World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 5, No. 5, 87-91, 2015

Mobile Secure Transmission Method Based on Audio Steganography

Alaa Alhamami, Avan Sabah Hamdi
Amman Arab University
Amman, Jordan

Abstract — Multi-media is one type of transferring data through the Internet, and this process becomes one of the most important types of threatened data. The threat can occur by listening or sniffing the data without giving any notice to the two parties. Therefore, we will find a specific solution to maintain the security of audio during the process of transferring between the two Mobiles. Although, there are many methods to provide secure transferring, the steganography is the best way to hide the audio inside another audio and it is the best solution to reduce the risk of intruders.

The Least Significant Bit method is used in this research. The proposed algorithm and method have been used by applying two mobiles that support the android operating system, and then we choose the Skype program as a host program. The main goal of using the host program is for transmitting the audio between two devices and each device located on separate network.

Keywords- Steganography; Threat; Skype; Least Significant Bit; Android Operating system; Audio.

I. INTRODUCTION

The rapid development of the broadband communication networks and multimedia data available in a digital format opened many challenges and opportunities for securing data transmission. Explosive growth of using audio data on the Internet today, should be taking audio as a carrier for information hiding, it is called Audio Steganography [1].

The main goal of steganography is to escape detection of secret message and its uses in different form generally digital form of steganography are used for communication over the internet. Steganography can be useful when the use of cryptography is illegal: where cryptography and strong encryption are banned, steganography can evade such policies to pass message covertly and Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text etc.) with bits of different, invisible information.

The sound files may be modified in such a way that they contain hidden information, these modifications must be done in such a way that it should be impossible for a pirate to remove it, at least not without destroying the original signal [2, 3]. The Internet provides various audio applications like voice query, voice activated websites, etc. On the Internet, the Windows Audio Visual (WAV), Audio Interchange File Format (AIFF) and motion picture experts group layer III (MP3) files support a data rate varying from 8 kbps to 44.1 k bps. Audio traffic on the Internet system is increasing rapidly, that's why it is obvious to choose an audio file as a cover media [4].

II. MOBILE SECURITY

Mobile devices are being widely used by the people, they are more than just phones; they are a lifeline to the outdoor world, entertainment platform, GPS system, a little black book and a shopping and banking tool. It is given the developments in hardware and software, mobile phones uses have been expanded to send messages, check emails, store contacts, store important dates, just to mention a few uses.

Portable communication is very much vulnerable to security than wired networks, the Mobile connectivity options have also increased. After standard GSM connections, mobile phones now have 3G, 4G and WLAN connectivity. Those meaning the mobile users send and receive data packets wirelessly. So that security mobile services are needed for authentication, integrity, user privacy and non- repudiation, and it can be used by a hacker as an access point into many other aspects of your digital life as well the lives of others in your network, making mobile security about more than just protecting your phone.

III. LEAST SIGNIFICANT BIT (LSB)

There are many methods used in steganography, but the popular used method in general is the Least Significant Bit (LSB). This method replaces the least significant bit in some

bytes of the cover file to hide a sequence of bytes containing the hidden data. In computing, LSB is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position. Data hiding in the Least Significant Bits (LSBs) of audio samples in the time domain is one of the simplest algorithms with very high data rate of additional information [7, 9].

One trivial technique is to start at the beginning of the sound file and perform LSB coding until the message has been completely embedded, leaving the remaining samples unchanged. This creates a security problem, however in that the first part of the sound file will have different statistical properties than the second part of the sound file that was not modified. One solution to this problem is to pad the secret message with random bits so that the length of the message is equal to the total number of samples [10].

IV. STATEMENT OF PROBLEM

The Internet server is providing virtual channel and not actual one for the transmission between parties, and this channel is change with each connection. The intruder is use the channel to find a suitable way to access the data, so the transfer process is securely weak and threat from intruder is possible, and we must find methods to reduce the risks that are difficult to be removed.

Host program used for the transmitter and receiver between devices in sites and networks are similar or different, and these programs found in the new generation of mobile like Skype, Whatsapp, ChatOn, Tango and etc. These programs cannot depend on existing security because they are dealing with traditional methods to provide the security, they need new method to provide more security like using steganography to transmit file in secret media. In this paper, we use Skype to transfer cover audio embedded secret audio, and we design model to hide audio in audio to provide the security of the data by using Least Significant Bit (LSB) method in the steganography. Figure 1 shows the steps of the proposed model. Figure 2 shows the used method.

