Three Layer Data Hiding Using Audio Steganography

Nishu Gupta[1], Mrs.Shailja[2]

Student, CSE, CDLU, Sirsa, India [1]
Asst Professor, CSE, CDLU, Sirsa, India [2]

Abstract: This paper is about the study of cryptographic and steganography techniques and provides the approach of security with the combination of these techniques. The transmission of information need to be secure over the network and confidentiality of information is main aspect for the critical information. This paper proposed the multiple layer approach for security of information which includes the hashing, cryptographic steps and steganography techniques for encryption and hiding of data. For more security, the LSB technique has been considered with audio file for hiding of encrypted information. Hashing for maintain the confidentiality of information, cryptographic for encryption and then hiding in audio. Audio steganography requires a text or audio secret message to be embedded within a cover audio message. DES cryptographic algorithm has been used with Hashing algorithm. This Paper provides a new way of securing the information to avoid hassle in transmission over network.

Keywords: Steganography, Cryptography, Hashing, Audio, LSB.

I. INTRODUCTION

Security of information is crucial part of any organization and it provides confidentiality and authentication as well. The information should be hidden from intruder and by steganography techniques, the confidential information can be communicated over the network. The encrypted information can retrieve by cryptanalysis attack but on the contrary side, the hiding information difficult to retrieve.

Steganography or Stego as it is often referred to in the IT community, literally means, “Covered writing” which is a Word derived from the Greek language. In other words, Steganography is the technique of transmitting the hidden information. Steganography is a technique of hiding the data in Files such as Image, Audio, and Video etc over the Network. Cryptography technique scrambles messages, so it cannot be understood. Cryptography is the study of methods of sending messages in hidden form and by this; the planned recipients can remove the disguise and read the messages. Cryptography defines the arts and science of conversion of information into a particular order of bits and these are random and meaningless to a side observer or attackers. There are lot of security importance for secure information and stego for data hiding, it is easy to implement and on the contrary side, complex hardware, easy to detect cipher patterns. It hides information in digital images. Steganography techniques provide efficient security and less possibility of message detection. But on other side usability and communicating same media files such as image in repetition can produce dishonesty to the intruder and possibility of detect hidden information.

Audio Steganography is the technique of hiding data in Audio files such as e.g. wav file. The audio steganography technique is for embed the secret message in media file such as sound, Mp3 or Wav. This secure information is embed in such a way that the media file should be remain same as before and embedded by alteration the binary sequence of sound file. The examples of sound files are AU, WAV or MP3. This whole process for sound file is bit difficult than the embedding in digital images. There are different methods in securing the data in audio file.

1. Parity coding
2. Spread spectrum
3. Echo Coding
4. LSB Coding
5. Phase coding

In this paper, we used the LSB coding method which stands for the Least Significant Bit Encoding and it is the Sampling technique to convert the analog audio signal into digital binary sequence.

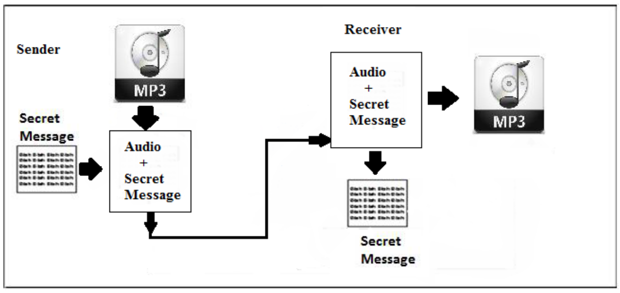

Fig 1 Graphical Representation of Audio Steganography

II. LITERATURE REVIEW

In today’s Research scenarios, there are many techniques, which have been discussed for security of the content. The data is converted in stegano-object, then communicated and on receiver side, this object is processed and retrieves the original information as described in the flowchart [5]. Author used two layers of security to secure the data. The Flow Diagram is described in which the data is to be decrypted, which has been embedded into the audio file. In next step, the Wave information and expected parameters is analyzed which includes the data-length, step-Size and frequency. Now, on receiver side, the de-steganography is need to be implement for extraction of cipher data and voice and this procedure will convert the cipher information in to original form [5]. The cryptography technique is for encryption and hiding of the information in any media file or plain file is Steganography [3].

In steganography, the possible cover carrier's are images, audio, video, text, or some other digitally representative code, which will hold the hidden information. A message can be information and it can be plaintext, hidden, image and it can be embedding in bit stream. Mutually, the wrap carrier and the embedded message create a stego-carrier. Hiding information may require a stego key which is additional secret information, such as a password, required for embedding the information [4].

The message hidden in the selected media is transmitted to recipient. At receiver end, reverse process is implemented to recover the original message. Author has described the different techniques for hiding the information [3].

