I J C T A, 9(11) 2016, pp. 5401-5408

REVIEW PAPER ON EFFICIENT METHOD OF INFORMATION SECURITY BASED ON WAVELET TRANSFORM AND LOW BIT ENCODING AUDIO STEGANOGRAPHY

Mahesh Kumar[*], and Nitin Kaul[**]

Abstract: In the world of emerging technology, data transmission over a secure channel is a major concern of security. We need to secure data transmission from unauthorized access by any third party. Steganography is an efficient method to resolve such major security issues. Steganography is method of hiding sensitive and valuable information in media such as image, text, audio, video etc. Steganography which is a Greek word composed of two words Stegano and graphy. Stegano means hidden and graphy means writing. So steganography is method of hidden writing. There is another term cryptography which is different from steganography .Cryptography converts the secret message in other than meaningful message or it disorganizes structure of the message but this technique is less secure as message can be accessed by any third party. Audio steganography deals with embedding secret message in audio sound. In this paper secret message in the form of image has been embedded in an audio using the LSB (Least Significant Bit) technique and the Discrete wavelet transform (DWT).To increase the robustness of the data and increase the capacity of system new algorithm is proposed which provides better result in term of PSNR.

Key Words: LSB; DWT; Steganalysis; PSNR; Capacity; HAS

1. INTRODUCTION

From the transmitter end, time when data is created and transmitted to the receiver where it is received we need that data should be secure without losing the important and sensitive information. A data can be in the form of Text, Image, Audio, and Video etc which is called cover. And Carrier also may be Text, Image, Audio, Video etc. An encryption technique is used at the sender side and decryption technique is used at the receiver side. Cover (Image, Audio, Video) information is hidden in the carrier file such as image, audio to embed the information from the unauthorized access. On receiver side, the information is decrypted to identify the originality of the cover information and stego file is obtained. Few techniques have been implemented to secure the information i.e. Watermarking, Cryptography, and Steganography.

In cryptography, the structure of original message is scrambled to make it meaningless so that intruders cannot identify the information. So aim of cryptography is transmitting information between transmitter and receiver in such a way that it avoids a third party from reading it. For verification of the identity of any person, cryptography provides authentication [2].

[*] Student, M.tech (Digital Signal Processing) Lovely Professional University, Punjab Email: mahesh.shr8@gmail.com
[**] Assistant Professor (Communications systems) Lovely Professional University, Punjab Email: nitin.16861@lpu.co.in

Steganography is a method of embedding some secret message in another message so that anyone else except the intended receiver cannot predict existence of the message .Message which is used to hide secret message is called host message or cover message [8]. Message after steganalysis is known as stego message which is combination of host message and secret message. Steganography can be applied to different type of media such as text, audio and video. We use audio file as carrier because audio files are considered excellent carriers [3].

Watermarking is useful when we have to secure copyright content. Where some information about cover media is hidden in the message. Watermarking is way to prevent the illegal claiming of any digital media in other words it helps in identification of the ownership of digital media. We can use these media for help but we cannot do illegal copying of that media [4].

1.1 Application of Steganography

- Steganography helps in data communication over an unsecure medium with security.
- Access control is provided easily to the digital information [5].
- To provide safety against data alteration.
- It can be used in TV Broadcasting
- In analysis of the network traffic of any user.
- Used for audio & video synchronization.

1.2 Classification of Steganography

1. ***Text Steganography:*** In this technique the secret data can be embedded in any text file which can be further transmitted across an unsecure medium.

   For example: At sender end **cover message** is--‘’Steganography is a method of hiding some secret message in another message so that anyone else except the intended receiver cannot predict existence of the message.’’

   Secret message to embed—‘’AUDIO STEGANOGRAPHY’’

2. ***Audio Steganography:*** This technique provides a way to hide secret data within any audio media. We have one audio cover file and a secret message file. After processing, obtained message is known as stego message, which is combination of host message and cover message. In figure 1, Audio steganography method is shown in block diagram.

