

Performance Analysis of Audio Steganography using Modified LSB Technique

Deepa Verma¹ Mr. Pushendra Singh²

¹M.E. Student ²Assistant Professor

^{1,2}Department of Electronics and Telecommunication Engineering

^{1,2}Chhatrapati Shivaji Institute of Technology Durg, Chhattisgarh India

Abstract— Cryptography is a one of the most interesting subject where the data can be hide in another data or it can say the security of the one data is taken by the another data. Steganography is a part of cryptography. Steganography is a technique where the cover file is required to hide or conceal the secret data. Confidentiality, imperceptibility from the adversary is a major part of encrypted data into a stego signal. The stego signal must be robust or transparent against adversary but It should not be perceptible for eavesdroppers. In this paper audio file is uses as cover file and the text (.txt) data is uses as confidential data. This paper includes the camparative analysis of different techniques of audio steganography with focusing on LSB and modified LSB techniques. Some Result obtained by using these two techniques. This obtained result is compared according to parameters.

Key words: Cryptography, Steganography, audio, HAS, SNR, MSE, LSB, DWT

I. INTRODUCTION

Cryptography is a technique where hide a one message into another message by simply jumbling sequence of original message or altered the sequence of message. Steganography stands for the cover writing. Steganography comes from Greek word stgano and garphy at where staganos means 'cover or protected' & graphin means 'drawing or writing'. Steganography is used for concealing the existence of secret message within the cover file. A secret file can be anything i.e. text, image, audio & video. Steganography is normally uses the features of cryptography. Hiding a message with Steganography methods reduces the chance of a message being detected from the adversary or unauthorised access & enemy. Terms used in steganography ;

A. Cover Signal:

Cover signal is an innocent signal at which the secret information is embedded called cover signal. Cover file can be any text, image, audio and video.

B. Stego file:

The file which obtained after the secret message is embedded into the cover signal called stego signal.

C. Stego key:

Key is used for provide more security for the secret message. This key is optional during the encryption & decryption process.

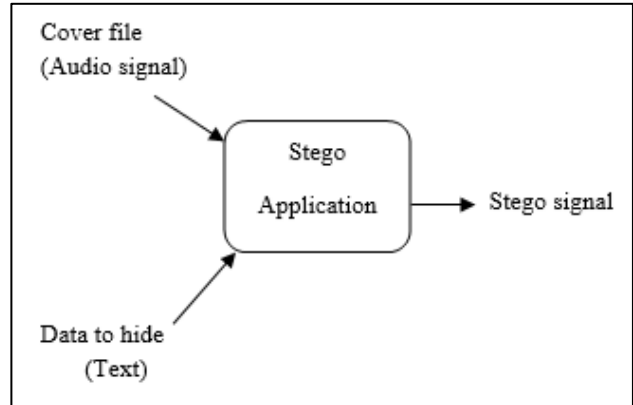


Fig. 1: Steganography Application Scenario

II. TECHNIQUES FOR ENCRYPTION AND DECRYPTION

A. Practical Approach on Text Encryption and Decryption Using LSB Technique:

In LSB technique, the text secret message is firstly converted into the binary sequence. Then separately the audio file is sampled & after sampling, quantization converted the sampled signal into the digital binary sequence. When both the text and audio signal is converted into its binary sequence then LSB technique used to replace the LSB bit of audio file to secret data bit. Fig. 2 illustrates that how the message 'HEY' is encoded in a 16-bit sample using the LSB method. Here the secret information is 'HEY' and the cover file is audio file. HEY is to be embedded inside the audio file. First the secret information 'HEY' and the audio file are converted into bit stream. The least significant column of the audio file is replaced by the bit stream of secret information 'HEY'. The resulting file after embedding secret information 'HEY' is called Stego-file [19].

S.No.	Technique	SNR (in db)
1.	LSB technique	27
2.	Modified LSB Technique	32

Table 1: SNR Values For LSB & Modified LSB

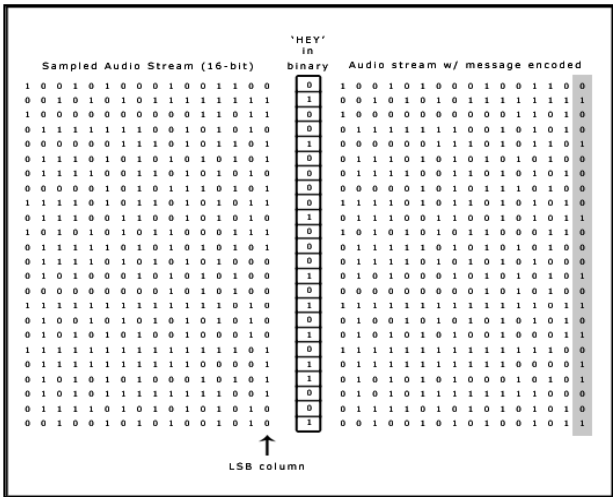


Fig. 1: LSB Coding Example

The secret text which is embedded in our experiment is embedded into the digitized audio file where each sample is represented with 8 bits. The SNR value obtained in our experiment is about 27db.

