SECURE COMMUNICATION USING AUDIO STEGANOGRAPHY - A SURVEY

Meghana K[1], Mehanaz[2], Mrs.Supriya A V[3]

[1]Meghana K,Information Science and Engineering, Srinivas Institute of Technology, Mangaluru, India
[2] Mehanaz, Information Science and Engineering, Srinivas Institute of Technology, Mangaluru, India
[3]Mrs.Supriya A V,Assistant Professor , Information Science and Engineering, Srinivas Institute of Technology, Mangaluru, India

---

Abstract - Steganography is the art and science of hiding messages in unsuspected multimedia data and is generally used in secret communication between two acknowledged parties. While sending data, there is always an issue with its security. Sensitive information can be hacked by a third party. Using steganography we can hide data bits in a cover file like an audio file. This paper reviews some important methods used for audio steganography. Also proposed method can be made to use AES algorithm for encryption and decryption as it very secure.

Key Words: AES Algorithm, Audio Steganography, Cryptography, Decryption, Encryption, LSB.

1.INTRODUCTION

In recent trends in the world, the communication is the basic necessity of every growing area. The growth of modern communication technologies imposes a special means of security mechanisms especially in case of data networks. Everyone wants the secrecy and safety of their communicating data. Information security is a major issue of concern while exchanging a data in an open network, as internet is not only a single network it is worldwide collection of loosely network. The network security is becoming more important as the volume of data being exchanged over the Internet increases day by day.

In this digital world the data security and data communication is changing and advancing day by day. The most excited thing is to know that the advancement in these fields had led to the improvement in secure data transmission. Broadband internet connections almost an errorless transmission of data helps people to distribute large multimedia files and makes identical data copies of them. Sending sensitive messages and files over the Internet are transmitted in an unsecured form but everyone has got something to keep in secret. The aim of steganography is to hide the secret data inside the cover medium without changing the overall quality of cover medium. In steganography actual information is not maintained in its original format but is converted in such a way that it can be hidden inside multimedia file e.g. image, video, audio.

2.Related work

In [1], A new method of audio steganography has been proposed by authors to increase the capacity of data embedding of carrier audio. This method hides the information in variable and multiple LSBs based on the MSBs of the samples of the carrier audio in comparison of standard LSB technique. Two MSBs of the samples of carrier audio file are checked in this method. The experimental results show that significant increase in carrier audio capacity for embedding additional information without having effects on the signal transparency of the host audio. Hidden data recovery without any error and no complicated calculations are the advantages of this proposed algorithm.

In [2], authors have proposed an algorithm which is composed of two variants of LSB technique of Audio steganography. The replacement of LSB is done at higher LSB layer i.e. 6th layer. The parity of samples of cover audio is checked along with secret message bit and accordingly LSB of sample is modified or unchanged. It also describes GUI application to hide data containing text in an audio file such that audio does not lose its original parameters. This method has advantages like, LSB at higher layer makes it undetectable and unsuspicious secondly capacity has increased since data is hidden at 6th layer and finally Parity method provides efficiency to algorithm since it reduces distortion due to noise and difficult to detect hidden text. The disadvantage is that it works only upon .wav files whereas this can be extended to other audio formats like .mp3, .au etc. Audio Processing can be used to reduce noise for more improved PSNR with data hiding.

In [3], a new method of using XORing of LSB's has been proposed by the authors. The basic idea of the paper is to present methods that hides information (audio, image and text) in cover audio using Least Significant Bit (LSB) coding method along with encryption so as to increase the security. In this method XOR operation is performed on the LSBs and

then depending on the result of XOR operation and the message bit to be embedded, the LSB of the sample is modified or kept unchanged. From experimental analysis, it is seen that the proposed methods are effective as no difference is found between the original audio signal and the stego audio signal from the listening tests.

In [4], the basic idea is to find the best way to embed text data in audio file using the steganography techniques. The proposed method uses LSB technique only in specific bit positions which are known only to sender and receiver. The results have shown that the quality of the audio remains same after embedding the secret text and also very less difference between the original audio and steganographed audio. The experimental results shown that the quality of the audio remains same after embedding the secret text and also very less difference between the original audio and steganography audio.

