitris Pados, "Extracting Spread-Spectrum Hidden Data from Digital media", IEEE transactions on information forensics and security VOL: 8 NO: 7 (Year: 2013).

[2] B. Padmavathi, S. Ranjitha Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique". (January, 2013).

[3] Bhagyashri Patil, Vrishali Chakkarwar, "Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach" IOSR Journal (ISOR-JCE), VOL: 9 Issues 1. (April, 2013).

[4] Fahimeh Rezaei,Tao Ma et.l, "An anti-steganographic approach for removing secret information in digital audio data hidden by SS methods" IEEE transaction on system security symposium. (Year: 2013).

