Android Environment and Information Security

Roopesh Kumar[1] Akhilesh Dubey[2]
[1,2]Lecturer
[1,2]Department of Computer Science & Engineering
[1,2]Mandsaur Institute of Technology, Mandsaur

Abstract— Now days, Internet and Mobile is widely used for communication. Messaging, voice calling over Internet, sending images and music files are commonly used activities over phones. In the field of communication new invention has changed the working environment for users. The recent trend is of smart phones. These smart phones work on new operating system known as android. Android is a software platform that's revolutionizing the global cell phone market. In these smart phones different application can be installed for specific purpose. The most popular apps for messaging is whatsapp. With the help of this app user can send music file, text and images. These techniques make the communication so fast. As well as the communication became easy attention toward information security increased. Data Security is the main concern for research. We use Cryptography or Steganography for secure communication. In Steganography we hide the message by different techniques. This paper provides the introduction to Android Environment and Steganography.

Keywords: Android, Steganography, Cryptography, Secure Communication

I. INTRODUCTION

Communication and digital technology has changed society's daily activities, using information in all spheres of its existence, having a major economic and social impact. After rapid growth of the Internet and Mobile Networks, nowadays we witness the development of smaller, faster and high-performance mobile devices, which can support a wide range of features that were, not so long ago, the attributes of personal computers. Mobile hand-held devices which are popularly called smart gadgets include: smart phones, tablets, e-book readers and are becoming essential to everyday social activities. These newly developed technologies make easier and cheaper the access, the processing, the storing and the transmitting of information. In this ever changing and evolving environment, establishing secure communication is an important target for researchers [1].Now day's smart phones have changed the way of communication. Messaging and Voice call over Internet has become popular among the peoples. These smart phones have different environment called android operating system. In these smart phones small application known as apps can easily be installed for specific functions. The extensively used messaging apps is WhatsApp messenger. In this app we can chat easily also can send images and music files. WhatsApp Messenger is a 'cross-platform messaging app which allows users to exchange messages without having to pay for SMS' (WhatsApp.com, 2012). The application is compatible with iPhone, BlackBerry, Android, Nokia, and other Windows smart phones. WhatsApp features include one-on-one chat, group chat, push notifications, sending and receiving both video and audio files. By April 2014 it was estimated that WhatsApp had approximately 500 million users (Statista, 2014), who send and receive more than 64 billion messages a day (Trenholm, 2014)[6].

Android environment has brought the drastic change in communication. As well as the communication has become fast and easy the risk of information security has increases. It has challenging task for researchers to provide security for information in Android environment. In this paper we are presenting introduction to Android Operating system and Information security technique known Steganography (The art of data hiding). First we are explaining the Android part and later on Introduction to Steganography.

II. ANDROID PLATFORM

Android is a software environment built for mobile devices. It's not a hardware platform. Android includes a Linux kernel-based OS, a rich UI, end-user applications, code libraries, application frameworks, multimedia support, and much more. And, yes, even telephone functionality is included! Whereas components of the underlying OS are written in C or C++, user applications are built for Android in Java. Even the built-in applications are written in Java. One feature of the Android platform is that there's no difference between the built-in applications and applications that you create with the SDK. This means that you can write powerful applications to tap into the resources available on the device [2].

Applications layer is the site of all Android applications including an email client, SMS program, maps, browser, contacts, and others. All applications are written using the Java programming language. Application framework layer defined the Android application framework. All Android applications are based on the application framework. The Android application framework including:

A rich and extensible set of Views that can be used to build an application with beautiful user interface, including lists, grids, text boxes, buttons, and even an embeddable web browser.

- A set of Content Providers that enable applications to access data from other applications (such as Contacts), or to share their own data.
- A Resource Manager that provides access to noncode resources such as localized strings, graphics, and layout files.
- A Notification Manager that enables all applications to display custom alerts in the status bar.
- An Activity Manager that manages the lifecycle of applications and provides a common navigation back stack [3]

A core element of the SDK is the actual Google Android Emulator which provides

All rights reserved by www.ijsrd.com

a graphical emulation of a possible handheld device running Google Android Furthermore, the SDK not only provides the core classes of the Android framework packed into a Java Jar-file: it also includes the documentation in HTML-form and several tools that improve the usability and interaction with the emulator. The architecture basically consists of four sections: the Linux kernel (system) as underlying operating system interface, the libraries (e.g libc) as important part of the operating system; the Android framework providing all necessary classes and methods in order to write Android-compatible applications; and, as top section, the actual Android applications.

