Journal of Theoretical and Applied Information Technology

www.jatit.org

EFFICIENT METHOD OF AUDIO STEGANOGRAPHY BY MODIFIED LSB ALGORITHM AND STRONG ENCRYPTION KEY WITH ENHANCED SECURITY

[1]R SRIDEVI, [2]DR. A DAMODARAM, [3]DR. SVL.NARASIMHAM
[1]Assoc. Prof., Department of Computer Science and Engineering, JNTUCEH, Hyderabad
[2]Prof., Department of Computer Science and Engineering, JNTUCEH, Hyderabad
[3]Prof., School of Information Technology, JNTUH, Hyderabad

E-mail: sridevirangu@yahoo.com, damadorama@gmail.com, svlnarasimham@jntuh.ac.in

ABSTRACT

In the current internet community, secure data transfer is limited due to its attack made on data communication. So more robust methods are chosen so that they ensure secured data transfer. One of the solutions which came to the rescue is the audio Steganography. But existing audio steganographic systems have poor interface, very low level implementation, difficult to understand and valid only for certain audio formats with restricted message size.

Enhanced Audio Steganography (EAS) is one proposed system which is based on audio Steganography and cryptography, ensures secure data transfer between the source and destination. EAS uses most powerful encryption algorithm in the first level of security, which is very complex to break. In the second level it uses a more powerful modified LSB (Least Significant Bit) Algorithm to encode the message into audio. It performs bit level manipulation to encode the message.

The basic idea behind this paper is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safer manner. Though it is well modulated software it has been limited to certain restrictions. The quality of sound depends on the size of the audio which the user selects and length of the message. Though it shows bit level deviations in the frequency chart, as a whole the change in the audio cannot be determined.

Keywords: *Stegenography, LSB Method*

1. INTRODUCTION

Steganography is the practice of hiding information "in plain sight". This technique relies on a message being encoded and hidden in a transport layer in such a way as to make the existence of the message unknown to an observer. Importantly, the transport layer - the carrier file - is not secret and can therefore be viewed by observers from whom the secret message itself should be concealed. The power of steganography is in hiding the secret message by obscurity, hiding its existence in a non-secret file. In that sense, steganography is different from cryptography, which involves making the content of the secret message unreadable while not preventing non-intended observers from learning about its existence1.Because the success of the technique depends entirely on the ability to hide the message such that an observer would not suspect it is there at all, the greatest effort must go into ensuring that the message is invisible unless one knows what to look for. The way in which this is done will differ for the specific media that are used to hide the information. In each case, the value of a steganographic approach can be measured by how much information can be concealed in a carrier before it becomes detectable, each technique can thus be thought of in terms of its capacity for information hiding.

There are numerous methods used to hide information inside of Picture, Audio and Video files. The two most common methods are **LSB (Least Significant Byte)** and **Injection.**

2.EXISTING SYSTEM:

The existing system of Audio Steganography poses more restrictions on the choosing of audio files. User can select only wav files to encode. It supports water marking method to encode .It complexity arises when more message to be encoded. The message length is restricted to 500 characters. It doesn't shows the variations occurred after encoding the message. The LSB algorithm in the existing system is not efficient because it hides the message in consecutive bytes received from audio files.

The disadvantages of existing system is

- Selection of audio formats is restricted to one.
- Non-Provision of encryption key
- Length of the message is limited to 500.
- Absence of frequency chart to show the variations.
- Lack in good user interface.
- Consume much time to encode and decode.
- Non-Provision of sending the file to the destination.
- User needs to understand better to know the operations.

These are the disadvantages in the existing system which can be overcome by the proposed system.

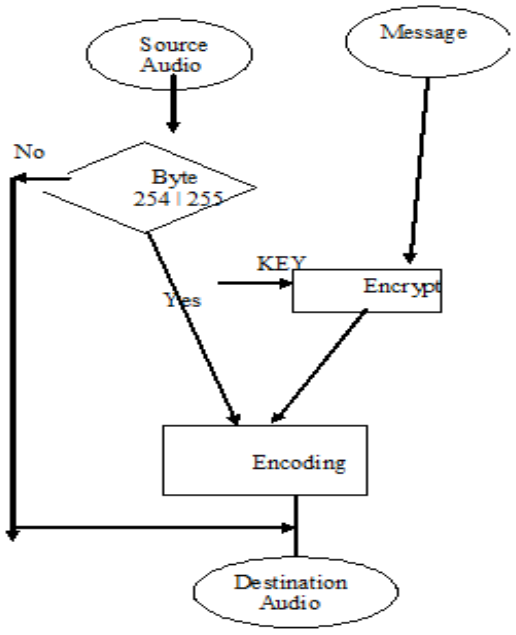
3.PROPOSED SYSTEM:

Enhanced Audio Steganography is a method of hiding the message in the audio file of any formats. EAS provides an easy way of implementation of mechanisms when compared with audio steganography. Apart from the encoding and decoding in Audio steganography, EAS contain extra layers of encryption and decryption. The four layers in EAS are:

- Encoding
- Decoding
- Encryption
- Decryption

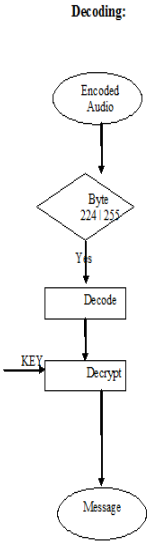
- **Encoding** is a process of hiding the message in the audio.

Figure:Encoding



- **Decoding** is a process of retrieving the message from the audio.

Figure:Decoding



Modified LSB(Least Significant Bit) Algorithm is used to encode the message into audio. 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.

