NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 3, ISSUE4, APR.-2016

SECURE AUDIO STEGANOGRAPHY BY LSB FOR HIDING INFORMATION

Rupali Patil
Department of Electronics and Telecommunications,
Savitribai Phule Pune University, TSSM's BSCOER, Pune, India

Prof. Dipak Pawar
Department of Electronics and Telecommunications,
Savitribai Phule Pune University, TSSM's BSCOER, Pune, India

ABSTRACT

Steganography is an art of sending hidden data or secret messages so that a third party cannot detect the presence of the secret messages. The goal of steganography is different from classical encryption. In this paper, secret message in the form of text file is embedded within the carrier audio file (.wav). The LSB embedding method replaces the LSB bits of carrier audio file by secret data bits. In the transmitter end the output is similar to the carrier with secret message embedded inside. At the receiver end the original message can be retrieved without any loss.

INTRODUCTION

Steganography is an art of hiding secret message in to different message without knowing anyone about presence of secret message except the receiver. Steganography is one of the ways which is used for secure transmission of secret information. Information Hiding in audio is less doubtful than communicating an encrypted file[2]. The main purpose of steganography is to transfer the information secretly by screening the presence of information in some other medium such as image, audio or video. After application of steganographic method the formed output file is known as stego-object.
The undisclosed information bit can be implanted by slightly shifting the binary sequence of an audio file. Available audio steganography software can insert messages in .WAV audio files. Injecting the secret information bits in audio file is usually a more difficult task than injecting information bits in other media, like digital images. To embed the secret information in digital audio different types of methods are used. For audio steganography, the methods that are commonly used include LSB coding, Parity coding, Phase coding, Spread spectrum, Echo hiding. Most frequently used technique for audio steganography contains bitwise manipulation of the cover object to insert the secret information bits. For bitwise steganography, Least Significant Bit (LSB) Steganography is a good approach, where the secret information bit to be hidden into the LSBs of the cover object [5].

STEGANOGRAPHIC LSB TECHNIQUE

The conservative LSB method and the proposed method are conferred in detail

CONSERVATIVE LSB METHOD

The data is hidden inside the cover object by changing the least Significant Bit of each sample of the cover object. If the LSB is varied, it will not disturb the characteristic of the sample and also the cover data that is audio. The asset of the LSB compared with the other bits in the sample is negligible. It will occur some noise, but the found noise level should be kept below a threshold. In conservative method, it is easy for the stalker to extract the message from the stego signal [1].
Figure 1 shows the basic steganographic approach. Here a secret data is being inserted inside an input signal to produce the stego signal. A key is usually needed in the embedding process. The accurate stego key is used by the sender for the embedding procedure. The same key is used by the receiver to extract the stego signal in order to view the secret data. The stego signal should look almost identical to the input signal.

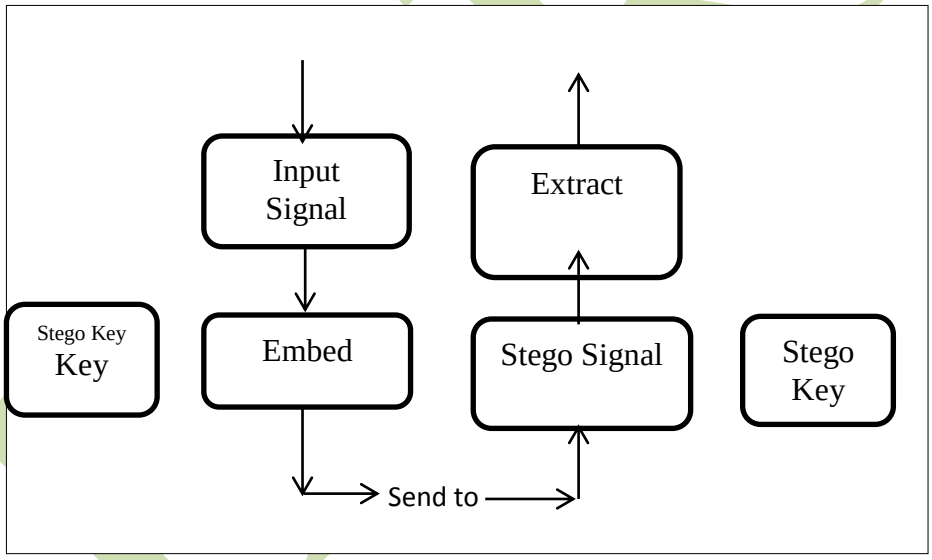

Figure 1: Basic Steganographic Approach

PROPOSED METHOD

Proposed method can be used to overcome this problem. Figure 2 shows the proposed LSB steganographic approach. Secret message is encrypted by using the AES-128; it will create the relation between plain text and cipher text. Encryption method decreases the capacity of insertion but increases it's robustness. In Figure 2, a secret data is being inserted inside a cover image to produce the stego image. A key is a important factor in the embedding process. The proper stego key is used by the sender for the embedding process. The same key is used by the receiver to extract the stego cover image to view the secret data. The stego image should look nearly equal to the cover image [2].

