IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 6, Dec-Jan, 2015
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Location Based Steganography On Mobile Smartphone Using Android Platform

Ms. Khushali Pandit[1], Ms. Varsha Bhosale[2]

[1] **Student, Vidyalankar Institute of Technology, Wadala, Mumbai.**
[2]**Lecturer, Vidyalankar Institute of Technology, Wadala, Mumbai.**

Abstract:

Steganography mechanism consists of audio files as the cover signal to hide the sensitive data in it. The application is developed on the Android platform using its IDE (Integrated Development Environment) provided by Eclipse. The covert nature is the desirable feature denies an unauthorized user from mining sensitive information or claiming the ownership of music in case of water-mark embedding. The purpose of this project is to implement the tool which will embed a secret message in a cover message (such as an audio recording) and provide the highly private and secure data transfer without third party intervention. Applications of steganography include protection against detection (data hiding) & protection against removal (watermarking) that seem to hold promise for copyright protection, tracing source of illegal copies, etc. Basically location is being considered for more security of data and tracking through GPS.

Keywords: Steganography, cover signal, secret message, Location, Android platform.

1. Introduction

Steganography is a means or a tool through which digital media can be manipulated in a way which the user requires through a very high level of security. In this the message is totally secure and can be accessed only by the person who has authorization through authenticate passwords or keywords. Steganography blankets the entire communication which is being taken place to the outside world. Hence, this is a type of communication in which exchange of information between any two parties which is to be kept confidential.

The project is based on providing a highly private and secure data transfer without the intervention, disturbance, disruption of anyone else except sender and receiver. The concept of this project is that the secret data to be hidden will be accepted from the user and will be encrypted and then embedded into the carrier file after performing suitable transformations. This will in turn make it difficult for the intruder to detect presence of any kind of data. Only the intended recipient will be able to retrieve the data with proper authorization of authenticate password.

1.1 Securing Data:

Many techniques suffice the entrenchment of information in a digital audio file. The binary message that has to be hidden, substitutes the bits of each sampling point. Firstly, the cover audio is taken and the message is embedded in it. The message is encrypted so that no other person than the desired recipient can receive the sent information. The information hiding at the transmitter side is shown in figure 1

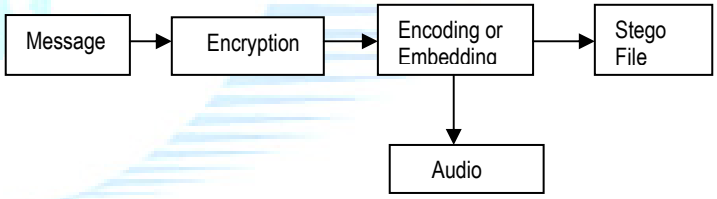

Figure 1: Information hiding at the Transmitter side.

At the receiver, figure 2 the decryption of the message takes place with help of the key which is available only with the recipient. Here the quality of plays a vital role, as it decides whether the file has been tampered or not. The three pillars of steganography are Confidentiality, Integrity and Unremovability which is inevitable to make the system full fledge protected.

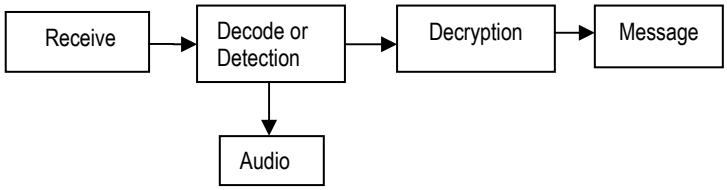

Figure 2: Information hiding at the Receiving side.

2. Existing Method:

To hide the messages from the intruders to hide the messages audio cover files are used in various steganography. Fever amount of data can be used as cover files are audio. If too much data embed in the cover file then it is easily detected. And if we increased the size of the message to store the more data then such messages as falls in suspect of hackers. Also there are some problems with existing system as reported. Even the audio file gets distorted. Noise gets added to the signal. There is neither security of login and password nor location security in the existing system. Least Significant bit (LSB) coding is used to embed files in digital audio file. Alternate LSB coding, the alternate layer is selected and according to that the message would be replaced.

