Enhanced LSB Based Audio Steganography

Prof.Dighe Mohit
Computer Department
SCSCOE, Rahuri.
Ahmednagar, India
dighe.mohit@gmail.com

Miss. Kavade Priyanka
Computer Department
SCSCOE, Rahuri.
Ahmednagar, India
kavade.priyanka@gmail.com

Mr. Raje Lakhan
Computer Department
SCSCOE, Rahuri.
Ahmednagar, India
lakhan2030@gmail.com

Miss.Harale prajakta
Computer Department
SCSCOE, Rahuri.
Ahmednagar, India
harale.prajakta15@gmail.com

Mr. Dubhalkar Eknath
Computer Department
SCSCOE, Rahuri.
Ahmednagar, India
eknath2690@gmail.com

Mr. Shelar Keshav
Computer Department
SCSCOE, Rahuri.
Ahmednagar, India
kss.sonu@gmail.com

***Abstract*— In day to day life information security has become very important phenomenon of our life. Hiding a information is an essential part information security. Due to hackers data transmission in public communication system is not secure. So the most powerful solution for this problem is an audio steganography. Existing systems have low implementation power, poor interface, it was not easy to understand and it has restricted message size. We implement "Enhanced LSB Based Audio Steganography" system which ensures secure data transfer between the source and destination. Encryption and Decryption technique are use in our system which is very complex to break. LSB coding is one of the earliest techniques of hiding the information in audio. Our paper mainly focuses hiding a data in an 8-bit audio file. By graphical representation we prove the results are time-efficient and effective.**

***Keywords*- MOS, LSB, AES, Steganography.**

I. INTRODUCTION

Have you ever wanted to hide secret information from your family, friends, or government? If yes, then you have to learn about STEGANOGRAPHY. In Steganography technique third party can't recognize the hidden secret information from the cover media objects like Audio, Image and video. The audio file which consists of hidden information is known as Audio steganography .The Audio Steganography method embed secret information in WAV sound files. The WAV media is much easier to handle in order to hide information and extract information because it includes redundant, unnecessary and unnoticed data spaces. The size of the information is generally quite small compared to the size of the media in which it must be hidden. We implement system that an audio file is used as a cover object to hide textual secret information without affecting the content of audio file and its structure. Since degradation in the perceptual quality of the cover object may leads to a noticeable change which may leads to the failure of objective of steganography.

We implement the proposed system using symmetric cryptography because cryptography is an extra layer of security and it help on adding randomness in information to be hidden with our methods. Term Steganography and cryptography are closely related. Scrambling of information is done in Cryptography which cannot be understood. Hiding of information is done by Steganography which cannot be seen by anyone.

Architecture of system consist of following blocks :

i. ***Cover Object:*** For hiding secret information we are using Audio as cover object. Just by listening or without using any detection tools we cannot detect information present in audio file.

ii. ***Secret Message:*** It is nothing but an original piece of information which is used to send the information to destination.

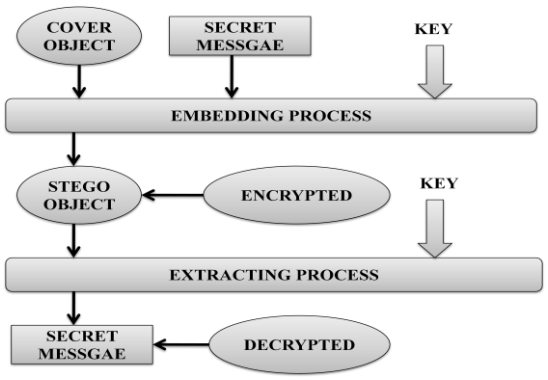

Figure.1 System Architecture of Audio Steganography

iii. ***Key:*** Key is used to do embedding process information with cover audio file. Encryption Key and Decryption Key are two types of key used in audio Steganography.

iv. ***STEGO Object:*** The output of the embedding process is STEGO object which hide secret information in cover audio file according with which technique or method used.

v. ***Encrypted:*** Encryption is nothing but converting original information into a cipher text. Secret key is also input for encryption process.

vi. ***Decrypted:*** Decryption is nothing restoring the plaintext from the cipher text. The key which is used for Encryption is also use for decryption process.

vii. ***Embedding Process:*** Embedding process is also known as encoding. In this, it takes secret information, cover audio and encryption key as input. Information is embedding in audio according to technique or method used.

viii. ***Extracting process:*** Extracting process is also known as decoding. In this, it takes STEGO signal as input and extracts hidden information from it by using decryption key to retrieved original secret information.