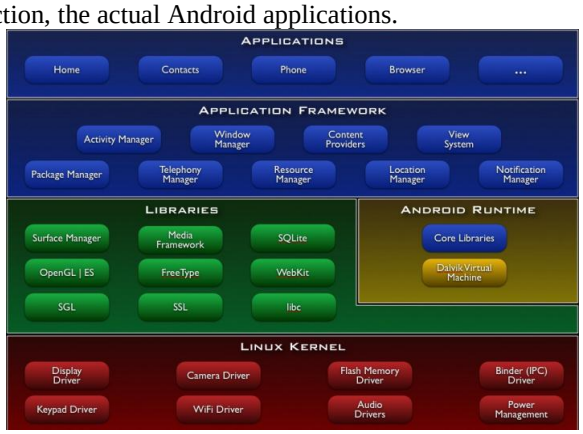

Fig. 1: The Google Android Architecture overview [12]

III. STEGANOGRAPHY

Steganography is the science of writing hidden message in such a way that no one can understand the existence of message. The word Steganography originally derived from Greek word steganos (στεγανός) which means, "Covered writing" With the time technologies have improved and steganography has gone to digital. One of the earliest methods to discuss digital steganography is credited to Kurak and McHugh, who proposed method which is similar to 4 LSB methods. It is the science that involves communicating secret data in an appropriate multimedia carrier such as images, audio or video [5]. Steganography may have different form the common forms are:

- Encoding message in text
- Encoding message in audio
- Encoding message in video
- Encoding message in images

For each encoding there are too many different algorithms. Mostly common algorithm is least significant bit which is used for embedding in image.

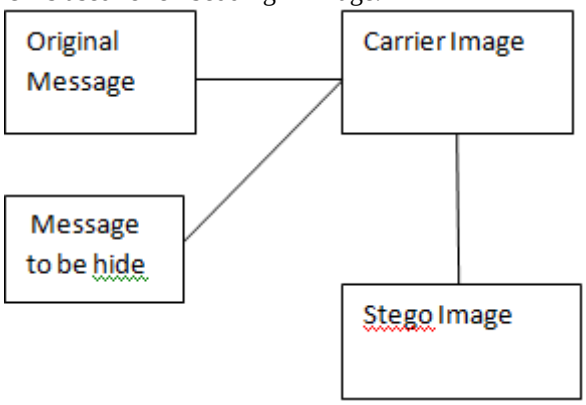

Fig. 1: Simple Diagram of Data Hiding

IV. RELATED WORK

A. Unique Approach:

The approach used for hiding crucial information is one which is unique as the data is divided and hidden into image and text cover files if text + image option is chosen. Also, if only image cover file is chosen, the entire secret message can be hidden in the image itself. The comparison shows various devices taking the amount of time that they use in encoding a particular message in a cover image file. Thus, this approach is unique and secure for communicating secret data through smart phones [4]

B. Exploring Steganography: Seeing the Unseen:

The authors review some recent steganographic tools freely available on the Internet this includes: StegoDos, White Noise Storm and S-Tools. After a general introduction to steganography, the authors discuss advantages and weaknesses of each tools.[7]

C. LSB Steganography Using Android Phone:

In this paper RSA algorithm is used for data encryption and decryption. Through LSB algorithm image steganography embedded the secret in the least significant bit of pixels values of cover image.[8]

D. Android Application for Secret Image Transmission and Reception using haotic Steganography:

In this paper author presented chaotic method for steganography .Chaotic systems are known for its randomness, it can be made utilized in achieving the encryption. In this paper chaos-based encryption algorithm for images is used. This algorithm is based on pixel scrambling where in the randomness of the chaos is made utilized to scramble the position of the pixels. Random pixel insertion method is used for hiding the secrete image in cover image. This Application is developed using the Java programming language in Android Software Development Kit. This application created for the Android operating system can be used in smart mobile phones for sending any image in a secrete manner by hiding it in another larger image.[9]