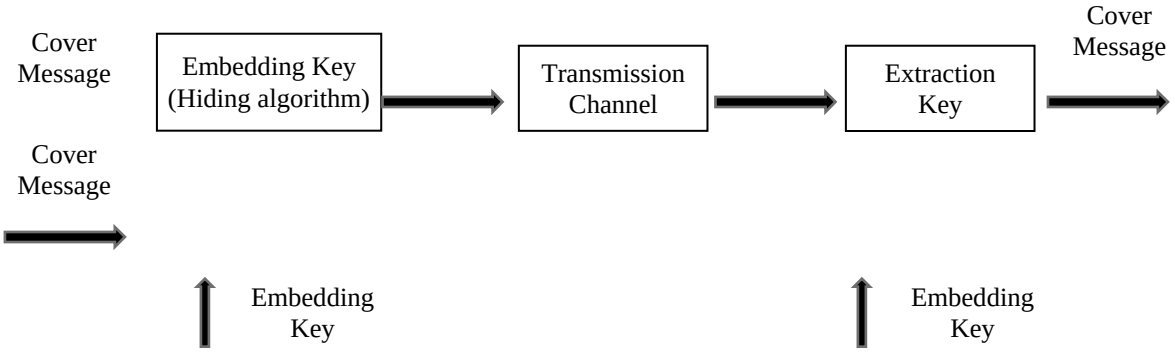

Figure 1: Audio Steganography method

3. ***Video Steganography:*** Secret message is hidden in video file as in figure 2.

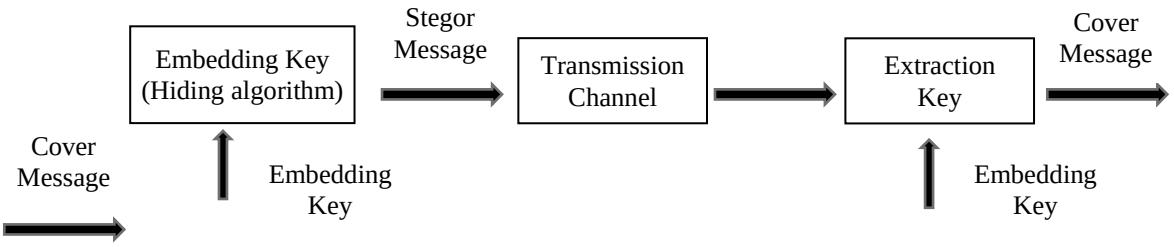

Figure 2: Video Steganography method

4. ***Image Steganography:*** In this technique the secret data can be in cover image. Secret data may be in the form of text or image. The stego image is generated after embedding. Fig. 3 is showing the Image Steganography view after steganalysis.

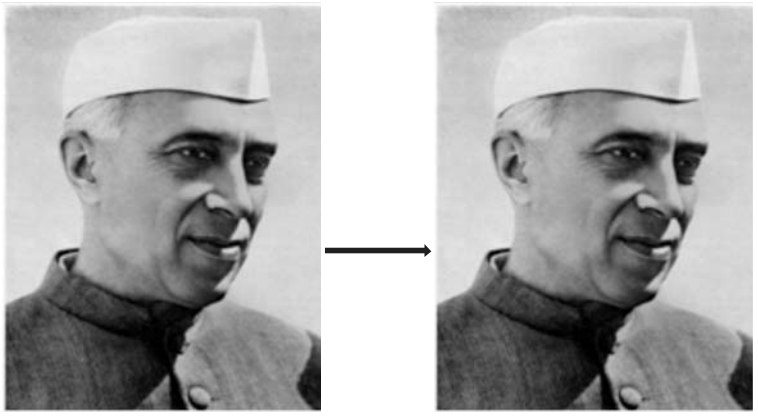

Figure 3: Image before and after steganalysis

2. AUDIO STEGANOGRAPHY

The methods that hides secret message in audio files use the properties of the Human Auditory System (HAS). The HAS is very sensitive it can even detect single variation in sound if there is any random noise present. But still there are some chances we can exploit. It is known that HAS have a large dynamic range, with small differential range. So loud sounds mask out lower sounds. So there are also some fluctuations that are ignored by the HAS. By the process of sampling and quantization the digital sound is converted in digital domain from analog domain.