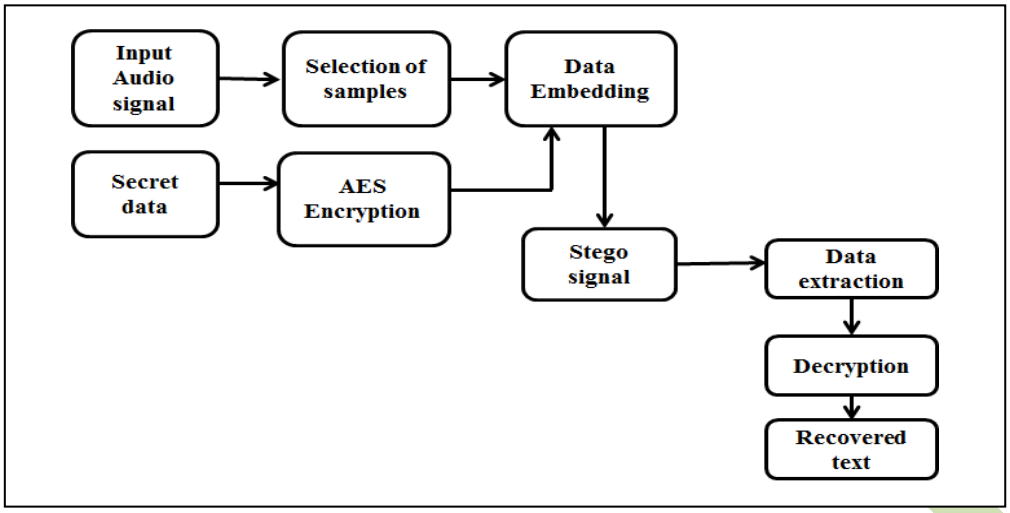

Figure 2: Proposed LSB Stegnographic Approch

METHODOLOGY

In randomized LSB algorithm, there are two methods named Bit Selection and Sample Selection to improve the conventional LSB method.

BIT SELECTION MAPPING

Same bits of cover audio sample never used to embed the secret message bits in order to confuse the intruder. So, to hide the secret message, proposed method produces randomness in selecting different bits of a sample. First two MSB (Most Significant Bit) of each sample will select which bit of the same sample would contain the secret message bit. Table 1 shows the proposed bit selection mapping. In this method secret message bit will embed in first three LSB bits [3].
If the first two MSB sample bits are equal to '00', then third LSB sample will be swapped with secret message bit. If the first two MSB bits are equal to '01', then second LSB will be swapped with secret message bit. If the first two MSB bits are equal to '10'or '11' then first LSB will be swapped with secret message bit.

Table1. Bit Selection Mapping

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

SAMPLE SELECTION MAPPING

Sample selection mapping offers another way to confuse intruder, means by selecting random samples of a cover audio file, it add some more randomness in embedding process. So, this

means that all the samples of audio file will not contain secret message bit but only few will contain secret message. Here using first three MSB values of a sample the randomness is obtained. Table 2 shows sample selection mapping. In this process some of the samples are skipped in between embedded samples.

Table 2. Sample Selection Mapping

1st MSB	2nd MSB	3rd MSB	Sample Containing Next Secret Message Bit
0	0	0	j+1
0	0	1	j+2
0	1	0	j+3
0	1	1	j+4
1	0	0	j+5
1	0	1	j+6
1	1	0	j+7
1	1	1	j+8

Suppose j is the initial value of sample, the last columns of table 2 shows that next sample have the secret message bit. In this procedure, number of samples is skipped in between two consecutive secret message bits. Initially (j=1), if the first three MSBs Bits of cover audio samples are equal to '010', then the last column indicates the next sample (j+3=4) contains second secret message bit in same audio cover sample. It shows that, first secret message bit is inserted in first sample and next message bit is kept in fourth sample. In the same way, when the fourth sample of audio file is equal to '011', and then the third message bit will be kept in eight sample of audio file [4].

EXPERIMENTAL RESULTS

Audio steganography is performed on fixed LSBs to find the threshold value after which the difference between host message and stego message becomes measurable. Fixed bits of every sample of host message are swapped with secret message bits without using the randomness proposed in Bit Selection and Sample Selection. The original host signal is shown in Figure 3. The host signal after LSB embedding is shown in Figure 4. The resulting Stego audio file (retrieved audio) after embedding secret message is shown in Figure 5. It is clear that, there is not much difference in original audio data and retrieved audio data.