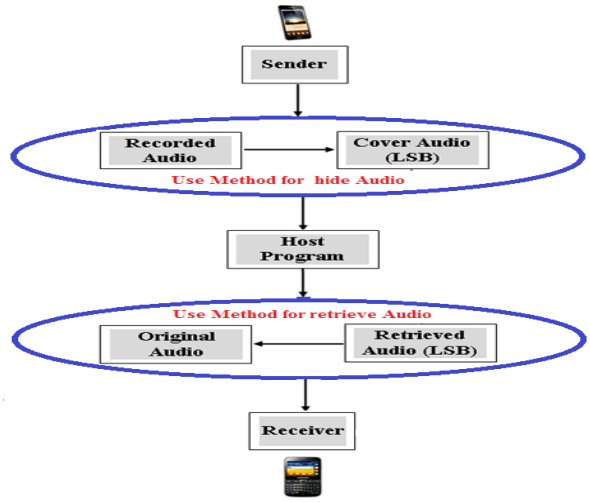

Figure 1 Steps of the Model

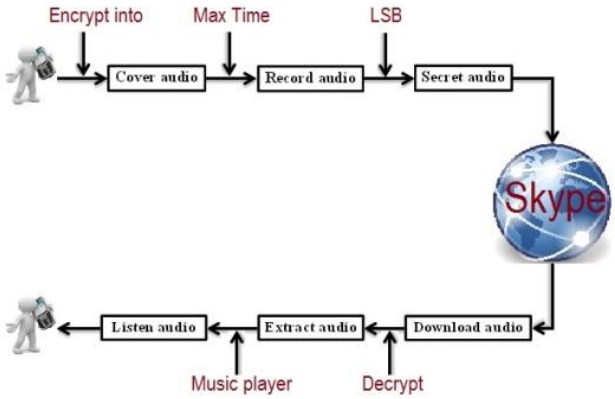

Figure 2. Suggested Method model

V. THE PROPOSED MODEL

Data transmission is one of the most important fields for the security techniques and many problems begun to appear, because the transmission in public communication system is not secured and the data to be transmitted requires secured channel to prevent unauthorized user from viewing or altering the data.

Voice transmission represents one type of data. Thus, we need a method which not only prevents others from knowing the hidden information, but also prevents them from thinking they exist of information that takes a lot of time to transfer.

Figure 3 shows the proposed model and the main steps in each procedure.

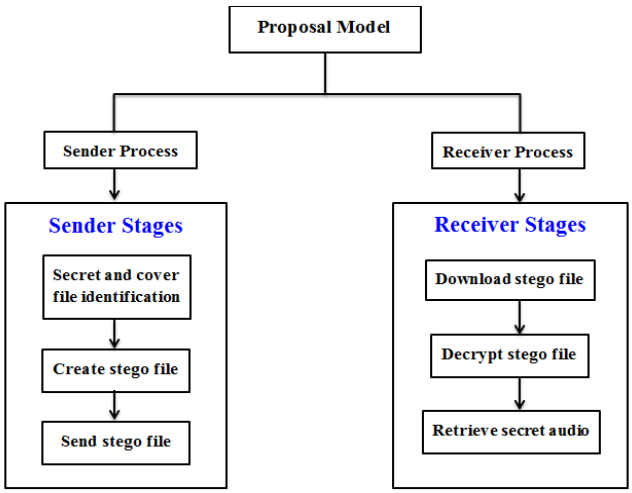

Figure 3. proposed model

A. *Sender procedure*

The first procedure is declared all the steps accrued in the part of sender, these steps will begin from identifying secret and cover audio to transfer complete of stego file by host program. This procedure includes three stages:-

- Secret and cover file identification.
- Create stego file.
- Send stego file.

1) *Secret and cover file identification*

The user is start use the application when the Icon application and selection (Encrypt into) button has been chosen, after that it will open browser to show set of audios that are stored previously in the phone's memory and it appears WAV type only without other types of audio. The user chooses one of these audios to be a cover, then the application will display notification to identify the period of time that can be used to record secret audio, the user is being process record for secret audio through pressing on the record button.

2) *Create stego file*

This step includes hide the record audio (secret audio) inside the cover audio by using LSB, i.e., that is dealing with the least significant bit from the cover, usually the last bit, and exploited to put bits of secret audio inside cover audio. This step include Encrypt-LSB algorithm:-

- *Encrypt Algorithm:-*

The work of this algorithm is to hide the secret audio inside the cover audio, the first step of the algorithm is checking the size of the cover, the cover size should be eight doubles of the secret size, addition to (88) bits as shown in Algorithm 1.

Algorithm (1):

// Input: secret and cover audio.

// Output: stego audio.

- Get the Cover and the secret audio
- Check the size of the cover and the Secret
- Compare between the two sizes
- Embed the Secret inside the Cover
- End

3) *Send Stego. Audio*

The secret audio is hidden inside the cover audio to produces stego audio, the application is activated by the icon used to the user to choose one type of the host programs for sending stego audio to the second party (receiver), where the sender selects user-name to the receiver through the host program is sending stego audio for the receiver as attachment.

B. *Receiver procedure*

The second procedure is declared all the steps accrued in the part of receiver, these steps will begin from receive the stego audio to retrieve secret audio, this procedure includes three stages:-

- Download stego audio.
- Decrypt stego audio.
- Retrieve secret audio.

1) *Download stego audio*

The second party is receiving the stego audio; it will load directly by the host program and stored it in the device. When the user log-in to the application, the notification is appearing to the user for existence of hidden audio and gives path of stego in the device.