B. A Modified Text Encryption Technique For Robust Audio Steganography:

In modified LSB technique, from the digitized audio signal some random deeper layer LSB bits are chosen for the secret text hiding. This technique has high capacity compared to the traditional LSB technique. This technique also gives good SNR value. The experimental value SNR of modified LSB technique is 32 db. The size of audio file is 175 kb for both & the size of text or data is 36 bytes taken for embedding. For example:

Audio sample: 10011101 (value 157)
 Message bits: 0 and 1
 After substitution: 10010101 (value 149)
 After modification: 10010111 (value 151)

1) Sender side:

- Convert the secret text message to binary format
- Select audio file and convert it into binary format
- Check the audio size must be greater than secret data size
- Without touching the header part, replace the 3rd or 4th LSB bits of audio bits with message bits
- Repeat this process until the message bit is not encrypted
- After encryption the stego signal obtained is different from original signal
- File is now ready for transmission

2) Receiver Side:

- Stego audio file is received
- The 3rd and 4th LSBs of each byte are calculated to obtain the length of the message.
- Now check the audio signal bits with the stego audio signal and obtain the different bits
- Now converted the obtained bits in ASCII and then into characters
- Now the secret message is obtained by receiver

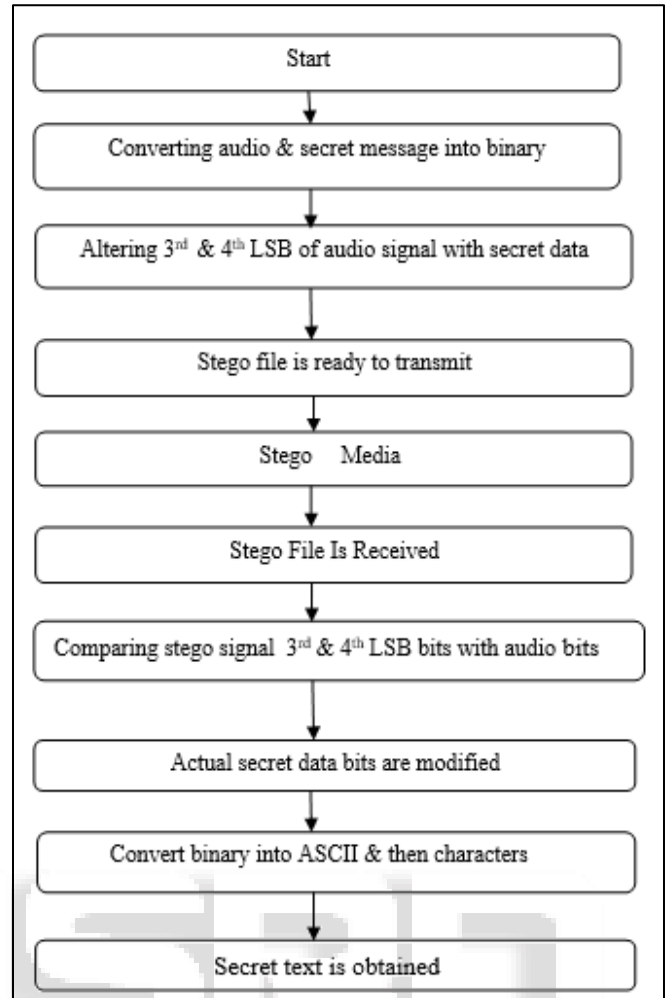


Fig. 2: Flow Diagram of Modified LSB Technique

C. Parameters Comparison of LSB & Modified LSB method:

Features	Traditional LSB	Modified LSB
SNR	low	high
Payload capacity	low	high
Imperceptibility	low	high
Robustness	low	high
security	low	high
transparency	high	high

TABLE 2: Parameters Comparison Of Both LSB & Modified LSB

III. PROBLEMS IN TRADITIONAL AUDIO STEGANOGRAPHY TECHNIQUES

When using different data hiding techniques the problems are always coming here to create difficulty for the security of secret data. The problem also comes when some attack is access during the steganography process.

- 1) The traditional technique like LSB has high capacity but low robust against attack.
- 2) Increases in embedded capacity of audio signal the decreases in the value of SNR get detected. This must be ensuring that the embedded or secret data size must be below from the cover file.
- 3) From all these problems the main problem is HAS which is very sensitive for the any degradation present into the audio signal.

