ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Dual Key Indexing Method for Least Significant Bit Modification based Audio Steganography

Vipul Sharma[1], Lalita Sharma[2], Ravinder Thakur[3]

P.G. Scholar, CSE Department, L.R. Institute of Engineering and Technology, Solan, India[1]

Lecturer, ECE Department, Shoolini University, Solan, India [2]

Assistant Professor, CSE Department, L.R. Institute of Engineering and Technology, Solan, H.P. India[3]

Abstract: In this era of emerging communication technologies, secure transmission of secret & sensitive information has always been a challenge due to various attacks on it. Audio Steganography is considered one of the reliable techniques to hide a secret message with in an audio. LSB technique is very efficient technique to embed secret message by replacing LSBs of carrier audio. In this paper Dual Key Indexing method is proposed to map secret message onto the LSBs of the carrier audio. Primary key is provided by Trusted-Third-Party (TTP) whereas secondary key is provided by the encoder which will be needed to extract the secret message at receiver end. The proposed method injects more randomness & confidentiality as compare to the traditional methods.

Keywords: Audio Steganography, Dual key indexing, Data Embedding, LSB method, Trusted Third Party.

I. INTRODUCTION

The term Steganography emerged from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". Steganography is the art of hiding information in a cover file. This technique relies on a message being encoded and hidden in a carrier file in such a way as to make the existence of the message unknown to an observer. There has always been confusion between Steganography and Cryptography. Cryptography changes the representation of the message while Steganography hides the existence of the message [1].

There are various steganography techniques used these days, amongst which Image, Audio and Video Steganography are popular. The audio steganography is the most secure and challenging method as Human Auditory System (HAS) is more sensitive than human visual system. Any slight changes in an audio can easily be detected by human ears [2].

The basic idea behind Audio Steganography is to hide the secret message in an audio signal called cover audio or the carrier audio. The resultant audio after steganography process is called stego message or stego audio, which is further transmitted to the receiver through a secure channel. At the receiver end audio is processed to extract secret message from it by applying appropriate algorithm on it.

The objective of this paper is to ensure more security towards steganalysis attacks, by using the concept of Dual Indexing Keys, one of which will be provided by Trusted-Third-Party (TTP) and other will be transmitted by the encoder. Apart from this capability is also taken into consideration so that maximum load can be embedded with the audio effectively.

Related work regarding LSB method, that has been done previously, is described in Section II. Section III describes the proposed methodology Discussion and Analysis of the proposed method appears in Section IV and Section V concludes the paper.

II. RELATED WORK

There are a number of methods which were previously used to embed a secret message with an audio file like LSB Substitution, Phase Coding, Eco Hiding and Spread Spectrum. LSB encoding method is one of the simplest methods that can help to embed a large message comparatively [3].

In conventional LSB encoding method Least Significant bits of the audio sample is replaced with the secret message bits. The index of placing the bits can be randomize so as to increase robustness [4]. In some cases MSB's are used to select the Bit positions and Samples to be coded. Afterwards bits of secret message are being placed on the selected locations [5].

In [6], an audio steganographic model is proposed which improves the confidentiality of the hidden message and also improves the capacity of the system. This system architecture consist of three different layers to fight against steganalysis: Huffman Coding [7], RSA encryption and dual randomness LSB method.

Concept of Stego-Key or password has also been used in Audio Steganography. In this method both the channels of a stereo audio file is used. Stego Key would determine a channel and exact bit position in a byte where the secret message bit will be place [8].

In [9], Generic Algorithm is proposed which hides the secret message in the deepest portions of audio file. Error produced by the modification is reduced by altering some other bits of wave file. If modification of one sample bits is not possible, it jumps to another sample.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

III. PROPOSED METHOD

In this section we have described our proposed methodology in following sequence: Model Description, Encoding & Decoding Algorithm, and Process Explanation.

A. Model Description

Our model uses a 32 bit CD-quality .wav file format. Stereo wave file contains two channels. The secret message is embedded in both channels which increases robustness of the model. Index of the selected bits is compiled with the help of stego keys.