II. EXISTING SYSTEM

The existing systems of audio steganography consist with four techniques:

i. Phase Coding
ii. Spread Spectrum
iii. Echo Hiding

All these technique have restrictions of size of message; have very low level implementation and poor interface. Following were some disadvantages of existing system:

i. In phase coding, only first signal segment of Secret message is encoded, so low data transmission rate offers.

ii. In Spread spectrum coding, while maintaining a high level of robustness. Moderate data transmission rate offers but introduce noise into a sound file.

iii. In Echo hiding technique, mix of echoes noticeable which increases the risk for detection.

III. PROPOSED SYSTEM

A. *LEAST SIGNIFICANT BIT (LSB) TECHNIQUE*

With reference to literature survey of audio steganoraphy, the least significant bit (LSB) technique gives effective results hence we consider it for our implementation.LSB coding is one of the modern techniques of hiding the information in WAV audio file. This technique allows large amount of information to be encoded So LSB of binary sequence of each sample of WAV audio File is replaced with binary equivalent of information. In our system to increase security level we take help of cryptography algorithm.

Steps To Hide Secret Information Using LSB Are:
Step 1: Audio file Convert them into bit stream.
Step 2: Each character in the secret information Convert into bit stream.
Step 3: LSB bit of audio file replace with LSB bit of character in the secret information.

B. *LOCATION TO WRITE*

First of all we have to skip the header of the WAVE file. The actual size of the header is 44 bytes. Before writing skip the headers 44 bytes and start the encoding of message bits from the very next byte.

Before encoding message, encode the Size information in the audio file. Basically 8 bytes will be enough to store message size, so encode these 8 bytes in subsequent 64 bytes of audio file after the header bits.

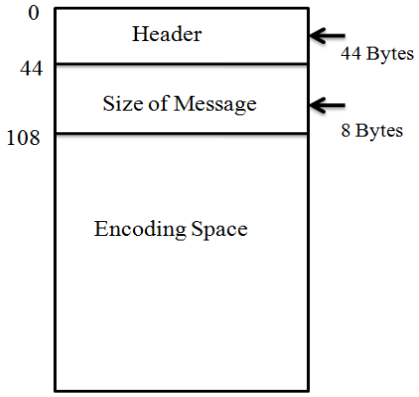

Figure. 2 Encoding Address Space

Now you can encode the message in audio file till the message is completely encoded. if the audio file size is large you don't have to worry, because the remaining bits are kept unchanged so that audio quality is kept intact as much as possible.

C. *ENCRYPTION AND ENCODING*

Actually the cryptography technique is used to make the message unreadable even if the encoded message is detected. This is the second layer of security. For Encryption purpose AES is used which is unbreakable up till now. It is a Symmetric cryptography technique. It is the most secure encryption algorithm. This can be implemented by using the JCA package of java.

After the message is encrypted then it can be encoded into Audio file after the encoding of size bits. Encoding is a process of hiding the message in the audio.

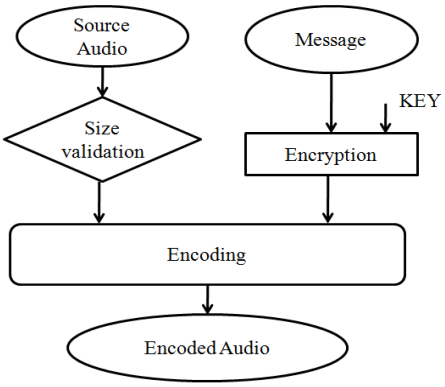

Figure. 3 Encoding

D. *DECODING AND DECRYPTION*

On receiving the encoded Audio file the receiver has to first decode the message so he has to skip first 44 bytes and then read the next 64 bytes to get the exact size of message file. On reading the message size, using counter only that amount of LSB bits can be extracted starting from 108 locations, since the message is encoded from that location onwards. Once the counter is reached to zero the decoding process stops and passes the extracted information to the decrypting block.

For the exact decryption of the message the receiver should know the key which was used to encrypt the message, this is because AES is a symmetric cryptographic algorithm. After the successful decryption the original message is displayed to user or it is stored back in the file. Decoding is a process of retrieving the message from the audio.

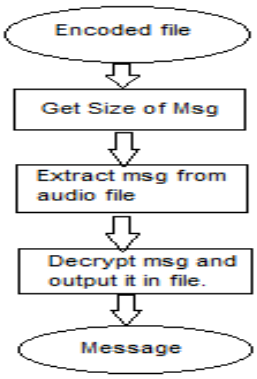

Figure. 4 Decoding

E. *ALGORITHM USED*

i. For Encoding:

STEP 1: Encode ().

STEP 2: Declare audio bytes, text bytes, output bytes as bytes and text length long.

int j=0;

STEP 3: Copy audio file header.

