Three Layered Model for Audio Steganography for Secured Data Transfer

Anjaliraj
P.G. Scholar,ECE Department
KMEA Engineering College
Ernakulam, Kerala

Dhanya. G
Assistant Professor , ECE Department
KMEA Engineering College
Ernakulam, Kerala

***Abstract*— Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdroppers. A technique for secure transmission of messages called Steganography, which send the messages in such a way that existence of the message is concealed. Audio Steganography is the scheme of hiding the existence of secret information by concealing it into an audio file. In this paper ,a novel technique which uses audio file as carrier to hide the secret information following Three Layered Model. The goal of this paper is to achieve highly secure data transmission to ensure confidentiality. The three Layers for increasing the security are : Encoding , Double Encryption and Embedding using Enhanced LSB Modification Technique. Two powerful algorithms are fused to double the level of Security. The data is embedded up to 3 LSBs. The roposed technique has been tested successfully on different .wav files. A performance analysis is carried out based on the parameters including Capacity, Transparency and Robustness.**

Keywords- Audio Steganography , Cover file, Stego file, key,Secret Transmission, LSB Steganography, HAS

I. INTRODUCTION

Due to the widespread use of public networks, the use of the internet has gained popularity whole over the world. There is a abundant variety of public and private data which is being transferred widely over internet which has stipulated the attention of various researchers to ensure security of various digital data. Data Hiding is most essential for Network Security issue. Sending sensitive messages and files over the Internet are transmitted in an unsecured form but everyone hasgot something to keep in secret.

Currently there are two methods of information hiding which includes cryptography and steganography . Steganography and Cryptography are the two popular approaches for secure and undetectable .In Steganography, the very existence ofmessage is hidden by embedding it in a cover media where as Cryptography protects the content of message .Steganography is different to cryptography in the way that steganography conceals the existence of message while cryptography conceals the meaning of message. Depending on the nature of cover object, Steganography[5] can be categorized into five types:Text Steganography, Image Steganography, Audio Steganography, Video Steganography. Audio and videofiles are considered to be excellent carriers for the purpose of steganography due to presence of redundancy [2].Audio steganography requires a text or audio secret message to be embedded within a cover audio message. Due to availability of redundancy, the cover audio message before steganography and stego message after steganography remains same. However, audio steganography is considered more difficult than image/video steganography because the Human Auditory System (HAS) is more sensitive than Human Visual System (HVS) [3]. To perform audio steganography successfully, the adopted technique should work against HAS.

For any audio steganography technique to be implementable, it needs to satisfy three conditions; capacity, transparency and robustness [4]. Capacity is the amount of secret information that can be embedded within the host message while transparency means how well the secret message is embedded in the stego message. Robustness of a technique indicates the ability of embedded secret message to withstand attacks.

Steganalysis is the process of detecting secret message hidden through steganography [5]. Two commonly used steganalysis techniques are auditory inspection and statistical analysis. In auditory inspection,one can detect the presence of secret message through HAS. In statistical analysis, the intruder compares the original host message and modified host message to extract the secret message.

The objective of this paper is to come up with a technique hiding the presence of secret message and working against steganalysis . For this purpose, the technique needs to satisfy transparency. Apart from this,capacity is also a major concern because an efficient technique is one which can embed more secret information. To increase robustness, the steganographytechnique could be backed by double encryption .

In a computer-based audio steganography system, secret messages are embedded in digital sound file. The secret message is embedded by slightly altering the binary sequence of the sound file. Existing audio steganography software can
embed messages in WAV, AU, and even MP3 sound files [3]. Embedding secret messages in digital sound is usually amore difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced.

A recent breakthrough in this field is hiding information in Audio files. The embedded data should be as immune as possible to modifications from intelligent attacks . Thus the hidden messages are encrypted before hiding behind Audio files. This system hides encrypted information in Audio files. Th[e text to be embedded is first encrypted and then embedded into the Audio file to allow maximum performance and robustness. This allows the users to carry data easily and securely .

The major task of the Audio Steganography is to provide the user the flexibility of passing the information implementing the encryption standards as per the specification and algorithms proposed and store the information in a form that is undetectable. This system has a reversal process, which is used to retrieve the data from Audio file and decrypt the data to its original format upon the proper request by the users.

