Data Hiding in Audio Signal Using Cryptography and Steganography Techniques

S.Jeeva(s.jeevarathinam93@gmail.com) , PG Scholar, Gnanamani College of Technology.
Mr.R.Prabhu[2](prabhuras@gmail.com)Assistant Professor, Department of ECE, Gnanamani College of Technology

ABSTRACT

Information sharing and Transfer has increased exponentially. The information is vulnerable to unauthorised access and so cryptography and steganography techniques used. In cryptography technique informations are scrambled and in steganography technique secret message are embedded into cover medium. The perceptual excellence of the host audio signal was not to be degraded while embedding. The main goal of Text data hiding in Audio signal is to hide messages inside the audio in a way that does not allow any enemy to even detect that there is a second secret text message present in the audio. It can also be used for inserting hidden data into audio files for the authentication of spoken words and other sounds and for monitoring of the song over broadcast radio. Hence in which the data is encrypted as well as the encrypted the encrypted data is hided. This system is to be simulated by Modelsim and synthesized by altera cyclone II fpga.

I. Introduction

Secured communication mainly base on cryptography, which encrypts plain text to generate cipher text. However, the transmission of cipher text may easily arouse attackers" suspicion, and the cipher text may thus be intercepted, attacked or decrypted violently. In order to make up for the shortcomings of cryptographic techniques, steganography has been developed as a new covert communication means in recent years. It transfers message secretly by embedding it into a cover medium with the use of information hidingtechniques.

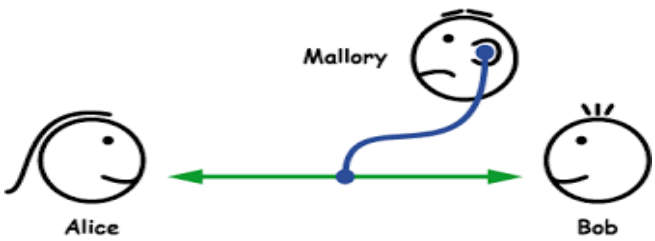


Fig 1: Interception

Fig2: Steganography Technique

Its goal is to hide the fact that communication is taking place. In the field of Stenography, some terminology has been developed. The term cover is used to describe the original, innocent message, data, audio, still, video and so on. The network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are required to protect against unauthorized access. This has resulted in an explosive growth of the field of information hiding. In addition, the rapid growth of publishing and broadcasting technology also requires an alternative solution in hiding information. The copyright of digital media such as audio, video and other media available in digital form may lead to large-scale unauthorized copying. This is because the digital formats make it possible to provide high image quality even under multi-copying.

II.Literature Review

Cryptography and steganography is a technique aimed at providing the secret communication. By combination of these two techniques the security of secret data increases. In this way encryption here used with pseudorandom key generation technique. Cryptography is the science that studies the mathematical techniques for keeping message secure and free from attacks. Steganography is the art and science of hiding communication.Steganographyinvolveshidinginformation soitappearsthatnoinformationishiddenatall.

III. Exisitng System

In existing system image is used as a cover medium so that the technique deals with the pixels followings are procedure for image steganography The sender's prospect of Proposed Technique in which the secret information is encrypted by using simplified data encrypted standard (SDES) encryption algorithm. Then encrypted message is embedded into cover image by

using Alteration component technique. Image containing the secret data is called stego image. Next phase is to select the stego key for encoding. In Embedding process data is hidden by using Alteration component technique in which

pixels have been replaced by key and secret message. Firstly key is converted into binary form and its binary form is filled in the first component of first pixels. After then, secret message is converted into binary form and its binary form is filled in first component of next pixels.

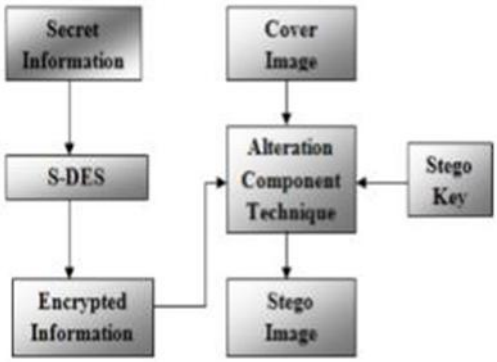


Fig 3: Sender Prospect

With the encrypted data, although a data hider does not know the original mesh content, he can embed an additional message into the mesh by modifying a small proportion of the encrypted data. The selection of mesh parts that are employed to embed messages is based on the following criterion. Since a vertex is contained within several triangles, once the vertex is modified to embed messages, the adjacent vertices should not be modified and are used to recover the central vertex by adjacent correlation at the receiver side.

