International Journal of Combined Research & Development (IJCRD)
eISSN: 2321-225X;pISSN:2321-2241 Volume: 4; Issue: 8; August -2015

Secure Data Transfer in Android Enabled Devices through Steganography (Secura)

Nirupadi Tidigol
Dept. of CSE, VTU
EIT, Ummathur, India

Thrilochana KumaraY.P
Dept. of CSE,
Mysore, India

T.P.Lokesh
Dept. of ECE, VTU
EIT, Ummathur, India

Srinivas.P.S
Dept. of ISE, SNP
Ramanagar,India

***Abstract*: Android is a mobile operating system (OS) based on the Linux kernel and currently developed by Google. With a user interface based on direct manipulation, Android is designed primarily for touch screen mobile devices such as smart phones and tablet computers Android enabled mobile phones will perform SMS/MMS Sending,Connect to internet Via Wi-Fi/mobile data,Data sending via Bluetooth/Wi-Fi or other software tools functions In android enabled mobile data transferring from one to another the data maybe insecure, to resolve this problem we use the concept of secura.Secura is a secure application to send/receive all types of data in an android Mobile, it uses steganography method to secure the data. Steganography provides better security to the android phones while transferring the data.**

***Keywords:* Android OS, Features, data transfer service & Applications , Secura, & steganography.**

I. ANDROID (OPERATING SYSTEM)

Android is a mobile operating system (OS) based on the Linux kernel and currently developed by Google. With a user interface based on direct manipulation, Android is designed primarily for touch screen mobile devices such as smart phones and tablet computers. The OS uses touch inputs that loosely correspond to real-world actions, like swiping, tapping, pinching, and reverse pinching to manipulate on-screen objects, and a virtual keyboard. Despite being primarily designed for touch screen input, it also has been used in game consoles, digital cameras, regular PCs (e.g. the HP Slate 21) and other electronics.

Symbol of Android

II.FEATURES

Interface

Tablet Interface

Android 2.3.6 Version Mobile Interface

Notifications are accessed by sliding from the top of the display; individual notifications can be dismissed by sliding them away, and may contain additional functions (such as on the "missed call" notification seen here).

Android's default user interface is based on direct manipulation, using touch inputs, that loosely correspond to real-world actions, like swiping, tapping, pinching, and reverse pinching to manipulate on-screen objects, and a virtual keyboard. The response to user input is designed to be immediate and provides a fluid touch interface, often using the vibration capabilities of the device to provide haptic feedback to the user. Internal hardware such as accelerometers, gyroscopes and proximity sensors are used by some applications to respond to additional user actions, for example adjusting the screen from portrait to landscape depending on how the device is oriented, or allowing the user to steer a vehicle in a racing game by rotating the device, simulating control of a steering wheel.

Android devices boot to the home screen, the primary navigation and information point on the device, which is similar to the desktop found on PCs. Android home screens are typically made up of app icons and widgets; app icons launch the associated app, whereas widgets display live, auto-updating content such as the weather forecast, the user's email inbox, or a news ticker directly on the home screen. A home screen may be made up of several pages that the user can swipe back and forth between, though Android's home screen interface is heavily customizable, allowing the user to adjust the look and feel of the device to their tastes. Third-party apps available on Google Play and other app stores can extensively re-theme the home screen, and even mimic the look of other operating systems, such as Windows Phone. Most manufacturers, and some wireless carriers, customize the look and feel of their Android devices to differentiate themselves from their competitors. Present along the top of the screen is a status bar, showing information about the device and its connectivity. This status bar can be "pulled" down to reveal a notification screen where apps display important information or updates, such as a newly received email or SMS text, in a way that does not immediately interrupt or inconvenience the user. Notifications are persistent until read (by tapping, which opens the relevant app) or dismissed by sliding it off the screen. Beginning on Android 4.1, "expanded notifications" can display expanded details or additional functionality; for instance, a music player can display playback controls, and a "missed call" notification provides buttons for calling back or sending the caller an SMS message.

III. Data Transfer

Android enabled mobile phones will perform the basic fallowing functions:

SMS/MMS Sending

Connect to internet Via Wi-Fi/mobile data

Data sending via Bluetooth/Wi-Fi or other software tools.

