STEGNOGRAPHY USING IN AUDIO FILES

Faiem Veg[1], Akshay Pathak[2], Veer Bhadra Pratap Singh [3]

[1] *Student, Information Technology, IMS Engineering College, Uttar Pradesh, INDIA*
[2]*Student, Information Technology, IMS Engineering College, Uttar Pradesh, INDIA*
[3]*Assistant Professor, Information Technology, IMS Engineering College, Uttar Pradesh, INDIA*

ABSTRACT

Today there is a huge demand for internet applications that require data to be transmitted in a more secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation. So the attractive solution for this problem is Steganography, which is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as audio, video or image file.

Keyword: - Cryptography, *Steganography, Audio Steganography.*

1. INTRODUCTION

Steganography is the art and science of covered writing (hide in plain sight) and its techniques are in use for more than years. Digital Steganography is the technique of securing digitized data by hiding it into another piece of data. Today, in the digital age the easy access to any form of data such as audio, videos, images and text make it vulnerable to many threats [1]. Text steganography can involve anything from changing the formatting of an existing text to changing words within a text to generating random character sequences or using context-free grammars to generate readable texts. With any of these methods, the common thing is that hidden messages are embedded in the character-based text.

1.1 Digital Data

The main task of the field of steganography is the storing, hiding, and embedding of secret data in all types of digital data. The main goal of steganography is to communicate securely in a completely undetectable manner [2].

1.2 Text Steganography

While there are various ways in which one may hide information in text, there is a specific set of techniques that uses the linguistic structure of a text as the space in which information is hidden. Text steganography uses text as the medium in which information can be hidden.

2. OBJECTIVE OF THE PROJECT

The application provides a friendly User Interface where the user had to specify just the required inputs (audio/image).After embedding or extracting the user can save /open the output of that particular operation according to their wish. To provide more security by avoiding an intruder to extract the embedded data a security key is used while embedding and extracting the message. The user should be an authorized one and are called authorized entity.

3. OVERVIEW OF AUDIO STEGANOGRAPHY

The word steganography comes from the Greek "Stegano", which means covered or secret and "graphy" mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding secret information in a cover file such that only sender and receiver can detect the existence of the secret information [3].

3.1 Secret Information

A secret information is encoded in a manner such that the very existence of the information is concealed. The main goal of steganography is to communicate securely in a completely undetectable manner [4] and to avoid drawing suspicion to the transmission of a hidden data [5].

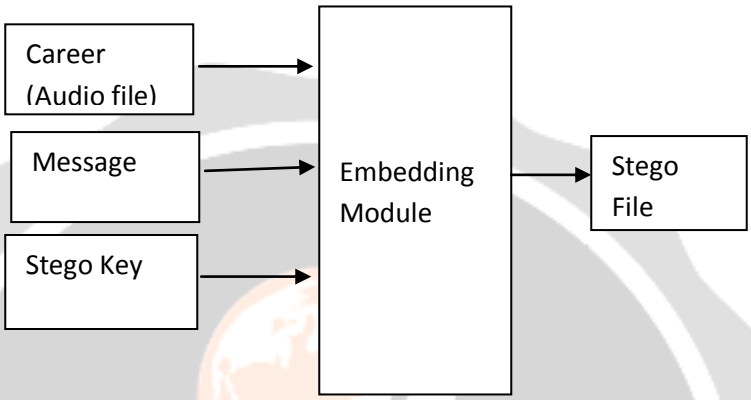

Fig -1: Basic Audio Steganographic model.

It does not only prevent others from knowing the hidden information, but it also prevents others from thinking that the information even exists. If a steganography method causes someone to suspect there is a secret information in a carrier medium, then the method has failed [6,7]. The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information. Basically, the model for steganography is shown in **Fig1**. A message is a data that the sender wishes to remain it confidential. A message can be plain text, image, audio or any type of file. The password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file [10].

3.2 Information Hiding process

The information hiding process consists of following two steps [8,9].

i. Identification of redundant bits in a cover-file. Redundant bits are those bits that can be modified without corrupting the quality or destroying the integrity of the cover-file.

ii. To embed the secret information in the cover file, the redundant bits in the cover file is replaced by the bits of the secret information.

3.3 Proposed Architecture and work

There are many algorithms developed for image steganography. Meanwhile, the interest in using audio data as the cover object in steganography is more reliable than image data. This paper describes the implementation of steganography in audio data using direct sequence spread spectrum method. This can be applied to embed a message in audio/video data & to send the hidden message through radio waves. Spread Spectrum method is known very robust, but it is expensive, the implementation is comparatively complex and the information capacity is very limited. Perfect audio steganographic techniques aim at embedding data in a robust way and then extracting it by authorized people. Hence the main challenge in digital audio steganography is to obtain robust high capacity steganographic systems. In this paper, a current state of art literature in digital audio steganography is presented. The potentials and limitations have been identified to ensure secure communication and a new idea is in this we can send the key to the recipients directly with the help of text messages for security purpose.