In [5], a new Steganography method based on Genetic algorithms has been proposed by authors to solve the two problems of less robustness against attacks and less robustness against distortion. Authors have provided two solutions respective to the problems. The solution to the first problem is provided by discovering which bites are embedded by modifying the bits else than LSBs in samples, and selecting the samples to modify privately-not all samples. The solution to the second problem is provided by embedding the message bits in deeper layers and other bits alteration to decrease the amount of the error.

In [6], author proposed a steganography technique for hiding digital data into digital audio files based on a random algorithm to select the carrier audio samples into which bits of the secret data are to be hidden. It uses two intermediates to transmit the secret data: The first intermediate is a carrier audio file embedding the actual secret data in the three LSBs of its audio samples. The second intermediate is a well-structured text that encodes the random locations of the carrier audio samples in the carrier audio file. The key advantage of the proposed technique is the use of two intermediates that complement each other to convey the secret information. As a result, the proposed technique is less susceptible to stego-attacks as third parties often assume that the secret data are hidden in one intermediate and not in two intermediates that together are needed to decode the secret data. In that sense, the sender can first send one of the intermediates, and then later on, send the other one, misleading eavesdroppers from the true location of the secret data. The second advantage is random selection of audio samples to hide the secret data; thus, making it irrecoverable and hard for unauthorized third parties to predict the location of the secret data and recover them.

The disadvantage is that they can make use of a semantic analyzer that would generate semantically structured English sentences using the presented context free grammar. Hence the intermediate text would be even less suspicious and more trusting while being transmitted.

In [7], the concept of cryptography and steganography are combined to perform a powerful encryption. In this paper authors proposed a novel approach where a duel encryption methodology has been implemented. In the first level of encryption a pattern matching algorithm has been employed to encrypt the text message in terms of their positional value. In second level, the conventional LSB method has been used to embed the positional value in the cover file. Such a duel encryption method will ensure data security in an efficient manner. The performance of the proposed method is evaluated in terms of means square error (MSE) and signal to noise ratio (SNR). The advantage is that the algorithm is highly efficient in terms of encryption and the capacity size of the text. The developed algorithm can be extended to have lesser bandwidth requirement by reducing the number of bits of the cover file. Different data compression algorithm can also be exposed to accommodate a large version of text into a cover file.

In [8], authors proposed and implemented an enhanced EMR information hiding system to protect medical records from unauthorized access in healthcare environment. The system combined NTRU cryptographic algorithm and LSB audio steganography to offer a more robust method for hiding the EMR secrete data from unauthorized access. The performance of the crypto-steganographic system was evaluated using Matlab environment. Evaluation of the performance showed little or no distortion to the sample audios after message embedment. The system could promote secure communication in healthcare systems, ensuring confidentiality, integrity, and availability.

The advantage is system is able to securely hide the medical records without causing significant distortions in the original audio. The disadvantage is that it could not consider other quantum-safe cryptographic schemes. This includes techniques based on lattice theory, coding theory, and multivariate quadratic polynomials.

In [9], a revision of the current standard of pairing process and formulation of a novel pairing structure based on steganography has been done. In this method, a key and secret message is embedded into an image, whereas a shared key will be generated to extract the secret message from the image. In this way, the pairing process will prevent any interception, because this technique utilizes the information of both the sender and receiver as well as steganography method. The advantage is method is very efficient and satisfies the requirements for security and robustness for secured pairing process.

In the future, proposed hybrid algorithm will merge three algorithms in order to present a robust security of data transmission in Bluetooth communication. This hybrid algorithm will be based on RSA (Rivest-Shamir-Adleman), AES (Advanced Encryption Standard), and TwoFish. In addition, an empirical model will be proposed in order to estimate the risk levels connected with MITM attacks. Positively, this contribution will provide an extra security layer to achieve a risk-free pairing. By adopting these ideas, there will be a remarkable protection against MITM attacks to guarantee a significant level of security for Bluetooth communications.

In [10], a new technique of LSB steganography has been proposed by considering LSB and MSB pixels for hiding and retrieval of the data which is an improvised version of one bit LSB technique. The effectiveness of the proposed method has been estimated by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR). In this paper, authors have investigated the problem of security in cloud computing, which is essentially a distributed storage system. To ensure the security of user data in cloud storage, authors proposed an effect and efficient stenographic strategy for enhancing security on data-at-rest. So, when these images are stored in the cloud data center, no one can view the original content of the data without any proper identification. Through detailed security and performance analysis, it has been seen that scheme almost guarantees the security of data when it is residing on the data center of any Cloud Service Provider (CSP).