II. RELATED WORKS

Relevant work has been done on Audio Steganography. Many have designed system which increase the capacity of the steganography approach and few has increased security. The most easy and commonly used algorithm for any steganographic application is LSB(Least Significant Bit) it has been used by many designers and in many applications.

In LSB modification method, one or multiple bit(s) in samples of a cover message is/are replaced with bit(s) of the secret message [4]. However, conventionally single bit is being used, the enhancements in the technique have proved that changing more than one bit in a sample has no differentiable change in the properties of the host message [2]. This increases the capacity of the technique but might also increase the amount of noise in the stego message [7].

The Enhanced Least Signi_cant Bit Modification Technique includes Bit Selection and Sample Selection Mapping. The first way is to randomize bit number of Cover message called bit selection Sampling for embedding secret message while the second way is to randomize sample number called sample selection containing next secret message bit.[1] Two novel approaches of LSBs of audio samples for information hiding using multiple LSB steganography [5].

A new steganographic Technique for embedding textual information in .wav file[6]. Steganography along with cryptography will result in more Security to data. Any alphabet and number can be represented by using the last 4 bits and adding either 1 or 0 at the first position.

III .PROPOSED SYSTEM

A novel approach to provide a good, well-organised method for hiding data by passing through a three layered model and sent to the destination in safer manner. The proposed technique consists of three different layers Character
Encoding, Double Encryption and Enhanced Steganography.

The Character Encoding is to convert characters into bits and bits to characters in reverse operation. Huffman Coding is used herefor encoding and decoding purposes. A code word is assigned to each possible characters in the message. The main advantage of using Huffman coding is that it will provide high compression ratio.

The character Encoding is followed by a double encryption in which two encryption algorithms are fused together. The encryption algorithms used here is RC4 and AES-256. The encoded message is first passed through RC4 _Algorithm and the encrypted text from RC4 is input to AES algorithm having 256 bit keylength.AES is still unbreakable and secret message is protected.

The final stage is the Enhanced LSB Modi_cation Technique in Audio Steganography. The encrypted text is then embedded into an audio file of .wav format. The embedding is carried out using Bit Selection sampling and Sample Selection sampling. The audio file embedded with secret message is
then sent to the destination.

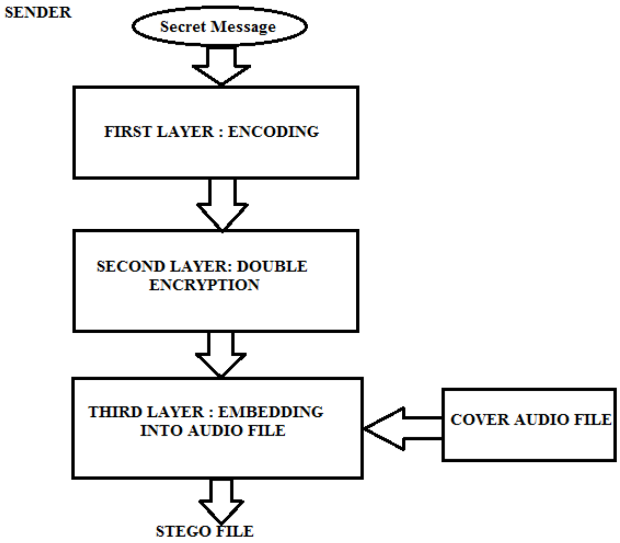

SENDER
Secret Message
FIRST LAYER : ENCODING
SECOND LAYER: DOUBLE ENCRYPTION
THIRD LAYER : EMBEDDING INTO AUDIO FILE
COVER AUDIO FILE
STEGO FILE

Fig1: Three Layered Model at Sender Side

At the receiver side the secret message is retrieved from the audio file by performing the reverse operations. The message from audio file is first extracted and it is decrypted first using AES Decryption algorithm and again the result is decrypted using RC4 Algorithm. Thus there are two passwords one for AES and one for RC4. The receiver can decrypt only if the password entered is matched with that of sender. Finally the message is decoded using Huffman decoding and the secret message is retrieved.