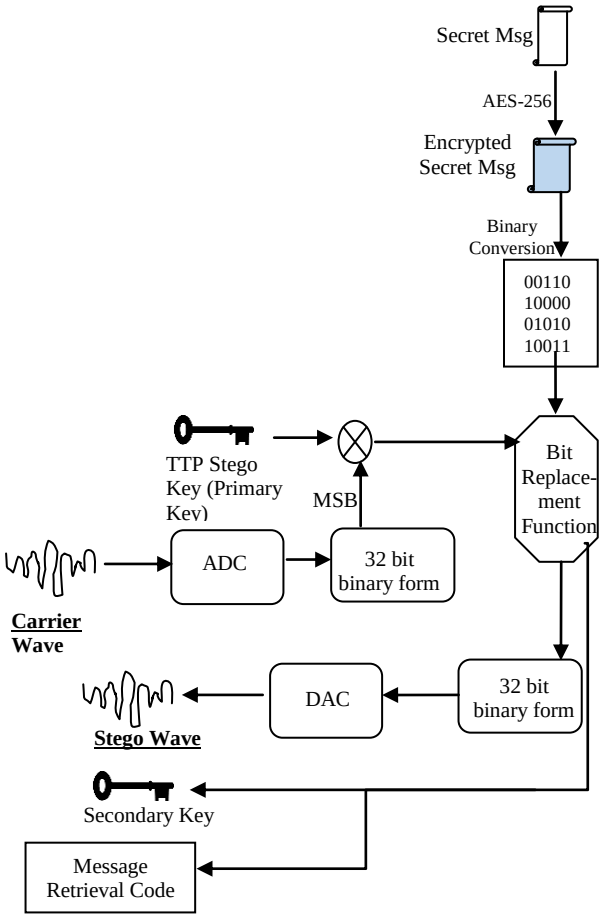

Fig. 1 Dual Key Indexing LSB Modification Technique Encoder Flow Diagram.

This model uses a new stego key technique which uses Trusted-Third-Party key to generate bit index. The secret message is first encrypted using AES-256. The encrypted message is further mapped into binary bits. Afterwards bit positions are calculated using TTP key and the secret message bits are placed on these calculated positions.

Fig. 1 shows the proposed methodology for the encoder part of stego audio. Unlike other LSB techniques our methodology uses a trusted third party key which generates the actual index for the encrypted message bits to be placed. XOR operation is performed on TTP key and the MSBs of the carrier audio to get the final indexes. The XOR operation makes the Key and the carrier audio counterparts to each other which ensures more security against steganalysis. The output of the proposed encoding process provides three elements: Stego Audio, Secondary Key and Message Retrieval Code. In addition to TTP key, secondary key and message retrieval code is supplied to the decoder end, which will be required to extract the actual message from the stego audio. This kind of method adds another layer in the security of the secret message.

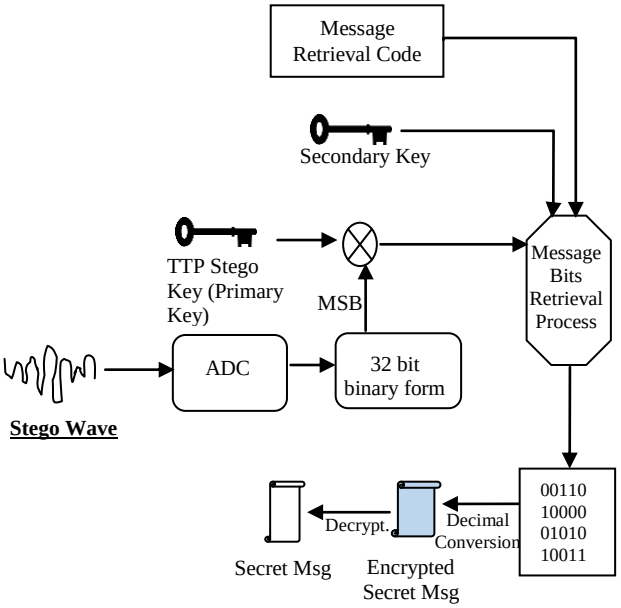

Fig. 2 Dual Key Indexing LSB Modification Technique Decoder Flow Diagram.

Channels of the stereo wave are selected alternatively and message bits are placed at the index positions calculated by the Bit Replacement Algorithm. This means that n^{th} bit of secret message can take any position in one of the LSBs of any sample.