Powerful encryption algorithm is used to encrypt the message before encoding for further security purpose. The following steps is used to encrypt the message

a. Adding all ASCII values of characters in the key given by user.

b. Converting the sum into bit pattern

c. Performing logical operation to the bit pattern.

d. Adding to the encoded character.

For more security enhancement the encoding is done only when the byte which is received from the audio is 254 or 255.This selection of particular bytes for encoding will reduce the lack in quality of audio after encoding. It can be proved by seeing the frequency chart indicating the deviations happened after encode. Thought it shows bit level deviations in the chart as a whole the change in the audio cannot be determined.

3.1 Basic idea of EAS:

The basic idea behind this is to provide a good, efficient method for hiding the data from hackers and sent to the destination in safe manner. Though it is well modulated software it has been limited to certain restrictions. The quality of sound depends on the size of the audio which the user selects and length of the message.

The main two features of this system are

1) Size of file is not changed after encoding.

2) Since it is bit level manipulation the sound variations cannot be determined by any current software.

The proposed system over comes all the restrictions made on the existing systems. It provides good looking environment to user .It also provide the user to give secret key for encryption. The length of message is more than the existing system, and provides frequency chart to see the variations after encoding. The quality of the audio doesn't change variably. It cannot detect the lack in quality of sound. The encryption key can be any combination of characters, symbols, numbers. The key which is used for encoding is also used for decoding .This is a secret key where the both user have to agree upon a single common key.

3.2 The advantages of proposed system is

- Different Audio formats are supported by the system.
- Provision of encryption key and performs simple encryption algorithm.
- The encryption key is modified by a strong algorithm to get a new key, which is used to encrypt the message. So even if the key is known for an intruder, he cannot break the code with that key.
- Presence of frequency chart to show the variations that helps the user to determine.
- Consumption of time to encode and decode is reduced.
- Provision of sending the file to the destination is given so that after encoding the user can send the file by giving destination IP address.

3.3 Encoding:

The audio file contains set of bytes. For e.g. take an audio file which play for 10 secs. It has more than 60,000 bytes. Each byte is received and checked if the received byte is 254 or 255.If it is byte 255 or 254, encoding is done.

So for one character to encode we need eight 254 or 255 bytes. One character is hidden in consecutive eight 254 or 255 bytes.In order to mark the end of message, the LSB bit of next eight consecutive 254 or 255 bytes which comes after all the messages have encoded are replaced by 1.Before encoding, message is encrypted using public key.

3.4 Decoding:

The encoded file is decoded to get the message .The message is decoded first and then decrypted by the public key. The eight consecutive 254 or 255 bytes are taken and decrypted with the public key. This decrypted byte have value less than 128.So if the value is 255 after decrypted then it is said to be end of message.

3.5 Encryption:

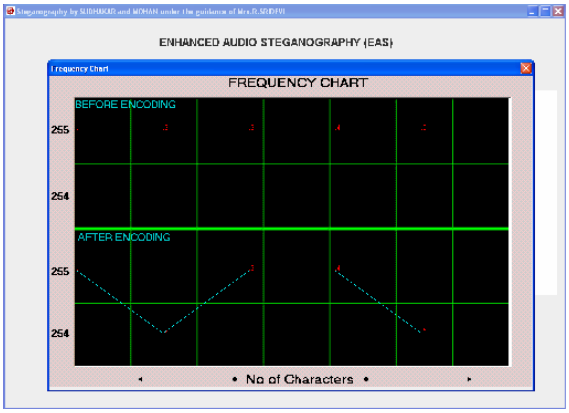
The user allowed entering the public key/shared key in any combination of numbers, symbols and characters. The key contains set of characters. All characters are converted to ASCII value and add all the ASCII value to get single number. And that single number is converted to bit pattern and by simple logical operation (XOR) you can get a single number less than 128.It is a new private key .It is added to the characters one by one in the message, before encoding.

3.6 Decryption :

The LSB bits of consecutive eight 254 or 255 bytes are taken and subtracted with the key to get the original character.

4.FREQUENCY CHART: The input audio file and the new encoded audio file can be compared using the frequency chart diagrams.The comparison is done using the chart button which is present in the EAS interface.

One of the sample outputs is shown below:



5. CONCLUSION

This proposed system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This proposed system will not change the size of the file even after encoding and also suitable for any type of audio file format. Encryption and Decryption techniques have been used to make the security system robust.

6.FUTURE ENHANCEMENTS

Though it is well modulated system, it has been limited to certain restrictions. The quality of sound depends on the size of the audio which the user selects and length of the message. The quality of the sound in the encoded audio file can be increased. There are number of ways that this project could be extended. Its performance can be upgraded to higher levels in practical conditions. There are also other weighting algorithms like spread spectrum, echo data hiding etc., and those can be implemented. Instead of having common secret key to encode and decode, a public–private key pairs will be introduced.

REFERENCES

[1]. F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding—A Survey," *Proc. IEEE*, vol. 87, no. 7,1999, pp. 1062–1078.

[2]. Increasing robustness of LSB audio steganography using a novel embedding method.Cvejic, N. Seppanen, T. MediaTeam Oulu Group, Oulu Univ., Finland.

[3]. [Anderson and Petit colas 2001] Anderson, R., Petitcolas, F.: On the limits of the steganography, IEEE Journal Selected Areas in Communications, 16, 4,474-481.

[4]. Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International **Conference on Publication Date: 5-7 April 2004 [ISBN:0-7695-2108-8]**

[5]. Audio Engineering Society E-Library - Steganographic Approach to Copyright Protection of Audio; Preprint Number: 7067 Convention: 122 (May 2007)

[6]. Author: Kumar, Suthikshn

Websites Refered :

- http://www.w3schools.com
- http://java.sun.com
- http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=1286709&isnumber=28683
- http://www.aes.org/e-lib/browse.cfm?elib=14052