The process starts with entering the secret message to be sent. The Message is then encoded using Huffman Coding which results in increasing the compression ratio thus increases the capacity. The encoded file is then encrypted if the password rendered is entered. If the password is not entered, it will not go to the second stage. If the password entered is correct, the
result is RC4 encrypted text .The RC4 encrypted text is again encrypted using AES-256 algorithm only if the password entered. Finally we will select a cover audio signal in .wav format to which data has to be hided. Then Data embedding is proceeded using LSB modification technique . The final output of it is the stego file in which the secret message is embedded without any detectable difference.

A. Algorithm for Embedding Data into Audio file at the Sender Side:

- Step 1: Enter the secret message.
- Step 2: Encode the text using Huffman Coding
- Step 3: Encrypt the encoded file using RC4 Algorithm.

- Step 4:Again Encrypt the encrypted file using RC4 Algorithm using AES-256 Algorithm
- Step 5: Select the Audio file for embedding the secret message.
- Step 6: Embed the encrypted message into the Audio file using Enhanced LSB Modification Technique.
- Step 7: Play the audio file so that it sounds clear to the end user.

The stego file is received at the Receiver side and the secret message is retrieved step by step. The reverse process of embedding is carried out for retrieval of message. The encrypted data will decrypt only if th e password matches with that of sender side. If the password is correct the AES data is decrypted and to decrypt the RC4 encrypted text second password should also match.Finally Huffman decoding is performed and the secret message is retrived at the receiver side.

B. *Algorithm for Extracting the Embedded text from Audio file at the Receiver Side:*

- Step 1: Select the Embedded Audio file for extracting the secret message.
- Step 2: Extract the secret message from Audio file using the inverse LSB Modification.
- Step 3: Decrypt the secret message using AES-256 Algorithm.
- Step 4: Decrypt the secret message using RC4 Algorithm.
- Step 5: Decode the secret message using Huffman Decoding.
- Step 6: Display the secret message to the end user.

For any audio steganography technique to be successful, it need to satisfy three conditions Capacity, Transparency and Robustness. Capacity is the amount of secret information that can be successfully embedded in the host message.I is the number of embedded bits within a unit of time (bps). Robustness is the ability of the stego message to withstand steganalysis and attacks by intruders. In this system the robustness is very high because of two level encryption. Transparency is simply the inaudibility of distortion. Since Human Auditory system(HAS) is more sensitive than Human Visual System, any detectable change in the audio will be more sensitive.

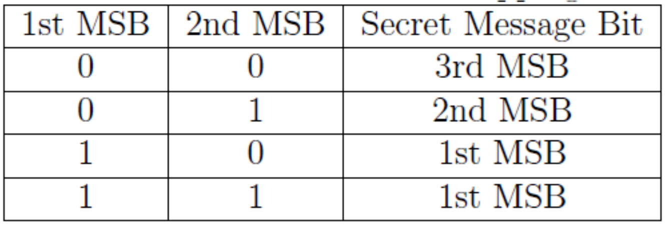
C. *Enhanced LSB Modification Technique*

The LSB modification is one of the simplest audio steganography technique and it provides high capacity . In this technique, data is being hidden in least significant bit(s) of audio samples. The weight of LSBs in comparison with the combined weightage of whole sample is very small.

Bit Selection Mapping and Sample Selection Mapping is used in Enhanced LSB Modification Technique. Inorder to confuse the intruder, same bit of a sample is never used to embed the secret message in the audio file. Randomness is produced by selecting a different bit for embedding in every sample to hide secret message. First two Most Significant Bits (MSBs) of a sample will decide which bit of the same sample would contain the secret message bit.

Table I shows Bit Selection mapping using two MSBs. Different Bit Selection mappings can be designed but the secret message bit should always be embedded only in first three LSBs of a sample. If the first two MSBs of a sample are equal to 00, then the third LSB will be replaced with secret message bit. If the first two MSBs are equal to 01, then the second LSB will be replaced and if the first two MSBs are either 10 or 11, then the first LSB will be replaced with the secret message bit.