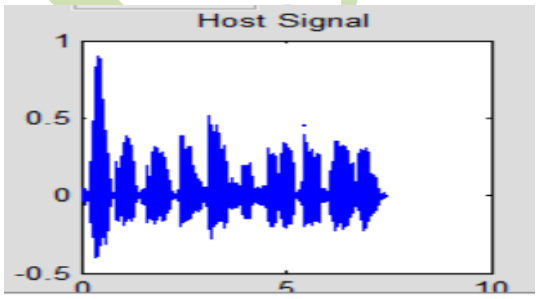

Figure 3: Host Signal

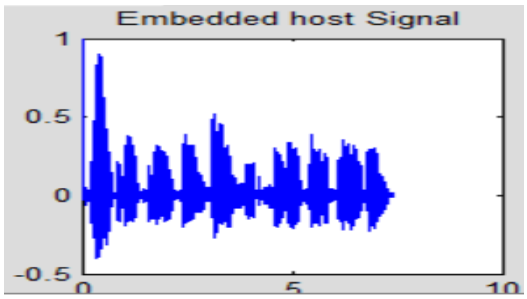

Figure 4: Embedded Host Signal

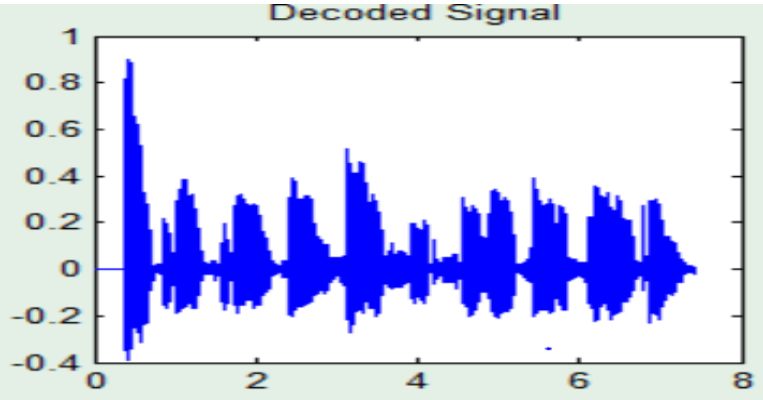

Figure 5: Decoded Signal

Firstly, the secret information is encrypted by using AES-128 cryptographic algorithm at the sender side. This AES algorithm makes the relation between plain text and cipher text complex. Cover audio data and Encrypted information is converted into binary digits. A secret information key is encrypted into audio frame as "BSCOER" is encrypted into audio frame as "#Zoq". For embedding this encrypted secret message, we have to change bits with higher weightage that will result in a detectable change in the stego message.
Transparency and robustness can be calculated in terms of Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). MSE is derived by equation (1) and PSNR is derived by equation (2) as given below-

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(xi - yi)^2 \quad \ldots\ldots(1)$$

$$\text{PSNR} = 20\log_{10}\left(\frac{2^{max}-1}{\sqrt{MSE}}\right) \quad \ldots\ldots(2)$$

Where N defines the total number of samples of the cover audio signal, max is the number of bits in one sample bit, xi is ith sample in cover audio signal(x), yi is the ith sample in stego audio signal(y) and value of i should be same for both original as well as stego audio signal. Secret message bits are implanted in binary form of cover audio.
So, performance analysis for MSE and PSNR are calculated as-

MSE = 6.7191e-09

PSNR = 129.892

CONCLUSION

A randomized LSB model for audio Steganography is presented in this paper to make it more secure against steganalysis. The stego message cannot be discriminated from host message which is formed on the basis of proposed methodology. The secret message on the receiver side can be removed from the stego message. The AES encryption technique is applied to secret message bits, therefore it changes the demonstration of the secret message. In hiding

the secret information, the proposed method meets all the requirements and it is satisfied with working against steganalysis. As there is no difference between original and retrieved audio signal i.e secret information recovered without any error. For secure data transmission, this proposed system satisfied all the requirements such as robustness capability, and security.

REFERENCES

[1] Gopalan, K., "*Audio Steganography Using Bit Modification", 2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, Page(s): II - 421-4 vol.2.*

[2] Zamani, M., Manaf, A, Ahmad, R.B., Jaryani, F., Taherdoost, H.,Zeki, AM., "*A secure audio steganography approach",International Conference for Internet Technology and Secured Transactions 2009, Page(s): 1 - 6.*

[3] Muhammad Asad, Junaid Gilani, Adnan Khalid, "*An Enhanced Least Significant Bit Modification Technique for Audio Steganography", 978-1-61284-941-6/11/ ©2011 IEEE*

[4] Kaliappan Gopalan ,"*A Unified Audio and Image Steganography by Spectrum Modification", International Conference on Industrial Technology, 2009, Page(s):1 - 5.*

[5] Gaurav Saini, Parulpreet Singh, "*Audio Steganography by LSB Method and Enhanced Security with AES", International Journal of Advanced Research in Computer Science & Technology (IJARCST),Vol. 2, Issue 2, Ver. 2 (April - June 2014)*

[6] Soumya Banerjee, Saikat Roy, M.S.Chakraborty, *Simpita Das, "A Variable Higher Bit Approach to Audio Steganography",978-1-4799-1024-3/13/©2013 IEEE.*