Fig. 2 shows the decoding part for our proposed model. In this decoding method Stego Wave is operated with TTA Stego Key, Secondary key and Message retrieval code given by the encoder. Same as encoder, the primary key (TTA Stego Key) and MSBs of the Stego Audio undergo XOR operation to calculate LSB index in a sample and secondary key points towards the sample having the secret message bit. Message retrieval code acts as a password to extract the secret message from stego audio. The binary form of the message is converted in its actual encrypted form that is further decrypted into the secret message.

B. Encoding and Decoding Algorithm

Following notations have been used to describe encoding and decoding algorithm.

- M_s: Secret Message to be embedded.
- M_e : Encrypted Secret Message Binary Sequence.
- W_r : 32-bit block of sampled Right Channel of Carrier wave.
- W_l : 32-bit block of sampled Left Channel of Carrier wave.

DOI 10.17148/IJARCCE.2015.4903

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

- P_k : TTA Stego Key or Primary Key.
- S_k : Secondary Key generated by encoder.
- P_w : Message retrieval code.
- S_r : 32-bit block of sampled Right Channel of Stego wave.
- S_l : 32-bit block of sampled Right Channel of Stego wave.
- i : stands for index

ENCODE MESSAGE:

- Select Samples of carrier wav ($R_i[k]$).

$R_i[k]$ = randperm(len_wav) */Generate Random Sequence of unique integers.*/

- Find Bit Positions corresponding to selected samples.

$Ci[k] = \text{decimal}\ \{P_k(1{:}len\_m,1{:}3) \otimes W_{rl}(1{:}len\_m,1{:}3)\}$

- Place secret message bits on generated index.

Alt_Select (W_r or W_l) */select left and right channels alternatively */
for k = 1:2*len_m do
$W_{(r\ or\ l)}(\ R_i[k], Ci[k]\ ) = M_e(1,k)$

$S_r = W_r$; $S_l = W_l$

OUTPUT:

Stego wave = Binary_to_wav($S_r + S_l$)
$S_k = R_i$ */ generated by encoder */
$P_w =$ len_m */ Length of the embedded message */

DECODE MESSAGE:

$Ci[j] = \text{decimal}\ \{P_k(1{:}len\_m,1{:}3) \otimes S_{rl}(1{:}len\_m,1{:}3)\}$

Alt_Select (S_r or S_l) */select left and right channels alternatively */
for j = 1:2*len_m do
$M_e(1,j) = S_{(r\ or\ l)}(\ S_i[j], Ci[j])$

Ms = Binary_to_char(M_e)

C. Process Explanation.

Unlike conventional LSB substitution method, this method takes TTP (Trusted Third Party) key as input stego key. This key is in form of array of size[length_audio,3]. Afterwards first three MSBs of Carrier wave sample are XORed with TTP key, which gives us column index as a result. Encoder uses a random function to generate a random sequence of unique integers up to the length of the secret message, which gives us row index. This will allow the encoder to randomly place the secret bits in randomly selected samples, which will be very difficult to detect by any intruder. An alternator function select Left and Right channels alternatively. After selection of the channel, secret message bits are placed on the positions determined by the column index and row index vectors.

The encoder generates two additional outputs other than stego wav. One is a secondary key, which points toward the samples to be searched for secret bit and other is message retrieval code, which will be required to encode the message. That means there are three parameters which are necessary to retrieve the secret message. This kind of methodology provided triple protection against steganalysis