2) *Decrypt stego audio*

When press on the stego path, this step is begin which include decrypt hidden and separated between the cover and secret audio, by retrieve the least significant bit from stego in each byte to produce the secret audio, and retrieve the other bytes to produce the cover audio. This step include Decrypt-LSB algorithm:-

- *Decrypt Algorithm:-*

The work of this algorithm is separated between cover and secret audio, the first step of the algorithm is checking exist the " encoded " word in the input audio, to ensure the audio is stego or not.

Algorithm (2)

// Input: - Stego audio.

Output: - Secret audio. //

- Get stego Audio

- Take 7 bytes from stego

- Retrieve 4 bytes

- Use LSB for Decryption

- End

3) Retrieve secret audio

This application is retrieving the secret audio from the previous algorithm, the type of this audio is WAV as recorded during the sender part and the receiver can listen to the audio by any program of the music player.

To increase the security in our model, the secret audio should be saved in receiver device as stego not as original form, and when the receiver wants to listen to the secret audio again should use the same application.

C. Limitation

We implemented our application between two devices that support the android operating system, and we choose the Skype program as a host program. We choose the Skype program for many reasons:-

- Can transfer audio file without any concerning about the size or type of the audio.
- Easy use and user friendly.
- Available in many devices and used in any operating system.

For the other types of the host programs that support different media transmission, but do not support attach file, such that:-

- Whatsapp: - This program supports all kinds of media transmission in general, in audio transmission of specific, before sending audio, the program will compress audio and convert it to standard form.
- Viber & Tango: - these programs support sending photo and video from library.
- Vonago: - this program supports image and direct record audio.

VI. CONCLUSION

In this paper, we are dealing with LSB method to hide secret audio in another audio for protection audio from any threats, the function of this method is hide each bit from secret audio in to the last bit per byte from cover audio to produce the stego audio. Then transfer the stego audio to another party by using android mobile through using one type of the host program.

In the end, there are two important points listed as the following:

1. We deal with the audio that WAV extension rather than other types of audio extension; because WAV extension contains original audio without any additions. While the other type of audios, like MP3, contains Compression audio that can be returned original audio.
2. We choose the Skype program as a host program to transfer audio for many reasons: (1) it can transfer audio file without concerning about the size or type of the audio, (2) it is easy to be used and friendly (3) it is available in many devices and can be used in any operating system, While the other types of the host programs support different media transmission, but they do not support attach file.

REFERENCES

1. Ashraf Seleym and Dina Darwish. “Real-time Covert Communications Channel for Audio Signals”, International Journal of Computer Science Issues, Vol. 9, Issue. 5, No. 3, 2012.
2. JayeetaMajumder and SwetaMangal. "An Overview of Image Steganography using LSB Technique" International Journal of Computer Applications,**Issue** 3, pp.10-13, 2012.
3. KritiSaroha and Pradeep Kumar Singh. "A Variant of LSB Steganography for Hiding Images in Audio". International Journal of Computer Applications, Vol. 11, No.6. , 2010.
4. Stefan Certic “The Future of Mobile Security “, http://www.cs-networks.net, access by August 2013.
5. Jayaram P., Ranganatha H. R., Anupama H. S. "Information Hiding Using Audio Steganography – A Survey". The International Journal of Multimedia and Its Applications, Vol.3, No.3, 2010.
6. ZaidoonKh. AL-Ani, A.A.Zaidan, B.B.Zaidan, HamdanO.Alanazi. "Overview: Main Fundamentals for Steganography". Journal of Computing, Vol. 2, Issue 3, 2010.
7. Ajay.B. Gadicha. "Audio Wave Steganography". International Journal of Soft Computing and Engineering, Vol. 1, Issue 5, 2011.
8. Jisna Antony, Sobin c. c, Sherly A. P. “Audio Steganography in Wavelet Domain – A Survey”, International Journal of Computer Applications, Vol.52, No.13, 2012.
9. Souvik Bhattacharyya and GautamSanyal. “Audio Steganalysis of LSB Audio Using Moments and Multiple Regression Model”, International Journal of Advances in Engineering and Technology, Vol. 3, Issue 1, pp. 145-160, 2012.
10. Pratap Chandra Mandal. "Modern Steganographic technique: A survey". International Journal of Computer Science and Engineering Technology, Vol. 3, No. 9, 2012.

AUTHORS PROFILE

Prof. Dr. Alaa Hussein Al-Hamami, Dean of Computer Sciences and Informatics College, Amman Arab University

Alaa Al-Hamami is presently Professor of Database Security and Dean of Computer Sciences and Informatics College, Amman Arab University, Jordan. He is a reviewer for several National and International journals and a keynote speaker for many conferences. He is supervising more than Twenty PhD, more than sixty MSc, and many Diploma thesis. His research is focused on Distributed Databases, Data warehouse, Data Mining, Cryptography, Steganography, Cloud

Computing, Big Data and Network Security. Dr. Al-Hamami published Seventeen Books in Computer Philosophy and other Computer topics in addition to several chapters in IGI and Springer publications. He is Chief Editor and Editor for several Magazines in addition to his participation in project research evaluations.

Avan Sabah Hamdi
Master Degree of science in Computer Science
College of Computer Sciences and Informatics
Amman Arab University