The basic model of Audio steganography comprises of Carrier as Audio file, Secret Message and Embedding key. We can say carrier as a cover-file, which covers the secret information. Secret message may be in the form of text message, audio message or image of different size or format.

There are three parameters which need to keep in mind while transmission and steganalysis. These parameters are as follow-

(i) Capacity: Number of bits of secret data that can be embedded in the carrier audio.

(ii) Transparency: Security in the system is measured by transparency. How secure the message is embedded.

(iii) Robustness: Ability of system to withstand against the attacks.

3. VARIOUS TECHNIQUES OF AUDIO DATA HIDING

LSB Coding: In LSB also known as Low Bit Encoding, method both the cover file and the secret message are first converted into their basic binary string. Then the LSB of some bytes of covered file are replaced with the sequence of bytes secret message. We chose the right most bit or least significant bit because it does not have that much impact over the quality of cover file [10].

Parity Coding: Basic concept behind this method is that the parity bit of cover file is checked and if they are similar then do nothing and if they are unlike then it changes the LSB of whether cover file or secret message so that parity bits are equal [3].

Phase Coding: In this method first audio file is segmented into parts .Then phase of an initial audio segment is replaced with a reference phase that characterizes the embedded data. It encrypts the secret message bits as phase shifts in the phase spectrum of audio signal [1].

Echo Data Hiding: In this method, the secret message is imbedded by adding echo to the cover file which is an audio signal. Data embedding is represented by taking into consideration that three parameters, decay rate, amplitude initial and delay vary. The initial amplitude is expedient to decide amplitude of original sound. Decay rate is used to decide the echo function. The offset function is used to find out the interval between the original audio signals with the echo that have been introduced [11].

4. PROPOSED WORK

For embedding the image in audio we use the concept of least significant bit by using DWT and introduce an algorithm. LSB is the most robust as well as simple and a conventional forward methodology to embed a message into a cover-audio signal. The message is embedded with sequence-mapping technique in the bit of a cover-audio. LSB embeds the information in such a manner that unauthorized prediction is not perceived easily, but still because of simplicity of this method some security issues are concerned. Therefore, extraction algorithm is needed to implant within the system to prevent malicious attack. For embedding, firstly we take the audio signal as input and convert this into string of binary format. Then secret image which is to be embedded is taken and converted it into binary bits. Using Discrete Wavelet Transforms on audio files and separates the higher frequency components. After we divide audio in block cell of 8x8.We pick cell of audio bits for each 16 bits audio data and inserts the image bits into the extreme bits of the audio file using a Random genetic algorithm and with embedding key. During the extraction of cover audio from stego audio, inverse algorithm and inverse embedding method is employed [1]

4.1 Steps of Data Hiding

1. Take input cover audio signal and convert it into sequence of binary bits in form of 1 and 0.
2. Read the Image which is to be embedded and convert into a sequence of binary bits say it info (Information).
3. Now apply DWT on audio sequence file.
4. Ignore the low frequency components and separates higher frequency component from audio file
5. Use an Embedding key to encrypt at sender side to protect and control the transmission using key generator logic.
6. Fragment binary audio sequence into sub blocks of size of 8x8 each with 16 bits
7. Define initially m = 1;

8. Len =length (cover)
9. For k=I: len
10. Cover (i, 12:16) = info (m, m+3);
11. m= m+4;
12. End
13. Generate audio file from Data.

4.2 Steps for Data Retrieval

1. Take received stego audio signal and convert it into sequence of binary bits.
2. Fragment binary audio sequence into sub blocks of size of 8x8 each with 16 bits
4. Initiate n=l;
5. For j=l: len
6. Info (p, p+3) = cover (i, 12:16);
7. p=p+4;
8. End
9. The Info is the original message.