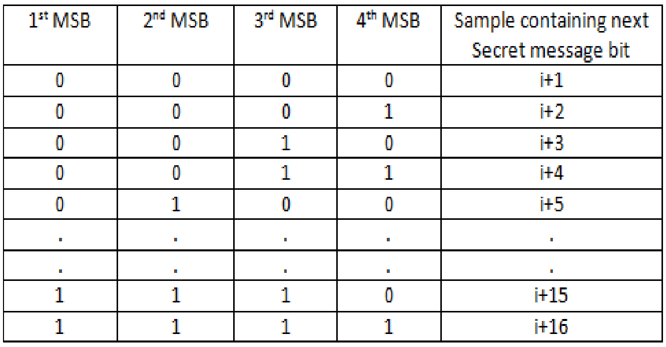
Table I – Bit Selection Mapping



1st MSB	2nd MSB	Secret Message Bit
0	0	3rd MSB
0	1	2nd MSB
1	0	1st MSB
1	1	1st MSB

Sample Selection is another way to confuse the intruder is to add some more randomness in secret message embedding by using selective sample numbers from a look up table to hide secret message. Samples are selected randomly to contain the secret message. This means all the samples will not contain the secret message bit but only a few. Consecutive samples of the cover message does not contain the secret message bits. This randomness will be controlled by the first four MSBs of the samples. Table II shows a possible Sample Selection mapping. Different Sample Selection mappings can be designed but skipping more number of samples will decrease the capacity.

Table II : Sample Selection Mapping



1st MSB	2nd MSB	3rd MSB	4th MSB	Sample containing next Secret message bit
0	0	0	0	i+1
0	0	0	1	i+2
0	0	1	0	i+3
0	0	1	1	i+4
0	1	0	0	i+5
.	.	.	.	.
.	.	.	.	.
1	1	1	0	i+15
1	1	1	1	i+16

IV . RESULTS & DISCUSSIONS

The three layered model for Audio Steganography has been designed and run successfully.The secret message is embedded into audio file and retrieved successfully without any difference between the host signal and stego signal. The proposed system is simulated using different audio files and a comparative study on the basis of Capacity, PSNR, and MSE is carried out.The three parameters of audio steganographiy technique Capacity, Transparency and Robustness is found out inorder to perform a performance analysis of the threelayere model. Capacity can be determined by measuring the minimum number of cover audio samples required to embed the secret message.Transparency and robustness can be measured in terms of Mean Squared Error (MSE) and Peak Signal to-Noise Ratio(PSNR).

$$MSE = \frac{1}{N}\Sigma_{n=0}^{N-1}((x[n] - x[n]))^2$$

$$PSNR = 10log\frac{(2^s-1)^2}{MSE}$$

where ‘S’ is the number of bits in one sample.

The size of the audio file is 1.01 MB before embedding. The size of audio file remains the same after embedding also. Thus the audio steganography is successful as there is anu detectable or audible difference between the original _le and Stego file. The cover message sample for embedding secret message is shown in Fig 2.The stego message containing the secret message after 3 layered model is shown in Fig 4.

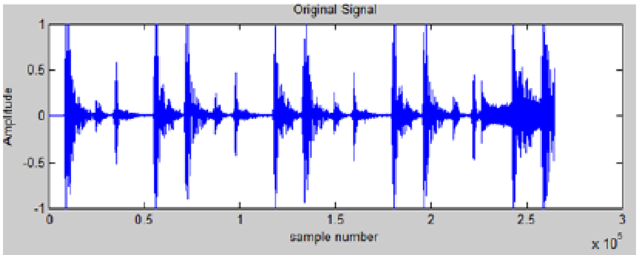


Fig.3- Cover Audio Signal.

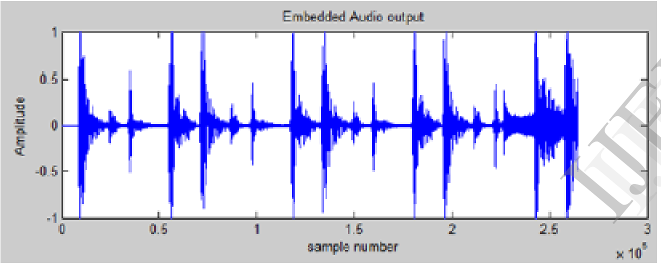


Fig.4 –Audio signal after Steganography

A comparative study of PSNR and MSE is carried out in an audio sample by varying the length of the secret message. From the experiment carried out , I found out that only secret message up to 32 characters can be sent successfully through this three layered model of Audio Steganography. The size of the audio file is 1.01 MB before embedding. The size of audio file remains the same after embedding also. Thus the audio steganography is successful as there is anu detectable or audible difference between the original file and Stego file. But there is slight variation in the MSE and PSNR as the length of secret message bits increases. The secret message is input with different number of bits . Binary sequences of 1100 ,1010 ,11110000 are tested with variable lengths.

