ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

Multi-Part Data Hiding in Audio Steganography

Uma Mehta [1], Mr.Daulat Sihag [2]

Student, CSE, JCDMCOE, Sirsa, India [1]

Asst Professor, CSE, JCDMCOE, Sirsa, India [2]

Abstract: In the networking scenario, the information is shared among the users and this information should be confidential and authenticated to the receiver. The information should be kept in secure medium for protect from the intruders. So the data hiding technique should be used for keep the information available to the users.. The basic idea of proposed method is that the host signals (the sound wave cover media) undergoes pre-processing. The secret data is then hidden in a pre-processed fragmented sound wave using a traditional Steganography technique. The least significant-bit (LSB) based technique are very popular for Steganography in spatial domain. The simplest LSB technique simply replaces the LSB in the fragmented or multi-part audio file with the bits from secret information. The proposed methods offer high quality of Audio file with no loss of audio data. Only minor changes in the contents of the audio file occur, which are indiscernible to human ears. The algorithm has been proposed for Multi-part Data Hiding.

Keywords: Cryptography, Steganography, Multi-Part Audio, LSB, Hashing.

I. INTRODUCTION

In Today's Business Environment, the information is necessary part of an organization that should be secure and private for keep the information confidential. From the security aspects, the information should be available when required. Intruder can alter; remove the information which will be resulted of Information unavailability. From the security perspective, the information should not be readable by intruder and cryptography technique can convert the plain text to encrypted text. The encrypted information can decrypt the intruder by get the key information. The objective of Steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Steganography implies that the hiding of one kind of data into another data means encapsulation of information. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present.

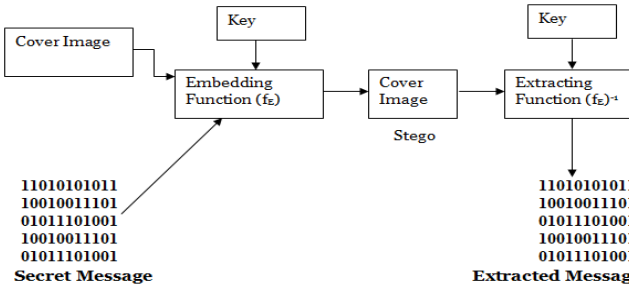

Fig 1 Graphical Representation of Steganography

Mainly because of their popularity on the Internet and the ease of use of the Steganography tools that use these data formats. These formats are also popular because of the relative ease by which redundant or noisy data can be removed from them and replaced with a hidden message. There are different types of Cryptographic Algorithms.

There are several ways of classifying cryptographic algorithms. Here they will be categorized based on the number of keys that are employed for encryption and decryption. The three types of algorithms are:

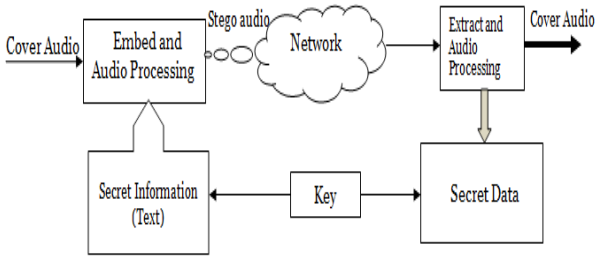

Fig 2 Audio Steganography Process

With secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

Audio Steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. It is the science of hiding some secret text or audio information in a host message. The host message before Steganography and stego message after Steganography have the same characteristics. Embedding secret messages in digital sound is a more difficult process. Varieties of techniques for embedding information in digital audio have been established. In a computer-based audio Steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio Steganography software can embed messages in WAV, AU, and even MP3 sound files. Embedding secret messages in digital sound is usually a more difficult process than embedding

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

messages in other media, such as digital images. There are different methods in securing the data in audio file.

II. LITERATURE REVIEW

Securing data is a challenging issue in today's era. Most of the data travel over the internet and it becomes difficult to make data secure. So Cryptography was introduced for making data secure. But alone cryptography cannot provide a better security approach because the scrambled message is still available to the eavesdropper. There arises a need of data hiding. So here author are using a combination of steganography and cryptography for improving the security. In this paper the author introduced two layers of security i.e. cryptography and steganography are used which makes it difficult to detect the presence of hidden message. But in some cases if the eve dropper has attacked the carrier of message then he will not be able to get the original message as all the relevant data here is in encrypted form. For cryptography Blowfish algorithm is used which is much better than AES and DES. In order to break blowfish algorithm he has to spend a lot of time and effort for trying several attacks and getting the original message. Although both of these techniques are easy to implement but there combination will provide much efficient and reliable security [1].

Author explained that in any network, the communication like Internet, there is need of data encryption technique to ensure information security. They explained that each type of data has its own inherent characteristics. Therefore, different encryption techniques should be used to protect the confidential data from unauthorized access. There are other areas also where image encryption techniques are proposed for security purpose. Author survey several image encryption techniques with their flaws and advantages; based on their survey, author also suggested some future suggestions of image encryption, which may provide better security enhancement in the case of various types of images. They also discuss about the chaos based crypto system for better analysis with data encryption standard (DES) encryption [3].

Author has assimilated the knowledge about data hiding techniques such as watermarking, steganography. They explained that the Data transmission needs security. Data hiding can be achieved through many methods. Different data hiding techniques are discussed in this paper which includes watermarking, steganography, fingerprinting, cryptography and digital signature. Since internet provides images, audio and video in digital form, distributing copies of copyright material are avoided by adding data hiding methods. The digital information such as images and videos are dominant in internet data hiding techniques are necessary. Many methods can be used for data hiding. Digital watermarking is the more secure method [4].