For (i=0 to 44)

Output bytes[i] =audio bytes[i];

STEP 4: write length of text to output file

For (i=45 to 45+64)

Output bytes[i]= convert(audio bytes[i],bit set(text length));

STEP 5: Write text to audio

Output bytes[i] = convert (audio bytes[i], bitset(text bytes[j++]))

ii. For Decoding:

STEP 1: Decode ()

STEP 2: Declare audio bytes, text bytes, output bytes as bytes and text length long.

int j=0;

STEP 3: for (i=45 to 45+64)

Text length= convert(byte set(Audio bytes[i]));

Text bytes[j++]= convert(bytetset(audio bytes[i]));

STEP 4: Recover Secret message.

IV. EXPERIMENTAL RESULTS

The carrier file should be strictly audio (.wav) file format and the secret information may be text file. And here for our experimental scenario the carrier audio file is 'TEST.*wav'* of 215 KB size and the secret text file is INPUT.*TXT'* of 1.57 KB size. In our system, at transmitter side secret text file is embedded in carrier audio file and at the receiver side it recovered back as shown in the following graphical Figure.

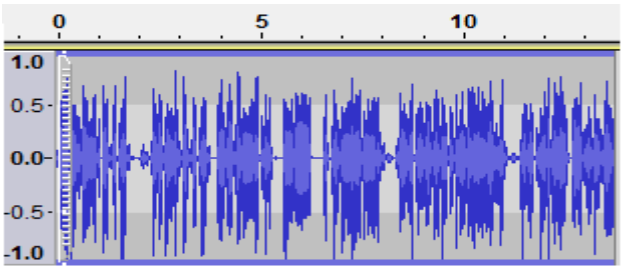

Figure. 5 Original Audio File (Test.Wav)

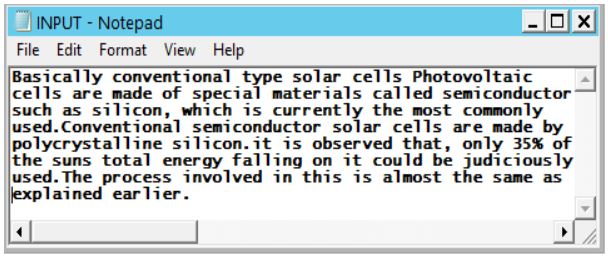

Figure. 6 Original Secret Information (INPUT.txt)

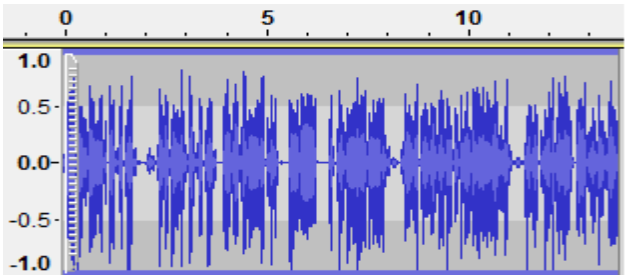

Figure. 7 Embedded Audio File (Stego File)

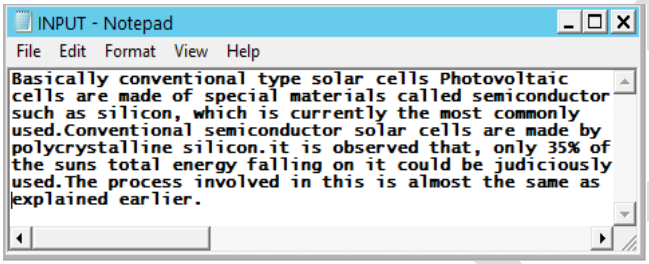

Figure.8 Recovered Message

Figure 5 shows the carrier audio file 'Test.wav' representation. Figure 6 shows the secret text file that to be embedded in that carrier audio file. Figure 7 shows the stego audio file after embedding the secret text file. Figure 8 shows the recovered secret text files at the receiver side. The results are taken as screen shots using audacity tool.

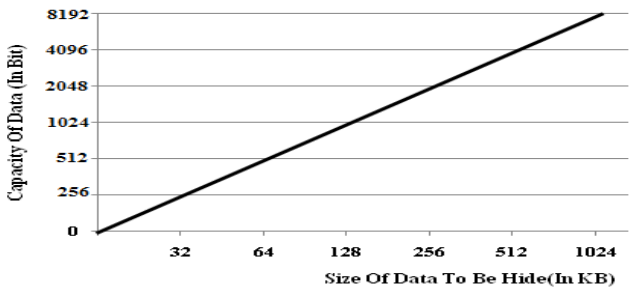

Figure. 9 Hiding capacity of with increasing size

As Shown Figure 9, In Our System as you knows we are using 256Bit capacity of data in which 32KB data is hide. As capacity of data increases the hidden capacity also increases so our Graph represent increases the hidden capacity of the data.