Embedding Algorithm

Step (a): Extract all the pixels in the given image and store it in the array called PixelArray.

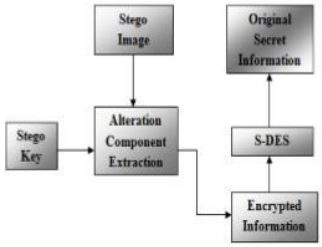
Step (b): Extract all the characters in the given text file and store it in the array called Character-Array. Step (c): Extract all the characters from the Stego key and store it in the array called Key- Array.

Step (d): Choose first pixel and pick characters from Key- Array and place it in first component of pixel. If there are more characters in Key- Array, then place rest in the first component of next pixels, otherwise follow step(e).

Step (e): Place some terminating symbol to indicate end of the key. „0" has been used as a terminating symbol in thisalgorithm.

Step (f): Place characters of Character- Array in each first component (blue channel) of next pixels by replacing it.

The receiver's prospect of Proposed Technique in which the sender sends a stego-image to the receiver or legitimate user. The legitimate user having the stego key to extract secret data from stego image. The legitimate user must have the same key with which the image is embedded. On Stego image Extracting process is applied by using Alteration component technique. After data



extraction I get the secret message which is in encrypted form. Simplified data encryption standard (S-DES) decryption algorithm is used to decrypt message. Finally we get the Secret Data which is embedded

Fig 4: Receiver Prospect

IV Proposed System

In a proposed system the audio signal is used as a cover medium. In which the LFSR technique is use to generate the pseudo random key. And the data is converted into hexadecimal value for convenience of encryption and where for this conversion hex-editor tool is used to get the value. After encryption the converted value is replace in the least significant bit in audio signal. LSB technique is used with LFSR technique (Linear Feedback Shift Register). A LFSR is shift register whose input bit is linear function of its previous state. The most commonly used linear function of single bits is XOR. In which the initial value is called seed and because the operation of the register is deterministic, the stream of values produced by the register is completely determined by its current state.

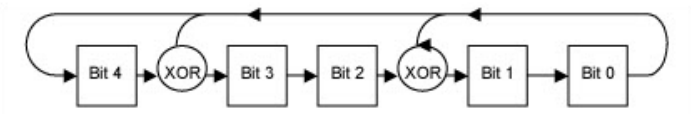


Fig 5:LFSR Technique

For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise. On the other hand, the same noise would be audible in a sound file containing a piano solo. To extract a secret message from an LSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is smaller than the total number of samples in a sound file.

In the sender prospect encryption is done by LFSR technique using Verilog program in modelsim software.

In the receiver prospect decryption is done by reverse process of encryption in which the received audio signal is converted

into hexadecimal value and then converted into original secret information.