3.METHODOLOGY

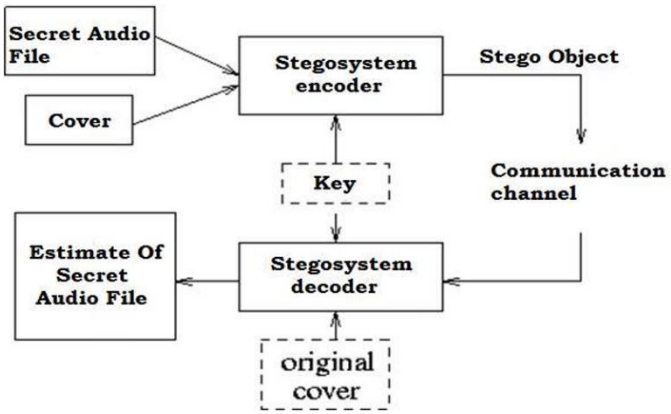

Fig -1: Block Diagram

Proposed method of steganography is shown in the Figure 1.In the transmitter's end a secret message is embedded to an innocent looking cover audio file and the resultant stego object which is visually same as the original cover is then transmitted over the communication channel without raising any suspicion in the minds of intermediate unintended sniffers/receivers.At the receiver's end the secret message is extracted by the authorized receiver using the extraction algorithm and a valid key. To make this process even more concealed and robust,the message is encrypted using the encryption technology before embedding and is also decrypted during the extraction to estimate the message in audio file.

3. CONCLUSIONS

Steganography helps in hiding secret information behind audio and image of video file by altering some components in the host or cover file. This paper provides a brief review of various techniques adopted for audio steganography in the past. Also a new method has been proposed.

In future, the steganography will become too advanced so that even a small messages inside the audio will be detected easily. Obtaining a steganography that satisfies both security and robustness is very difficult.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the support for this paper from Mrs.Supriya A V, Department of Information Science and Engineering, Srinivas Institute of Technology, Mangaluru, India and the anonymous reviewers of this paper.

REFERENCES

1. Mohsen Bazyar, Rubita Sudhirman, "A New Method to Increase the capacity of Audio Steganography Based on the LSB algorithm", Journal Teknologi Science and Engineering, 74:6 (2015), 49-53.

2. Jyoti Bahl, Dr. R. Ramakishore," Audio Steganography using Parity Method at higher LSB layer as a variant of LSB Technique", IJIRCCE-Vol. 3, Issue 7, July 2015.

3. H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale, "Information Hiding in Audio Signals", International Journal of Computer Applications (0975 – 8887) Volume 7– No.9, October 2010.

4. P. Rameshkumar, M. Monisha and B. Santhi,"Enhancement of Information Hiding in Audio Signals with Efficient LSB based Methods", Indian Journal of Science and Technology- Vol. 7(S4), 80–85, April 2014.

5.Mazdak Zamani, Azizah A. Manaf, Rabiah B. Ahmad, Akram M. Zeki, and Shahidan Abdullah, 'A GeneticAlgorithm-Based Approach for Audio Steganography" World Academy of Science, Engineering and Technology 54 2009

6. Youssef Bassil "A two Intermediates Audio Steganography Technque" Journal of Emerging Trends in Computing and Information Sciences (CIS), ISSN: 2079-8407, Vol. 3, No.11, November 2012.

7. Ratul Chowdhury , Debnath Bhattacharyya ,Samir Kumar Bandyopadhyay and Tai-hoon Kim "A View on LSB Based Audio Steganography" International Journal of Security and Its Applications Vol. 10, No. 2 2016.

8.Adamu Abdulkadir, Shafi'i Muhammad Abdulhamid, Oluwafem Osho, Ismaila Idris, John K Alhassan "Secure Electronic Medical

Records Transmission using NTRU Cryptosystem and LSB in Audio Steganography" 2018.

9. Marwan Ali Albahar, Olayemi Olawumi, Keijo Haataja, Pekka Toivanen "A Novel Method for Bluetooth Pairing using Steganography" International Journal on Information Technologies & Security,No 1 (vol. 9), 2017.

10. D.Suneetha, Dr. R. Kiran Kumar "A Novel Algorithm for Enhancing the Data Storage Security in Cloud through Steganography" Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 9 (2017) pp. 2737-2744.