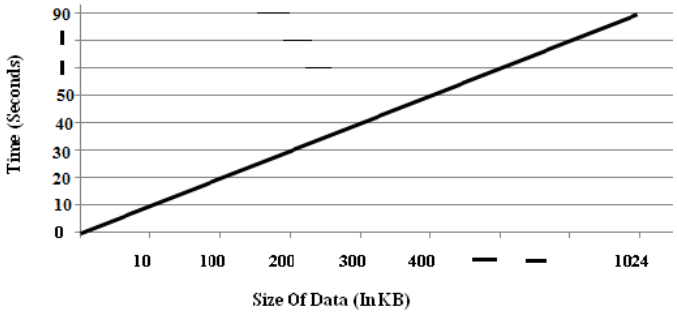

Figure. 10 Encoding Process time VS Size of data

As Shown Figure 10, This graph represent encoding process in which X-axis consist with size of data and y-axis consist time required for encoding data.As in our figure 10kb data require 10 seconds for encoding so as further this graph represent liner increment in both size as well as time. Encoding require more time to encode given data.

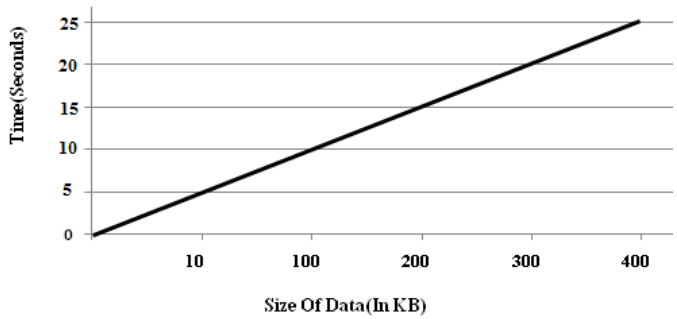

Figure. 11 Decoding process time VS Size of data

As Shown Figure 11, Above graph represent the decoding ratio of time verses size of data in which X-axis consist with size of data and y-axis consist time required for decoding data. In above graph represent us that10kb data require only 5 seconds for decoding process while for encoding process it require more time than decoding process.

Result shows 100% correct extraction of the embedded text. And there is no major difference in the signal representation so it ensures the security.

V. CONCLUSION

In this paper, we implement enhance audio steganography system by using LSB Coding and cryptographic key algorithms to make security system robust. In our system we used enhance version of the LSB technique which gives high embedding capacity and it can be retrieved without any loss in transmission. So our system is efficient for hiding the data from hackers. Hence, this system is well efficient for transmission of digital data via internet or other communication systems. It proves that our system gives best results that satisfying steganography concept.

REFERENCES

[1] Swati A.Patil, K. P.Adhiya,"Hiding Text in Audio Using LSB Based Steganography" in Information and Knowledge Management ISSN- Vol 2, No.3, 2012.

[2] Bandyopadhyay Barnali, Prof. Samir Kumar ,Gupta Banik, "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited", in International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4,June 2012.

[3] Bankar Priyanka R. ,Patil Komal K., Katariya Vrushabh R., Sanghavi Mahesh R., Shashikant M. Pingle, "AUDIO STEGANOGRAPHY USING LSB" in 1st International Conference on Recent Trends in Engineering & Technology, Mar 2012.

[4] Vittapu Sravan kumar, Budda Lavanya," Combination of Cyphertext and Audio Steganography Technique for Secrete Communication" in International Journal of Emerging Technology and Advanced Engineering,ISSN 2250-2459,Volume 2, Issue 12, December 2012.

[5] M. R.Dixit, Burate D.J,"Performance Improving LSB Audio Steganography Technique", in International Journal of Advance Research in Computer Science and Management Studies Volume 1, Issue 4, September 2013.

[6] P. Ramesh Yadav, K. Padmapriya,V. Usha Shree, "Hiding Data in Audio Using Audio Steganography" in International Journal of Computer Applications in Engineering Sciences,VOL I, ISSUE II,JUNE 2011.

[7] Vikas Bhagasara, Navnath S. Narwade, Mahesh Kanthali, Rushikesh Pilwar, "Enhanced Data Hiding Model in Audio to Ensure Secrecy", in International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9,March 2013.

Biswajita Datta, Samir Kumar Bandyopadhyay, "Higher LSB Layer Based Audio Steganography Technique", in IJECT vol 2,Issue 4, oct-dec-2011.