This system is based on steganography for security purpose. So we are using the algorithm and the necessary step. The technology which will be used in this system is JAVA and ANDROID. The JAVA technology will be used for providing platform independence to the application and for doing the bit level calculations in the modules. The ANDROID technology would be used to build modules which will be meant for development of the application.

In Fig2 describes the basic working of how the actual process is been takes place in the application. First, the plain text will be encrypted with encryption key k1. This plain text will be converted into ciphertext which will go for the further process that is decryption which will be done at an end user side. For decryption, a decryption key K2 will be used and with the help of that key, the end user can get his desired output that is plain text.

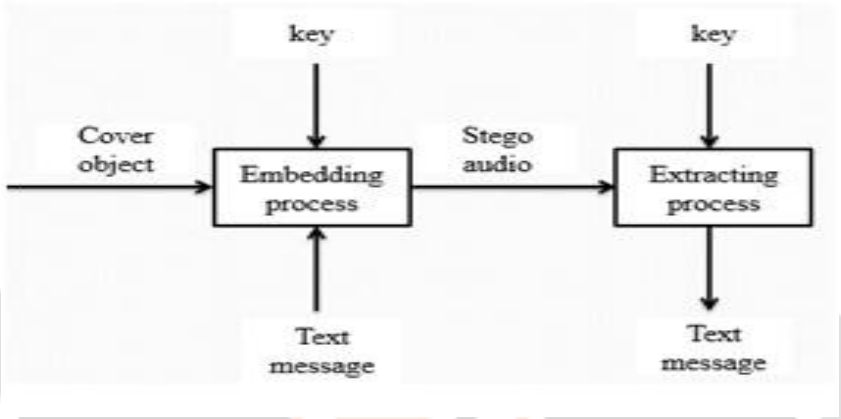

Fig2: Steganography in Audio File

3.4 Result Analysis

This system has a high steganographic capacity. The algorithm helps to prevent visual attacks. The user will communicate more securely then existing available software. This project provides the safe & secure way for data transmission like text transmission which will be helpful to the users. This application will be useful in various fields like e-shopping, email etc. It will be also helpful for the military purpose for secret data transmission. Use of this application is one can send the message more secretly with the fewer chances of data loss.

3.5 Audio Steganography Application

In this type of steganography method, we can embed secret messages into digital sound in audio steganography. It is the more complex process as compare to embedding messages in other media. This steganography method can embed messages in WAV, AU And even MP3 sound files [11]. In the business world, Audio data hiding can be used to hide a secret chemical formula or plans for a new invention. Audio data hiding can also be used in the non-commercial sector to hide information that someone wants to keep private. Terrorists can also use Audio data hiding to keep their communications secret and to coordinate attacks. Data hiding in video and audio is of interest for the protection of copyrighted digital media, and to the government for information systems security and for communications. It can also be used in forensic applications for inserting hidden data into audio files for the authentication of spoken words and other sounds, and in the music business for the monitoring of the songs over broadcast radio.

4. CONCLUSIONS

This system provides a good, efficient method for hiding the data from hackers and sent to the destination in a secure manner. This system maintains the size of the file even after encoding and also suitable for any type of audio/video file format. Encryption and Decryption techniques have been used to make the security system robust.

Thus this method provides a more reliable way for secure communication and helps to achieve high capacity robust steganography system. The main goal is to provide high security. It decreases the number of changes which are necessary for message hiding.

5. REFERENCES

[1]. Artz, Donovan. "Digital steganography: hiding data within data." internet computing, IEEE 5.3 (2001): 75-80.

[2]. Amin, Muhalim Mohamed, et al. "Information hiding using steganography." Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on. IEEE, 2003.

[3]. Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

[4]. Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[5]. Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.

[6]. Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[7]. Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.

[8]. Spector, A. Z. 1989. Achieving application requirements In Distributed Systems, S. Mullender.

[9]. Amin, M. M. Salleh, M.Ibrahim, S.et.al, Information Hiding using Steganography, 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, IEEE, Oct 2012.

[10]. Nedeljko Cvej, "Algorithms for audio watermarking and steganography", Oulu 2004, ISBN: 9514273842.

[11]. Prof. Samir Kumar, Bandyopadhyay Barnali, Gupta Banik," LSB Modification and Phase encoding Technique of Audio Steganography Revisited". Vol(4) IJARCCE 2012.