2.1 Material and methodology:

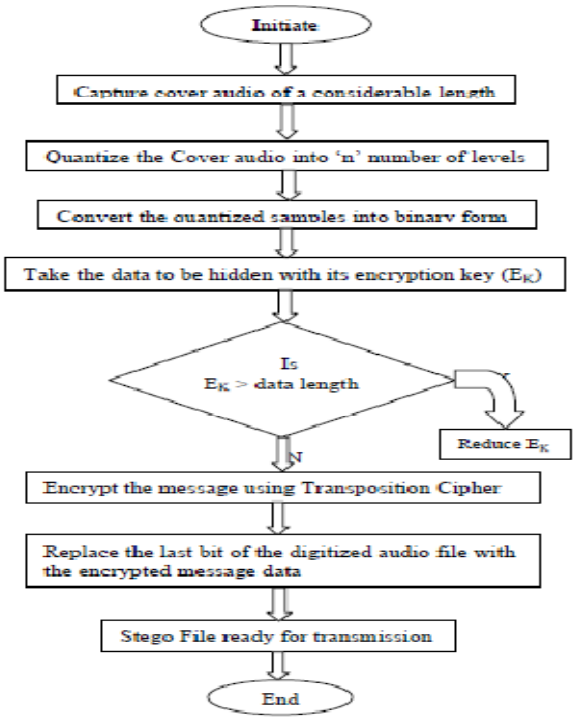

Figure 3: Flow chart representing the sequential steps involves in the LSB hiding technique.

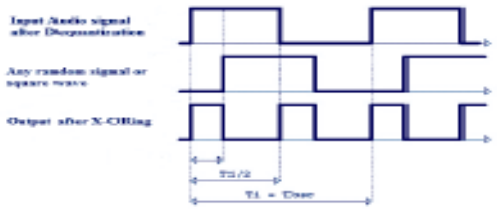

Figure 4: Direct Sequence Spread spectrum using X - ORing

1. **Click on stego app**
2. Record voice input

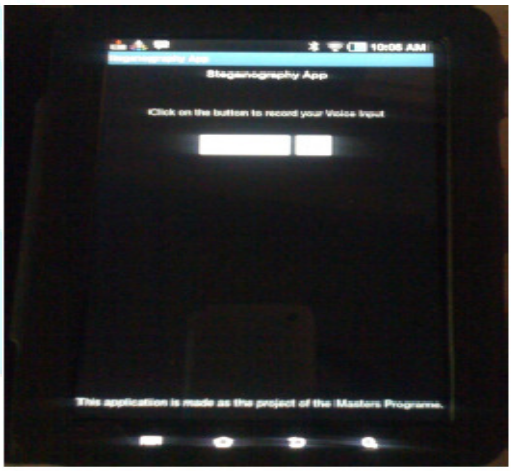

Figure 5: voice input

3. Encode encrypted file into original file.

Figure 6: Android Emulator showing application of Steganography.

4. Decode the encrypted file from the original file.

4. Proposed Method :

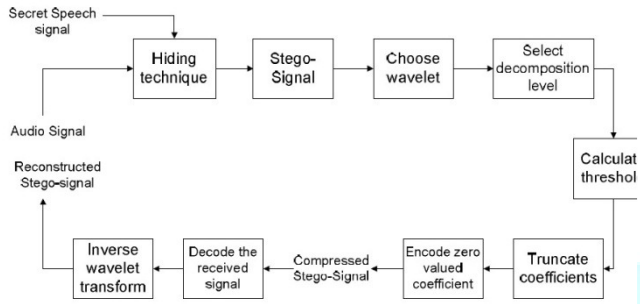

Figure 7: Flow of the complete system

Steganography Algorithm:

- Audio Steganography Coding Using the Discrete Wavelet Transforms.
- Wavelets to be used **(Haar, Daubechies)**. Selected on basis of Energy the wavelet signal can concentrate.

Wavelet transforms Algorithm:

Message is embedded into cover image by modulating the original coefficients in transform domain such as Discrete Cosine Transform or Wavelet transform. The wavelet transform transforms the signal from the time domain to the wavelet domain. This new domain contains more complicated basis functions called wavelets, mother wavelets or analyzing wavelets. The fundamental idea behind wavelets is to analyze the behavior of the signal with respect to scale. Any signal can then be represented by translated and scaled versions of the mother wavelet. Wavelet analysis is capable of enlightening aspects of data that other signal analysis techniques are unable to perform, aspects like trends, discontinuities in higher derivatives, breakdown points and self-similarity. The basic idea of DWT for one-dimensional signals is shortly described. The wavelet analysis enables splitting a signal in two parts, usually the high frequencies and the low frequencies part. This process is called decomposition. The edge components of the signal are largely limited to the high frequencies part. The signal goes through series of high pass filters to analyze the high frequencies, and goes through series of low pass filters to analyze the low frequencies. Filters of different cutoff frequencies are used to analyze the signal at different resolutions.

Android:

Android is open source and Google releases the code under the Apache License. This open-source code and permissive licensing allows the software to be freely modified and distributed by device manufacturers. Additionally, Android has a large community of developers writing applications ("apps") that extend the functionality of devices, written primarily in a customized version of the Java programming language.

3.1 Material & Methodology:

1. Click on stego app enter the login id and password

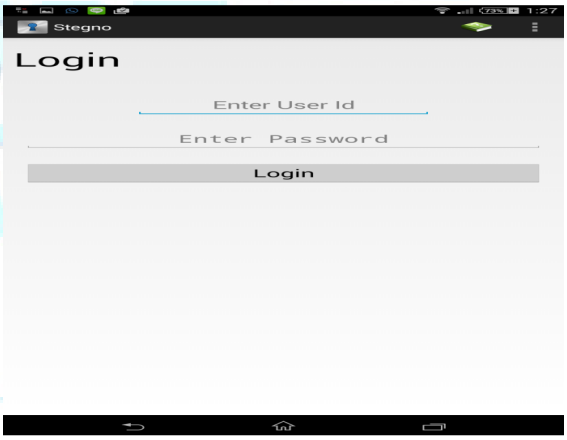

Figure 8: Login id and password

2. Steganography:

Figure 9: Encryption

- User will record the file and select another audio file.
- User will enter key for security.

Figure 10: encrypted speech recording, cover audio file and security key

- On click of the steganography/send both the audio file and key will be send on server with the user current location (lat and long) and entry made in database and file stored on server.
- Matlab will take the uploaded file from server and perform the steganography on the audio file and generate the final output audio file which contains the original audio file data.
- After file generated on server Application user can download it and share with others.

3. Reverse Steganography

- User will select the shared stegno file and provide the key.
- File name key and user current location will be checked with database entry. If all the data matched user will get message file found.
- Matlab take the stegno file and perform Reverse steganography and generate the original file.
- As the original file is generated user can download the data and get the original message.
- User will record the file and select another audio file.
- Implemented on android platform

Advantages over existing System:

Proposed steganographic system will able to embed the secret message file in the Audio file for hiding more amounts of data with efficient data hiding techniques. The purpose of this paper is to implement the tool on android platform which will embed a secret message in a cover file (such as an audio recording) and provide the highly private and secure data transfer without third party intervention and at the receiver end this app will decrypt the message.

4. Conclusions

The proposed system should be more robust in effectively audio and speech signal. The model should achieve high security. As a future work, without any complication system can provide highly secured transfer of data in this proposed model.

Acknowledgments

Thanks to my honourable Guide Ms. Varsha Bhosale, Lecturer in Vidyalankar, Wadala for giving me valuable guidance.

References:

[1] "Alureon trojan uses steganography to receive commands," September 2011, http://www.virusbtn.com/-news/2011/09_26.

[2] D. Alperovitch, Revealed: operation Shady RAT. McAfee, 2011, http://www.mcafee.com/us/resources/-white-papers/wp-operation-shady-rat.pdf.

[3] S. Analysis and R. Center, "World's largest digital steganography database expands again," SARC Press Release, February 2012, http://www.sarc-wv.com/news/press_releases/2012/safdb_v312.aspx

[4] Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.

[5] N. Falliere, L. Murchu, and E. Chien, "W32.Stuxnet dossier," White paper, Symantec Corp., Security Response, 2011.

[6] www.google.com

[7] Wikipedia – The Free Encyclopedia. Android [Online] http://en.wikipedia.org/wiki/android