Table III : Performance Analysis of MSE & PSNR

Secret Message Bits	PSNR	MSE
16	222.5452	4.8889 E-007
40	222.1197	5.1344 E-007
80	222.2969	5.0307 E-007
96	221.8941	5.0307 E-007
128	222.2372	5.0655 E-007
160	221.6275	5.3687 E-007
256	221.7321	5.4337 E-007

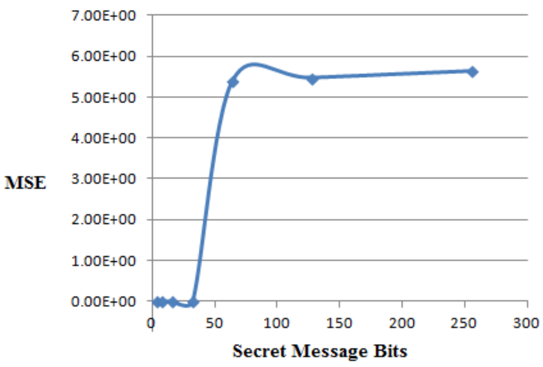


Fig.5 – Plot of Comparison of MSE

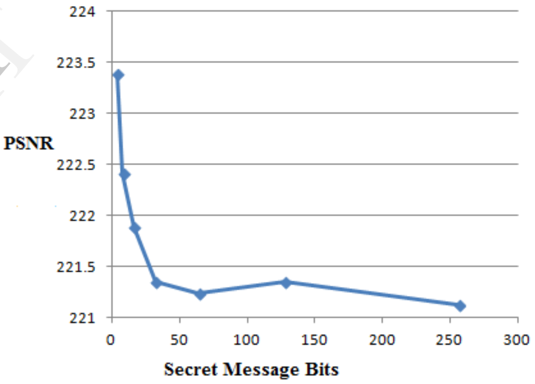


Fig.6 – Plot of Comparison of PSNR

As the number of characters increases , there is a slight increase in the MSE. But there is no gradual increase or decrease in PSNR. Only very small variations are noted in case of PSNR.The Value of PSNR should be high for perfect reconstruction of data. On the other hand , the Mean Square Error should be a small value.

V.CONCLUSION

A new three layered model for audio steganography with double encryption is presented in this paper. As steganography becomes more widely used now a days in computing ,there are some issues to resolve. In case of Audio Steganography , the main challenge is the perceptual quality of the stego audio File which is satisfied. The objective of this paper meet all the requirements in hiding the message and presence of secret message and working against steganalysis is satisfied completely. The system satisfied all the requirements such as capacity,security and robustness for secure data transmission.

REFERENCES

[1] Muhammad Asad, Junaid Gilani, Adnan Khalid, "Three Layered Model for Audio Steganography,*International Conference on Acoustics, Speech, and SignalProcessing*, 2012

[2] B.Geethavani, E.V. Prasad, "A New Approach for Secure Data Transfer in Audio Signals Using DWT",*International journal of Network Security and its Applications (IJNSA), Vol.2*,No.1,pp 43-55, Jan 2013

[3] 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, Pages: 143 - 147.

[4] Muhammad Asad, "Text Steganography Using Huffman Coding",*International Conference on* Intelligent and Information Technology 2010, Volume: 1, Pages: 445 - 447.

[5] Walter Bender, Daniel Gruhl, Norishige Morimoto,"Techniques for Data Hiding", *IBM Systems Journal*, Volume: 35,Pages: 313 - 336.

[6] B.Geethavani, E.V.Prasad, R.Roopa, "A New Approach for Secure Data Transfer in Audio Signals Using DWT", *International journal of Network Security and its Applications (IJNSA)*, Vol.2, No.1,pp 43-55, Jan 2013

[7] Vipul Sharma, Sunny Kuma, "A New Approach to Hide Text in Image Using Steganography"-*IJARCSSE-ISSN*: 2277 128X, Volume 3, Issue 4,April,2013.