The steganography algorithms tradeoffs are between the amount of covert information being embedded, called stego-data, and that the insurance for its presence to remain undetected. The recent advances allow more and more the use of advanced watermarking techniques to embed large amount of covert information that is also robust against removal and detection [4]. There are LSB audio steganography technique and RSA Cryptographic algorithm. Steganalysis is the techniques for hide the information and recover the information from image. The probability of matching data with an image data is less and attacker not able to identify the correct data and difficult to implement Steganalysis technique and for more security, firstly encrypt and then hide in image [1].

III. OBJECTIVES

In the research scenario, the different layer data securing technique will be implemented. These layers will secure the content from intruders. This technique will secure the confidential content over the network. These layers are described as:

1. First layer will convert the data using Hashing algorithm.
2. The output of the first step will be encrypted using cryptography technique
3. The outcome of these two layers will be embedded to Sound files.
4. These three layers will work fine from the sender side and sound file will be transmitted over the network.

This file again will be in process form receiver side for getting the right data.

IV. PROPOSED METHODOLOGY

The steganography and cryptography methods have been used for maintaining the security of the information over www. The intruder's can crack the information by cryptanalysis attack but in layered approach, it is difficult to retrieve, because it hides in some carrier. The combination of the techniques has been proposed for the better security of information. To maintain the confidentiality of the information, the hashing method has been proposed and verification receiver side as explained in diagram for sender as well as receiver.

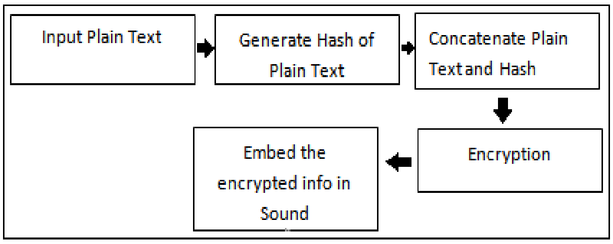
Input Plain Text
Generate Hash of Plain Text
Concatenate Plain Text and Hash
Encryption
Embed the encrypted info in Sound

Fig 2 Transmitter Block

In this, the sender having the plain text is transmitting information over the www with steganography and cryptography methods.

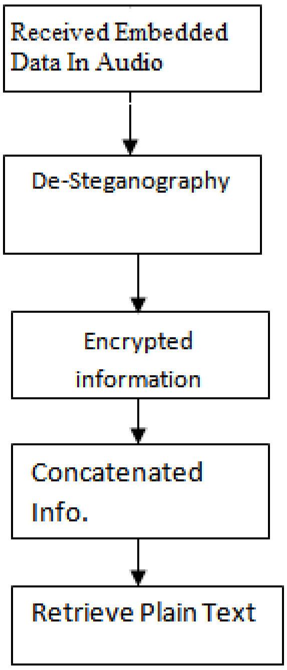

Fig 3 Receiver Block

V. APPLICATION

1. Confidential transmission and store protected data:

The confidentiality of the hidden and embedded data is the critical in transmission.

a. It provides the method to hide the confidential information.

b. Difficult to analyze the hidden information or embedded data and pattern.

c. Strengthen the secrecy of the cipher information.

2. Data Integrity Provision for assure and maintain accuracy.

3. Resource Protection using access control system for content sharing:

The information sharing over the network is common now days. The example can be of music industry which release the latest music albums and distribute over the network. In this scenario, the content is shared equally to the user and they can easily access it by accessing the particular page. The sharing cannot be to the specific user or to page requested user. So the information is hidden and publicizes it to the user which can be further transmitting to the customer either by E-mail service or by social web services.

4. Databases for Media Files

In this media Databases system, the problem is the separation of data from the media files such as image, sound, etc. There is need to associate the Media data such as picture, movie, etc with media database system. A photo picture, for instance, may have the following.

1. Time and Data of Picture Snapshot.
2. Electronic Devices information such as camera information.
3. The picture's information.

VI. CONCLUSION AND FUTURE WORK

In this paper, we have been proposed the security algorithm and methods which can be used for secure transmission of the information over the inter-network and intra-network. The proposed is not implemented yet.

The implementation part will be covered in the next paper, which will demonstrate the real working of proposed algorithm.

REFERNCES

[1] Juneja, M., Sandhu, P.S. (2009), "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", IEEE, Advances in Recent Technologies in Communication and Computing, 2009. International Conference on, pp.302 – 305.

[2] Arvind Kumar, Km. Pooja(2010), "Steganography- A Data Hiding Technique", Research paper, International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November.

[3] Sujay Narayana, Gaurav Prasad (2010), "Two new approaches for secured image Steganography using cryptographic Techniques and type conversions", International Journal (SIPIJ) Vol.1, No.2, December.

[4] Guizani, S., Nasser, N. (2012), "An audio/video crypto - Adaptive optical steganography technique". IEEE,Wireless Communications and Mobile Computing Conference (IWCMC), 8th International, 1057 – 1062.

[5] Tanmaiy G. Verma, Zohaib Hasan, Dr. Girish Verma(2013),"A Unique Approach for Data Hiding Using Audio Steganography",International Journal of Modern Engineering Research (IJMER) Vol. 3, Issue. 4, Jul - Aug. pp-2098-2101