E. Real Time Implementation of Secured Multimedia Messaging Service System using Android:

In this paper encryption and steganography algorithms are implemented using JAVA™ with android platform to provide the security for real time multimedia messaging service system. Establishing hidden communication for mobile has become an important subject of security. One of the methods to provide security is steganography. Steganography is used to hide secret information inside some carrier. To improve the security, encrypted secret data will be hidden inside MMS. The image is made to be hidden into image from MMS which provides more secured transmission than text information embedded into the MMS. The Least Significant Bit (LSB) embedding technique is used to hide the secret information (image). Different sizes of secret images are taken and later the calculations have been done for the PSNR (Peak Signal to Noise Ratio) of image in MATLAB. Encryption and steganography algorithms are ported on HTC Desire mobile device with android version 2.2.3.[10]

All rights reserved by *www.ijsrd.com*

F. Securing Data Using Jpeg Image over Mobile Phone:

In this paper Discrete Cosine transform (DCT) for image steganography and tiny encryption algorithm for cryptography has been used. Tiny encryption algorithm (TEA) is block cipher algorithm .It is simple and fast but best for mobile application [11].

V. CONCLUSION

We have studied different techniques for data security using steganography. As method mentioned in [9] is implemented in java .Most of the application for android written in JAVA. This method can also be implemented for android environment. It will provide comparatively more secure information Exchange over messaging apps. Before sending the image encrypted message hided in the images. Receiver will get original message from the image by decrypting it.

VI. FUTURE WORK

Suggested technique has implemented on Emulator for java based mobile phones which is used for sending MMS .The implementation of this technique for android environment is carried out in future.

REFERENCES

[1] D. Bucerzan, C. Ratiu, M.J. Manolescu, "SmartSteg: A New Android Based Steganography Application", INT J COMPUT COMMUN, ISSN 1841-9836,8(5):681-688, October, 2013.
[2] W. Frank Abelson, Robi Sen, Chris King, C. Enrique Ortiz, Android in Action, Third Edition Sample Chapter.
[3] Jianye Liu, Jiankun Yu, "Research on Development of Android Applications"2011 Fourth International Conference on Intelligent Networks and Intelligent Systems
[4] Prof. Sharmishta Desai, Sanaa Amreliwala, Vineet Kumar, "Enhancing Security in Mobile Communication using a Unique Approach in Steganography" IJCSMC, Vol. 3, Issue. 4, April 2014, pg.433 – 439
[5] A.Cheddad, J.Condell, K.Curran, P.M.kevitt , "Digital image Steganography:Survey and analysis of current method" Signal Processing pp 727-752,2010
[6] Richard Shambare ,The Adoption of WhatsApp: Breaking the Vicious Cycle of Technological Poverty in South Africa, Journal of Economics and Behavioral Studies Vol. 6, No. 7, pp. 542-550, July 2014 (ISSN: 2220-6140)
[7] 'Exploring Steganography: Seeing the Unseen' N. F. Johnson, S. Jajodia, Computer, vol. 31 no. 2 pp. 26–34, Feb. 1998
[8] Rajashri Ghare, Pruthvi Bansode, Sagar Bombale , Bilkis Chandargi ,"LSB Steganography Using Android Phone" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1027-1029
[9] Savithri G1, K.L.Sudha, "Android Application for Secret ImageTransmission and Reception Using Chaotic Steganography" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 7, July 2014
[10] Geetanjali R. Kshirsagar*, Savita Kulkarni, "Real Time Implementation of Secured Multimedia Messaging Service System using Android" International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013
[11] Yogendra Kumar Jain,Roopesh Kumar, Pankaj Agarwal, "Securing Data Using Jpeg Image over Mobile Phone"Global Journal of Computer Science and Technology Volume 11 Issue 13 Version 1.0 August 2011
[12] Hans-Gunther Schmidt, Karsten Raddatz, Aubrey-Derrick Schmidt, Ahmet Camtepe, and Sahin Albayrak, " Google Android - A Comprehensive Introduction" March 16, 2009

All rights reserved by *www.ijsrd.com*