Multi Agent Based Audio Steganography

T. Kartheeswaran
Department of Computer Science and Technology
Uva Wellassa University
Badulla, Sri Lanka
tkarthees@gmail.com

V.Senthooran , T D D L Pemadasa
Department of Physical Science
Vavuniya Campus, University of Jaffna
Vavuniya, Sri Lanka
senthooran@mail.vau.jfn.ac.lk

Abstract*— Today's Information Technology grows rapidly with new technologies and need more security for the data transmission over the internet. Steganography is one of the solutions to ensure the data secure over the internet. An audio steganography is a method to transfer concealed information by changing the cover audio file without degrading the quality of the original file. The cover medium before steganography and stego medium after steganography should have the same characteristics of a good steganographic system. The Agent technology involves distributing the services with flexible manner. As most of the applications are created as services in present computing scenario and data security also can be served as a service. Agent-based steganography will improve the efficiency of the secure steganographic system and it will be more convenient in terms of flexibility and availability. In this research paper, we present a trusted communication platform for multi-agents that are able to hide the confidential message in the cover audio stream according to the user request and retrieve the hidden information from the stego audio file. This system provides high availability and flexibility in this context and a more feasible way to trust the message transmission. This work is currently being done and designing part of this work has been done successfully with satisfied results.

Keywords*— Multi Agent System, Audio steganography, Software agents, Least significant method, Stego-Agent

I. INTRODUCTION

In the modern world of data communication, we regularly observe a popular activity termed "Data Hacking". Data hacking is the process called as an illegal admission of data hackers during the data transmission. In the field of steganography, this process is called as steganalysis that is a method in which a steganalyser hack the covered file to receive the concealed information [1]. At present, the most of the steganographic techniques use multimedia elements such as video, image, and audio as the covering medium to conceal the confidential message because those are frequently transferred through the emails and another internet of things. In audio steganographic techniques, confidential messages are hidden in the digital sound file that supports WAV, AU, MP3 and other various formats. The confidential message is concealed by slightly changing the format of an audio file into binary [2]. It is harder to embed data bits in the sound clip than a trick to embed data bits in another medium, such as videos and digital images [2]. To facilitate successful data embedding in the sound file, so many data hiding techniques in the audio file have been developed by several researchers in the literature [3, 5, 7, 8]. The audio steganography is an emerging and growing technique to secure transform of data in an efficient manner.

Using this, we can hide the information without making the significant human detectable difference in the audio file. It's a more difficult process to hide some message in the audio file without making significant changes. There are several techniques available for audio steganography such as Echo, the Least Significant Bit (LSB) and temporal hiding. The LSB is simple and secure compared to other techniques. Application of Audio steganography through agent technology will be an efficient application of the agent-based approach. The goal of steganography is for sending a message through an insecure medium.

In audio Stenographic techniques, the limitation of the human hearing system should be considered while hiding the data in the audio file [2]. Though, hiding confidential message bits in the audio file is typically complicated process, then hiding data bits in another medium is visually noticeable. Stego audio file with hidden information will be protected from fewer steganalysis approaches that attack the audio file during the transmission. In addition, usual understanding and complexity with working an audio file and improved techniques related to audio steganography are required. All these techniques compact with a small number of steganographic techniques that depend on the dissimilarity of the audio file that used as a cover medium. It yields that the cover audio will be used to conceal the data bits as carrier object. Audio Stenography impacts the role of many applications that are digital watermarking, covert communication and access control [3].

Any audio steganographic system should have the some special characteristics: It measures the perceptible distortion as a result of cover audio file alteration that is made by data embedding or hackers attacking during the transmission. The perceptual quality is determined by measuring the distortion for stego audio file. The robustness of the system are measured and it will enable the ability of the hidden message bits owing to various attacks made by the hackers during the transmission. Unplanned hits generally consist of ordinary data manipulation techniques. Those are resampling and re-quantization. On purpose, attacks contain an accumulation of noise, resizing techniques, etc. [4]. The third is the data hiding rate (embedding capacity): It is the amount of confidential message bits that can be utilized by the data hiding scheme without perceptual distortion. The number of hidden bits per pixel is the bit rate of the confidential message or transformed coefficients within a stipulated time period and is often measured by bits per second (bps) [4]. In the present computing scenario, we are entering the enlargement of distributed systems services. The

978-1-4799-7849-6/15/$31.00 ©2015 IEEE