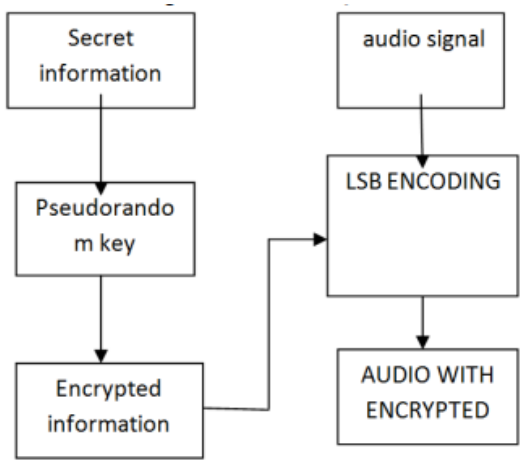


Fig 6: Sender Prospect

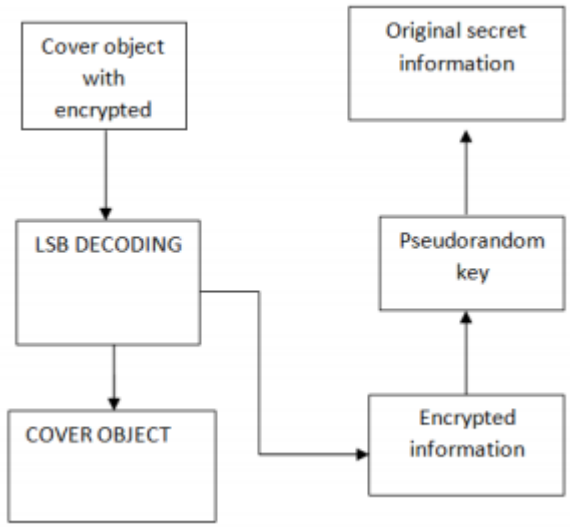


Fig 7: Receiver Prospect

V. SIMULATION RESULT

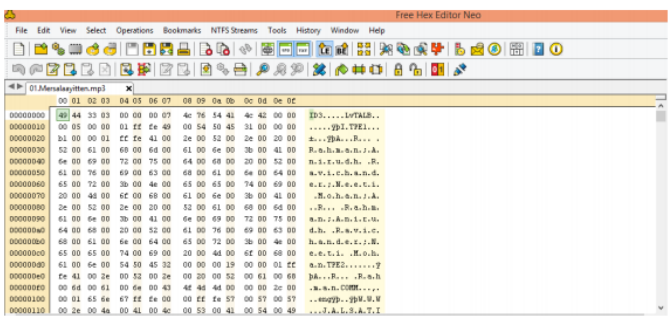


Fig 8: Hex Editor Tool Result

In the Hex editor tool, it is used to convert the audio signal data into hexadecimal value so that the encrypted data hided into the Least Significant Bit in audio signal conveniently.

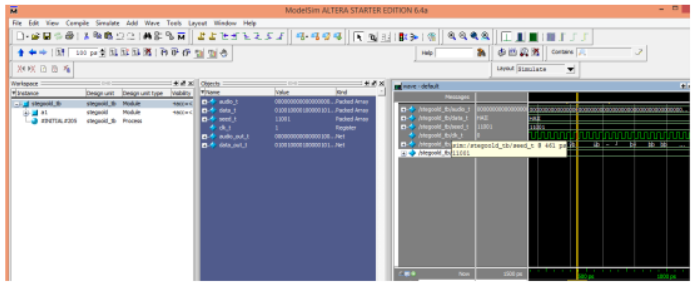


Fig 9:Modelsim Simulation Result

In the Modelsim software, the Verilog program is coded for encryption and decryption. In which encrypted data can be hided into the cover medium as audio signal by Verilog program. So the security of the communication is increased.

VI. Conclusion

This system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This proposed system will not change the size of the file even after encoding and also suitable for any type of audio file format. Thus we conclude that audio data hiding techniques can be used for a number of purposes other than covert communication or deniable data storage, information tracing and finger printing, tamper detection. Thus I have successfully inserted and recovered the hidden data in an audio file. Audio file is manipulated in a way that may be detected by the receiver with a proper key. Thus Text data is hidden in audio file without disturbing the quality of the audio file. Another way to embed is to pad the secret message with random bits for that the length of the message is equal to the total number of samples. This increases the Probability that a would-be attacker will suspect secret communication.

REFERNCES

[1] Kessler, G. "An Overview of Steganography for the Computer Forensics Examiner ", Computer & Digital Forensics Program, Champlain College, Burlington, Vermont, February 2004.

[2] S. Hetzl, StegHide, http://steghide.sourceforge.net, 2003.

[3] Bennett, K. "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text" Technical Report, Center for Education and Research in Information Assurance and Security (CERIAS), 2004.

[4] Fridrich ,J, M. Goljan, and R. Du, "Detecting LSB steganography in color and grayscale images," IEEE

Multimedia Special Issue on Security, pp. 22–28, October-November 2001.
[5]. B. Ou, X. Li, Y. Zhao, R. Ni, and Y.-Q. Shi, "Pairwise prediction-error expansion for e cient reversible data hiding," IEEE Transactions on Image Processing, vol. 22, no. 12, pp. 5010–5021, 2013.
[6]. C. D. Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," IEEE Transactions on Multimedia, vol. 5, pp. 97–105, March 2003.
[7]. Dalal N. Hmood, Khamael A. Khudhiar and Mohammad S. Altaei (2012). A New Steganographic Method for Embedded Image In Audio File. International Journal of Computer Science and Security(IJCSS) 6(2): pp.135- 141.
[8]. D.R.DenslinBrabin and Dr.J.JebamalarTamilselvi. "Reversible data hiding: a survey," International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 3, May 2013
[9]. F. Willems, D. Maas, and T. Kalker, "Semantic lossless source coding," in Proc. 42nd Annu. Allerton Conf. Communication, Control and Computing, 2004.
[10]. H. S. Malvar and D. A. Florˆencio, "Improved spread spectrum: A new modulation technique for robust watermarking," IEEE transactions on signal processing, vol. 51, no. 4, pp. 898–905, 2003.
[11]. K. Wang, G. Lavou´e, F. Denis, and A. Baskurt, "Three-dimensional meshes watermarking: Review and attack-centric investigation," in International Workshop on Information Hiding, pp. 50–64, Springer, 2007.