4.3 Embedding Key Generation Algorithm

1. Take two initial values, say 0, 1.
2. Define control bit, say C.
3. Step 9 is repeated until whole sequence is embedded and retrieved for both end transmitter and receiver respectively in synchronization.

5. RESULTS

Peak signal-to-noise ratio (PSNR): It measures the quality of audio signal. PSNR compare the original audio signal with stego signal obtained .PSNR is measured in decibels (dB). PSNR in decibels (dB) is computed by using [7]

$$\text{PSNR (in dB)} = 10\ log_{10} \frac{\sum_{n=0}^{N} x\ (n))^2}{\sum_{n=0}^{N} (x(n) - y(n))^2}$$

It also helps in quality comparison of reconstructed signal and original audio signal. Example: In Compression of text, video and audio etc. In above equation x (n) is cover audio file and y (n) is combination of host message and cover message [6].In figure 4 here is audio file before and after steganalysis.

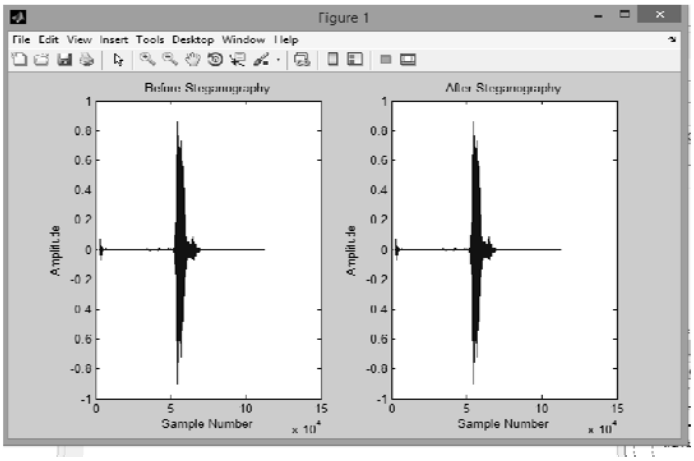

Figure 4: Audio before and after steganalysis

Mean square error (MSE): If there is any variation and distortion in the audio signal after recovering, it is measured by mean square error. It is calculated by taking the square of error between original audio signal and stego audio signal obtained [6].

$$\text{MSE (in dB)} = 10\ log_{10} \sum_{n=0}^{N} (x(n) - y(n))^2$$

Bit Error Rate (BER): For robustness performance error in embedding process is measures by BER.BER is calculated as [2].

$$BER = \frac{\text{No. of total errors during process}}{\text{Total no. of bit transmitted}}$$

Following is the comparison of traditional method used before and proposed scheme in paper giving better result.