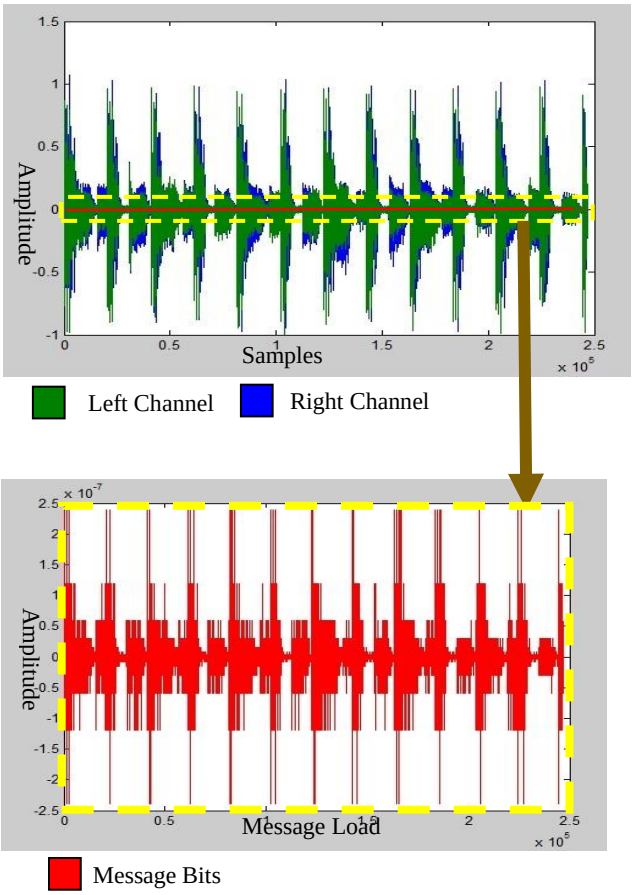

Fig. 3 Stego Audio and Message Load inside it.

IV. RESULTS AND DISCUSSION

The main objective of this methodology is to provide more security to the message content embedded with an audio wave. There is always a trade-off on perceptibility and data robustness for heavy payload [10]. Maximum locations with minimum effect on original sample are being selected so as to utilize all the suitable locations to place secret bits. Fig. 3 shows how the message load occupies the position in original wave file with minimum effect and high robustness. The figure consists of stego audio and secret message within it, which has been plotted just below the wave.

In this case, 32 bit Stereo wave file having size 1927 kb & length 6 sec. with sampling rate of 44100 samples/sec have been taken to carry a message load of 1524 bytes. To evaluate the quality of the stego wave SNR and BER (Bit Error Rate) have been calculated and thereafter tabulated in Table I.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

TABLE I

Attribute	Left Channel	Right Channel
SNR (dB)	144.0048	143.4112
Bit Error Rate (BER)	0.1412%	0.1543%

V. CONCLUSION

Use of Trusted Third Party stego key increases the confidentiality of the secret message to be embedded in the audio files. The randomized secondary key facilities proper utilization of the samples of carrier wave and also adds a layer of protection to the decoding process. As compare to the conventional LSB methods, this method produces much lesser Bit Error Rate (BET) & very suitable SNR, which makes it very effective.

REFERENCES

[1] Neha Gupta and Ms. Nidhi Sharma, "DWT and LSB Based Audio Steganography" ICROIT 2014, India, Feb 6-8-2014.
[2] Shahreza S.S. and Shalmani M.T.M., "Adaptive wavelet domain audio steganography with high capacity and low error rate", in Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, pp: 1729 – 1732, 2008.
[3] Gunjan Nehru and Puja Dhar, "A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach" , IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012, ISSN (Online): 1694-0814.
[4] Harish Kumar, Anuradha, "Enhanced LSB technique for audio steganography", IEEE International Conference on Computing, Communication and Networking Technologies (ICCCNT'12).
[5] Muhammad Asad, Junaid Gilani and Adnan Khalid, "An enhanced least significant bit modification technique for audio steganography", IEEE International Conference on Computer Networks and Information Technology (ICCNIT), 2011.
[6] Jithu Vimal and Ann Mary Alex, "Audio Steganography Using Dual Randomness LSB Method", IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014.
[7] Muhammad Asad, "Text Steganography Using Huffman Coding", International Conference on Intelligent and Information Technology 2010, Volume: 1, Pages: 445-447.
[8] Ashis Kumar Mandal, Mohammed Kaosar, Md. Olioul Islam and Md. Delowar Hossain, "An Approach for Enhancing Message Security in Audio Steganography", IEEE 16th International Conference on Computer and Information Technology, 8-10 March, 2014.
[9] Mazdak Z., A.M. Azizah, B.A. Rabiah, M.Z. Akram and A. Shahidan, "A Generic Algorithm Based Approach for Audio Steganography", World Acad. Sci. 2009.
[10] Kaliappan Gopalan and Qidong Shi, "Audio Steganography using Bit Modification – A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Steganography", IEEE 19th International Conference on Computer Communications and Networks (ICCCN), 2010.