IV. DISCUSSION AND CONCLUSION

All these above problems has the main problem is HAS which is very sensitive for the any degradation present into the audio signal. This two technique gives the main point according to their implementation or as observation i.e. According to obtained SNR values of these two techniques, LSB technique reduces its speech quality than the modified LSB technique.

This paper gives the result of some traditional techniques apart from these, here need of new technique which fulfils the aspects of audio steganography. As the sky is not limit the work with the audio steganography is also not limited with only few techniques. The new techniques will also welcome with their good capacity, good signal quality & which gives the better robustness against existing methods.

REFERENCES

- [1] Mahmood Maher Salih & Mudhafar Al-Jarrah, "Secret Message Integrity of Audio Steganography Using Bi-LSB Embedding", IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.7, July 2015.
- [2] Abdulalem Z. Al-Othmani¹, Azizah Abdul Manaf² and Akram M. Zeki³, "A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012.
- [3] Satish Singh Verma, Ravindra Gupta & Gaurav Shrivastava," A Novel Technique for Data Hiding in Audio Carrier by Using Sample Comparison in DWT Domain", 2014 Fourth International Conference on Communication Systems and Network Technologies.
- [4] S.S. Divya & M. Ram Mohan Reddy, "Hiding Text In Audio Using Multiple Lsb Steganography And Provide Security Using Cryptography", International Journal Of Scientific & Technology Research Volume 1, Issue 6, July 2012 Issn 2277-8616.
- [5] Rohit Tanwar, Bhasker Sharma & Sona Malhotra , "A Robust Substitution Technique to implement Audio Steganography", 2014 International Conference on Reliability, Optimization and Information Technology ICROIT 2014, India, Feb 6-8 2014.
- [6] Prof. Samir Kumar Bandyopadhyay & Barnali Gupta Banik, "Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 1, Issue 2, July – August 2012 ISSN 2278-6856.
- [7] Ronak Doshi, Pratik Jain & Lalit Gupta, "Steganography and Its Applications in Security", International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638 ISSN: 2249-6645.
- [8] K. Gopalan, "Audio steganography using bit modification", Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 2, pp. 421-424, April 2009.
- [9] Soodeh Ahani, Shahrokh Ghaemmaghami, & Z. Jane Wang, "A Sparse Representation-Based Wavelet Domain Speech Steganography Method", IEEE/ACM Transactions On Audio, Speech, And Language Processing, Vol. 23, No. 1, January 2015.
- [10] Preeti Jain & Vijay Kumar Trivedi , " A Novel Technique for Data Hiding in Audio by Using DWTS", IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 ISSN (Online): 2230-7893.
- [11] M. G. Jafari & M. D. Plumbley, "Fast Dictionary Learning For Sparse Representations Of Speech Signals", IEEE J. Sel. Topics Signal Process., vol. 5, no. 5, pp. 1025–1031, Sep. 2011.
- [12] Linu Babu, Jais John S, Parameshachari B D, Muruganantham C & H S Divakaramurthy, "Steganographic Method for Data Hiding in Audio Signals with LSB & DCT", IJCSMC International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 8, August 2013.
- [13] NITHYA POORANI & L.JAWAGAR , "AUDIO BASED STEGANOGRAPHY FOR HIDING SECRET DATA", IJRSET INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY , VOLUME 3, SPECIAL ISSUE 3, MARCH 2014.
- [14] Richa Saxena, Navita Agarwal & Prachi Agarwal, "Data Hiding and Extraction in Audio Files", MIT International Journal of Computer Science and Information Technology, Vol. 5, No. 2, August 2015.
- [15] Nagaseshu.K, Srinivasa Rao.V & Hima Deepthi.V,"A Novel Approach for Embedding Text in Audio to Ensure Secrecy", IJCSIT International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011.
- [16] Aarti Mehndiratta," Data Hiding System Using Cryptography & Steganography: A Comprehensive Modern Investigation", IRJET International Research Journal of Engineering and Technology, Volume: 02 Issue: 01, Apr-2015.
- [17] Masoud Nosrati, Ronak Karimi & Mehdi Hariri," Audio Steganography: A Survey on Recent Approaches", World Applied Programming, Vol (2), No (3), March 2012.
- [18] Monika Gunjal & Jasmine Jha," A Survey Paper on Image Encryption Techniques", IJSRD - International Journal for Scientific Research & Development| Vol. 1, Issue 9, 2013.
- [19] Jayaram P, Ranganatha H R, & Anupama H S," Information Hiding Using Audio Steganography – A Survey", IJMA The International Journal of Multimedia & Its Applications Vol.3, No.3, August 2011.