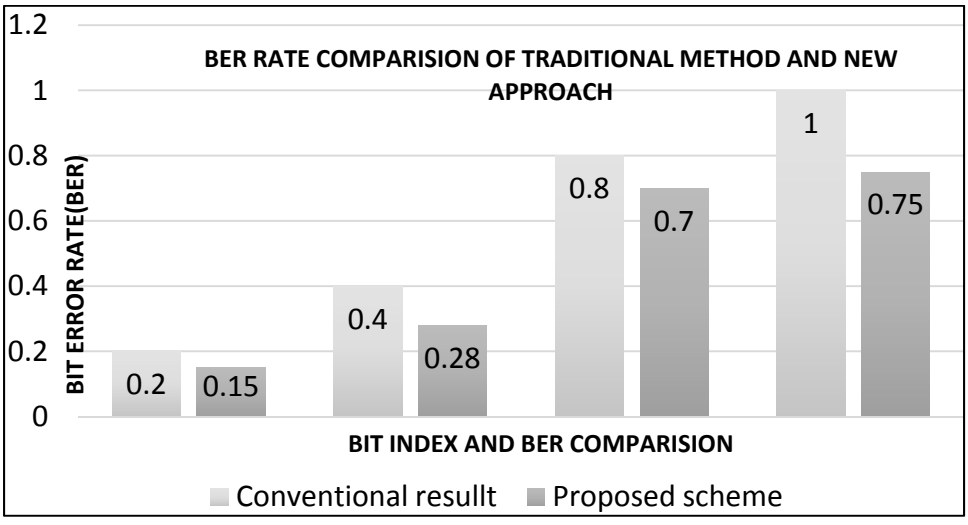

Figure 5: Comparison of proposed method result with methods used before

6. CONCLUSION

The main aim of this paper is to know about a technique to hide the data in audio file keeping in mind that we get better improved result, more robust and with higher capacity. Also, if the message

in form of image is also scrambled such that we have encryption technique to encode then we will get satisfactory security level. Thus no malicious attack can predict existence of sensitive information. Same concept is used here because only with LSB which is easily retrieved, we cannot be confidential about security. Proposed Algorithm is discussed in this paper for embedding image in cover audio file for different size of audio file and format such as wav. Prime focus is on proposed algorithm from convention LSB based data hiding in audio. Proposed method is employed by using the concept of DWT (Discrete Wavelet Transform) and Low Bit Encoding technique.

7. ACKNOWLEDGEMENT

I have taken efforts in this paper. However, it would not have been possible without the kind support and help of many individuals and organization. I would like to extend my sincere thanks to all of them. I am highly indebted to Nitin Kaul for his guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing our project. I would like to express our gratitude towards our parents & member of lovely professional university for their kind co-operation and encouragement which help us in completion of this project. I would like to express our special gratitude and thanks to all our friends for their support.

References

1. Rina Mishra, Praveen Bhanodiya, “A Review on Steganography and Cryptography” in 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA)IMS Engineering College, Ghaziabad, India.
2. B. H. Barhate, Prof.Dr.R.J.Ramteke"Audio Steganography using Combination of LSB and Key for Images, Audio and Text Messages"(ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 5, Issue 7, July 2015).
3. Jasleen Kour, Deepankar Verma, “Steganography Techniques –A Review Paper,” International Journal of Emerging Research in Management &Technology ISSN: 2278-9359, Volume-3, Issue-5, May 2014 pp.132 -135.
4. Neha Gupta, Ms. Nidhi Sharma, “DWT and LSB Based Audio Steganography”, 2014 International Conference on Reliability, Optimization and Information Technology ICROIT 2014,India, Feb 6-8 2014.
5. Yali Lillo Ken Chiang, Cherita Corbett, Rennie Archibald, Biswanath Mukherjee, Dipak Ghosal, "Novel Audio Steganalysis Based on High-Order Statistics of a Distortion Measure with Hausdorff Distance", ISC '08 Proceedings of the 11th international conference on Information Security,2013.
6. Harish Kumar & Anuradha, “Enhanced LSB technique for Audio Steganography”, IEEE July 26, 2012.
7. B.Santhi, G. Radhika and S. Ruthra Reka: “Information Security using Audio Steganography - A Survey”, Research Journal of Applied Sciences, Engineering and Technology 4(14): July 15, 2012.
8. GS Kang, TM Moran, DA Heide, Hiding Information under Speech, Naval Research Laboratory, (Washington, DC NRL/FR/5550–05-10, 126, 2005), 20375-5320, 2012

9. S. Rekik, D. Guerchi, S. A. Selouani, and H. Hamam, ”Speech steganography using wavelet and Fourier transforms,”EURASIP Journal on Audio, Speech, and Music Processing 2012, no. 1, pp. 1-14, Aug 2012
10. S. Bhattacharyya, A.Kundu and G. Sanyal,” A Novel Audio Steganography Technique by M16MA” International Journal of Computer Applications, Vol30– No.8, September 2011.
11. Haider Ismael Shahadi, Razali Jidin,” high capacity and inaudibility audio steganography scheme”, 2011 7th international conference on information assurance and security,978-1-4577-2155-7/11/$26.00 c_2011 IEEE.