A rapid growth in E-Commerce market is seen in recent time throughout the world. With ever increasing popularity of online shopping, Debit or Credit card fraud and personal information security are major concerns for customers, merchants and banks specifically in the case of CNP (Card Not Present). This paper presents a new approach for providing limited information only that is necessary for fund transfer during online shopping thereby safeguarding customer data and increasing customer confidence and preventing identity theft. The method uses combined application of steganography and visual cryptography for this purpose [6]

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. Design/Modify an Algorithm by which Secret Data will be hidden in Audio Format.
2. MD5 Hashing of the information and integrate with Hashed Output.
3. Encrypt data before embed it into audio files to provide two layer security.
4. Design an algorithm to embed data in Multi-Part Audio Files.
5. Output Audio files will be more than one to improve security.
6. Size of output file should be less or equal in size without loss of Data.
7. Embedding data into the file does not alter the integrity of the file.
8. A software need to be designed to perform this task.
9. Perform different data hiding experiments to verify this technique.
10. Experimental results and provides a brief analysis of the application.

IV. PROPOSED METHODOLOGY

The algorithm design is for solving the problem in proper order to achieve the goal. To write a computer program, there is need to tell the computer, step by step, exactly what exactly the user want it to do. The computer then "executes" the program, following each step mechanically, to accomplish the end goal. It is the Procedure that produces the answer to a question or the solution to a problem in a finite number of steps. An algorithm that produces a yes or no answer is called a decision procedure; one that leads to a solution is a computation procedure. It is an effective method expressed as a finite list of well-defined instructions for calculating a function. The step by step procedure can be implemented with help of programming in any language. In our security scenario, the cryptography, Steganography, hashing with media files such as image and sound file has been considered. For effective results of this proposed work, the algorithm has been designed and explains the flow of security mechanism applied on sound file bit stream, hashed-Encrypted information with image Steganography and sound as well for keep the information hidden from the intruder.

V. APPLICATION

The majority of today's Steganography systems use multimedia objects like image, audio, video etc as cover media. In a computer-based audio steganography system,

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary

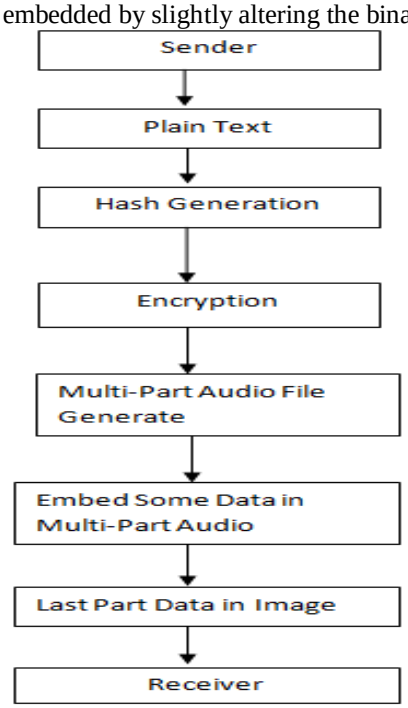

Fig 3 Flow Chart

of a sound file. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. These methods range from rather simple algorithms that insert information in the similar to watermarks on actual paper and are sometimes used as digital watermarks. We will split out output file in multiparts, So that all information should not be centralized. If the information carrier becomes corrupted or modified, all the secret data becomes irretrievable. Having the secret data residing in one location is prone to the threat of intrusion. If an attacker manages to get hold of the information carrier, revealing its contents becomes easy. This article proposes the use of a secret sharing scheme to address the mentioned weakness. The secret shared data is then hidden in audio files to increase the level of security. In two layer security, the data is not much secure because cipher text can be decrypt from the encrypted text by using the cryptanalysis technique. In network scenario, security of data and transmission is main aspect which cannot be handled by just encryption and stegano techniques and it is dangerous because information can reveal.

VI. CONCLUSION AND FUTURE WORK

The information security is the main goal of organization and it should be protected. The Storage of secret information is a constant security concern, and the reliability and integrity of this information is important. In the existing work, the problem with steganography and cryptography was the single location storage of all the secret data along with the all key information. This means, if the security breaches at single point, the complete data will loss. We have proposed a method for information security which hides the information in different parts of audio and also, the some part in image. The both media files have been jointly used for improve the security. The complete media files will be required to get the complete secured information and then cryptographic method will be used to decrypt the message and then hashing for identification of confidentiality of information.

REFERNCES

[1] Ajit Singh, Swati Malik(2013), "Securing Data by Using Cryptography with Steganography"
[2] Jagbir Singh, Savina Bansal, R.K. Bansal (2013), "Performance Analysis of Data Hiding Using Adjacent Pixel Difference Technique".
[3] Sonam Pathak, Rachana kamble(2013), "A Review: Chaotic System with DES (Data Encryption Standard) Image Encryption Technique".
[4] Dr.K.Sathiyasekar, S.Karthick Swathy Krishna K S (2014), "A Research Review On Different Data Hiding Techniques".
[5] Krati vyas1, B.L.Pal2 (2014) , "A Proposed Method in Image Steganography to Improve Image Quality with LSB Technique", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 1.
[6] Roy, S. (2014), "Online payment system using steganography and visual cryptography", Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE