ISSN:0975-9646

Implementation of Location based Steganography on mobile Smartphone using Android Platform

Ms. Khushali Pandit
Student,
Vidyalankar Institute of Technology,
Wadala (E), Mumbai.

Ms. Varsha Bhosale
Associate Professor,Department of IT,
Vidyalankar Institute of Technology,
Wadala (E), Mumbai.

Abstract: Steganography in this project is a mechanism in which audio files are used as the cover signals to hide the sensitive/confidential data in it. The application is developed on the Android platform ADT (Android Developer Tool) using its IDE (Integrated Development Environment) provided by Eclipse. The purpose of this project is to implement the Android tool which in co-ordination with MATLAB code that will embed a secret message (i.e. an audio recording) in a cover audio file and provide the highly private and secure data transfer without third party intervention. Application of Steganography includes data hiding & 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. This project uses the cross platform implementation between ANDROID and MATLAB which makes it a unique project. The entire project is done through a WAMP Server which interfaces Android Based mobile and the system using the MATLAB code to embed and extract the secret message into a cover audio file. For higher security, Login ID and password and even app lock provisions are also given on the Android App.

Keywords: Steganography, mobile based, cover signal, secret message, Location, Cross Platforms, Security, ADT.

I. INTRODUCTION

Steganography is an art or science of hiding information within information. It 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. This volume of the paper explains the embedding and encrypting technique of the actual message audio recording file (.wav) onto a cover audio file which cannot be broken into without the password key decided by the transmitter of the cover file. The encryption is done using **MATLAB Version 12** and **Stegno App** developed using the **Android Development Tool**. The Decryption on the other hand is when the message is sent to the other device and similar **MATLAB** codes from the server separates the message from the cover file using the server already established.

II. OVERALL PROJECT FLOW

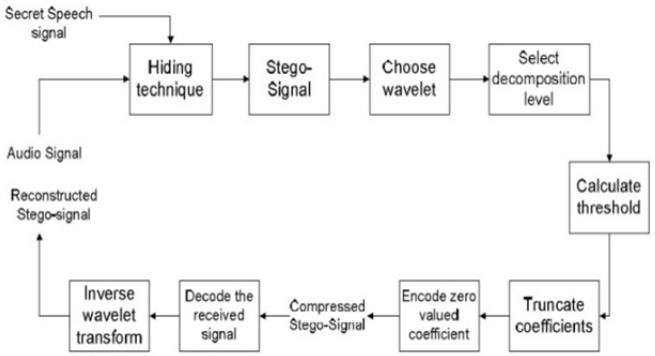

Figure 1: Flow of the complete system

III. TECHNIQUES FOR INFORMATION HIDING

1. Embedding flow:

Embedding of the original recorded message file is blanketed by or covered by a cover file using the android app developed using Android SDK in which coding is done through Eclipse. This application is interfaced with MATLAB program using WAMP Server.

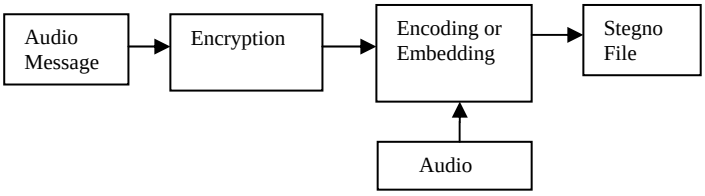

Figure 2: Information hiding at the Transmitter side.

The above flow diagram explains the embedding process of this project.

2. Extraction flow:

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.

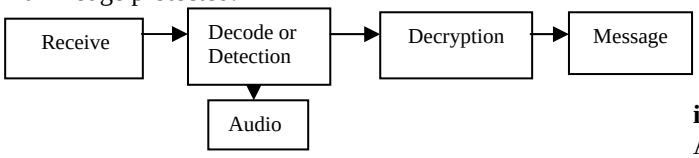

Figure 3: Information hiding at the Receiving side.

IV PLATFORMS AND SERVER USED

i. MATLAB

MATLAB is a high-level language and interactive environment for numerical computation, visualization, and programming. Using MATLAB, you can analyze data, develop algorithms, and create models and applications. In this project, MATLAB version R2012b is used. Only Embedding and extraction of the Speech audio message from the cover audio file is done using MATLAB. Coding in MATLAB are done using DWT and IDWT algos. MATLAB is interfaced with android platform using local server i.e. wamp server.

A. DWT (Discrete Wavelet Transform)

The discrete wavelet transform (DWT) is an implementation of the wavelet transform using a discrete set of the wavelet scales and translations obeying some defined rules.

B. IDWT (Inverse Discrete Wavelet Transform)

The inverse discrete wavelet transform performs a single-level one-dimensional wavelet reconstruction with respect to either a particular wavelet or particular wavelet reconstruction filters.

C. Embedding Algorithm

The Embedding Algorithm is as follows:

Step 1: Pass argument in a function.
Step 2: Read cover audio file and secret audio speech message.
Step 3: Perform levels of DWT on the original signal.
Step 4: Store the length of the original signal along with the length obtained after DWT
Step 5: Calculate the threshold and encode zero valued co-efficient and compress the secret audio file in the cover file
Step 6: Reconstruction of the signal is done using the haar transform and vectors.
Step 7: The final watermarked signal and the merged file is stored in the cover file without changing file size.
Step 8: Process of Embedding is completed.

D. Extracting Algorithm:

Step 1: Pass argument in a function.
Step 2: Read the recorded file from the server database and cover file from the receiver side and is stored as watermarked signal
Step 3: Perform different levels of DWT for the watermarked signal.
Step 4: Cover file is read from the database then sampled and stored.
Step 5: Perform IDWT on the original signal. An array of zeros is created and stored.
Step 6: As the for loop breaks, the speech recorded file is overwritten on the cover file and is stored in the device.
Step 7: Process of Extraction Completed.

ii. Android Platform:

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. The Snapshot
of the Stegno App is shown as follows.

Figure 4: Screenshot of Android App

iii. Wamp Server:

Wamp Server is a Windows web development environment. It allows you to create web applications with Apache2, PHP and a MySQL database. Alongside, PhpMyAdmin allows you to manage easily your databases. WampServer's functionalities are very complete and easy to use and manage. Apache and MySQL services, switch online/offline (give access to everyone or only localhost) install and switch Apache, MySQL and PHP releases, manage servers settings, access logs, access settings files, create alias. In this project Wamp Server is used to create an interface between Android and MATLAB platform and even for database.

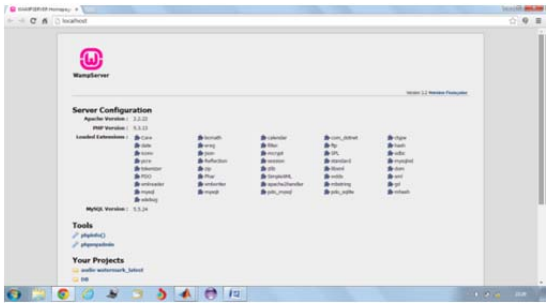

Figure 5: Snapshot of Wamp Server used in the project

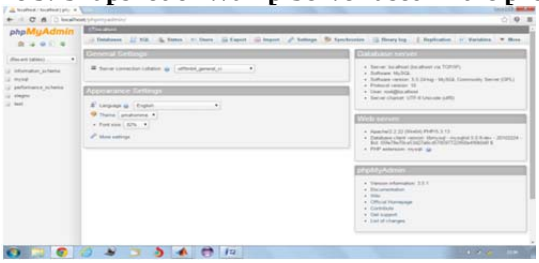

Figure 6: phpmyadmin of Wamp Server

V. EXECUTION RESULTS:

Following will be the step by step procedure of the execution of the project implemented.

Step 1: The Stegno App is clicked on by the user on the Android Smartphone and gets automatically connected to the Wamp server. The App is also given with a feature of Applock.

Step 2: Login Id and Password to be input in the App as per database

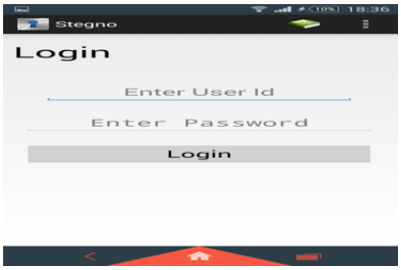

Figure 7: Login Id and Password

Step 3: After the login ID and password is correctly matched as per database than the next window is for selection Encryption or Decryption.

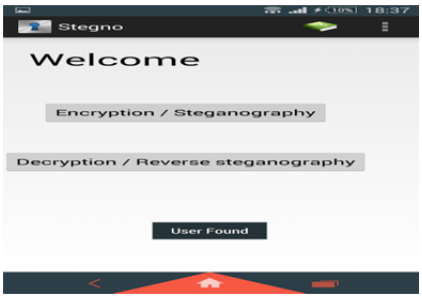

Figure 8: Encryption and Decryption

Step 4: User will record the secret audio message and select cover audio file and even user will enter key for security. The key can be sent to the required recipient using mobile messaging service in an encrypted format.

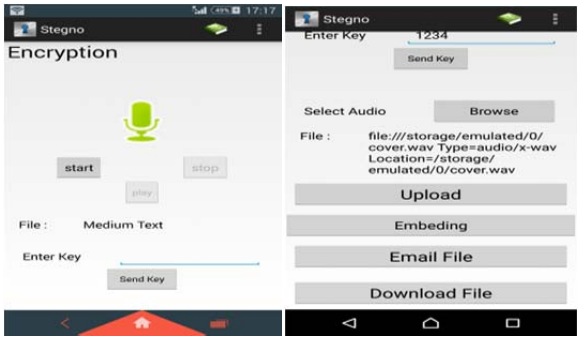

Figure 9: Message recorded; cover file selection and entering the security key.

Step 5: On click of Upload process both the audio file and key will be sent on server with the user current location (lat and long) and entry made in database and file stored.

Step 6: On clicking the Embedding button MATLAB embed.exe file will be executed which will take the uploaded file from server and embed the audio message in the cover file using a secret key.

Step 7: After the audio file is embedded, user can download it and share it with others.

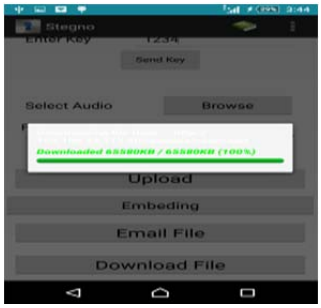

Figure 10: File downloaded after embedding

Step 8: File after download will be sent to the receiver's device. There the receiver will start the app login and then select decryption option.

Step 9: The encrypted key will be received and to be pasted on the decrypt option. OK button is clicked and the encrypted key will be decrypted and key will be extracted.

Step 10: File name key and user current location will be checked with database entry. If all the data matched user will get message file found.

Figure 11: Decryption process

Step 11: On clicking on extraction the MATLAB extract.exe file will take stegno file and perform Extraction and generate original file.

Step 12: As the original file is generated user can download the data and get the original message.

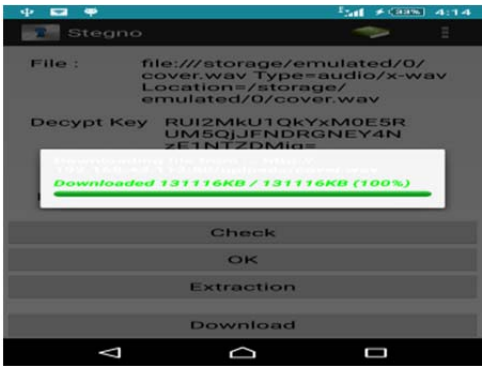

Figure 12: File downloaded after extracting

Step 14: Implemented on android platform.

Note: If the sender or the receiver are stuck on some point in the app the can use the help option where everything is explained in detail. Even there a admin login the app if somewhere something goes wrong user can complain the admin department in their local area.

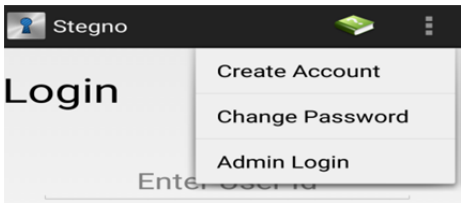

Figure 13: Admin login and help option

TABLE I COMPARISON OF MOBILE OPERATING SYSTEM

MOBILE OS	ANDROID	IPHONE	WINDOWS MOBILE
3rd Party Multi Tasking	Yes	Yes from Iphone 4	Yes
Memory Management	It is done by Linux and uses more compact executable files instead of conventional format.	Memories for objects are freed based on reference counting.	It has custom memory management.
Kernel Type	Modified Linux	XNU Kernel	WinCE Kernel
Thread Priority Levels	40	10	256
Customization	With some effort you can personalize things to work exactly as you want it to	Apple decides what you can do. If you're a techie you can jailbreak your IPhone but you're always jumping through hoops.	Not open to customizations.
Design, Affordability and Variety	Lots of phones to choose from, ranging from average to excellent build quality, offering different features such as physical keyboards.	Only 1 device to choose from per 12-18 months. Expensive unless you go for an old model.	Microsoft's strict hardware requirements mean there will be less handset variety than Android.
Synching and Backup	Wireless automatic syncing via 3rd party apps. Excellent syncing with Google services Google sync, drive.	Synching is tedious in case of IOS.	Syncing app that replaces Zune is inferior and incomplete, e.g. no Wireless syncing, poor music management.

VI. APPLICATION:

The app is used for transferring secret messages and this app is basically used by many different agencies in real world. This app also has its application in women safety in the current scenario society.

VII. CONCLUSION

The proposed system is robust in effectively audio and speech signal. The model achieves high security. System can provide highly secured transfer of data.

ACKNOWLEDGMENTS

Thanks to my honourable Guide Ms. Varsha Bhosale, Associate Professor in Department of IT in VIT, Wadala (E) 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] www.google.com
[6] Wikipedia – The Free Encyclopedia. Android [Online] Available at : http://en.wikipedia.org/wiki/android
[7] Lan F Dardvin 'Android cook book'
[8] Waei – Meng Lee "Beginning Android 4 application development"
[9] Wyken Seagrave "Basic 4 Android"
[10] Rajkumar Bansali "Matlab"
[11] Rudra Pratap "Getting start with Matlab"
[12] www.mathworks.com