APPLICATIONS

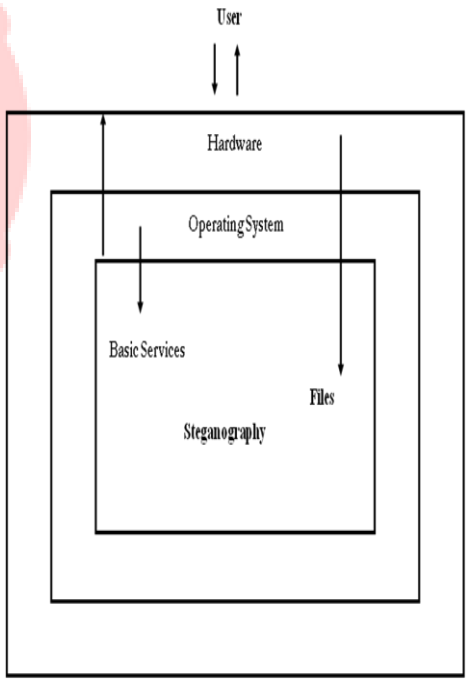
Applications ("apps"), that extend the functionality of devices, are developed primarily in the Java programming language[] using the Android software development kit (SDK). The SDK includes a comprehensive set of development tools, including a debugger, software libraries, a handset emulator based on QEMU, documentation, sample code, and tutorials. The officially supported integrated development environment (IDE) is Eclipse using the Android Development Tools (ADT) plug-in. Other development tools are available, including a Native Development Kit for applications or extensions in C or C++, Google App Inventor, a visual environment for novice programmers, and various cross platform mobile web applications frameworks. In January 2014, Google unveiled an Apache Cordova–based framework

for porting Chrome HTML 5 applications to Android, wrapped in a native application shell.

Android has a growing selection of third-party applications, which can be acquired by users by downloading and installing the application's APK file, or by downloading them using an application store program that allows users to install, update, and remove applications from their devices. Google Play Store is the primary application store installed on Android devices that comply with Google's compatibility requirements and license the Google Mobile Services software Google Play Store allows users to browse, download and update applications published by Google and third-party developers; As of July 2013, there are more than one million applications available for Android in Play Store. Due to the open nature of Android, a number of third-party application marketplace also exist for Android, either to provide a substitute for devices that are not allowed to ship with Google Play Store, provide applications that cannot be offered on Google Play Store due to policy violations, or for other reasons. Examples of these third-party stores have included the Amazon Appstore, GetJar, and Slide Me. F-Droid, another alternative marketplace, seeks to only provide applications that are distributed under free and open source licenses.

IV.SECURA

In android enabled mobile data transferring from one to another mobile the data maybe insecure to resolve this problem we use the concept of secura.Secura is a secure application to send/receive all types of data in an android Mobile, it uses steganography method to secure the data. Steganography provides better security to the android phones while transferring the data from one device to other via SMS, MMS, bluetooth sending. Steganography is the art of hiding data in a seemingly innocuous cover medium. For example – any sensitive data can be hidden inside a digital image. So no one apart from the authorized sender and receiver will be aware of the existence of the secret data. Steganographic messages are often first encrypted by some traditional means and then a cover image is modified in some way to contain the encrypted message. The detection of steganographically encoded packages is called steganalysis. In this paper, we propose three efficient Steganography techniques that are used for hiding secret data. They are LSB based Steganography, Steganography using the last two significant bits and Steganography using diagonal pixels of the image. Symmetric and asymmetric key cryptography has been used to encrypt the message.



System Architecture

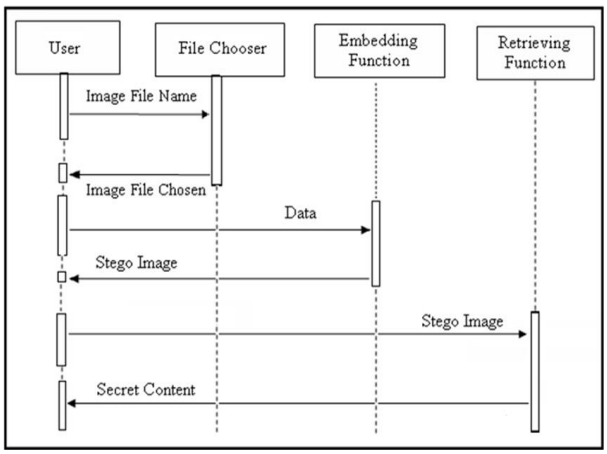
Steganography is the art or practice of concealing a message, image, or file within another message, image, file, audio or video. The word steganography combines the Ancient Greek words steganos (στεγανός), meaning "covered, concealed, or protected", and graphein

(γράφειν) meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic.

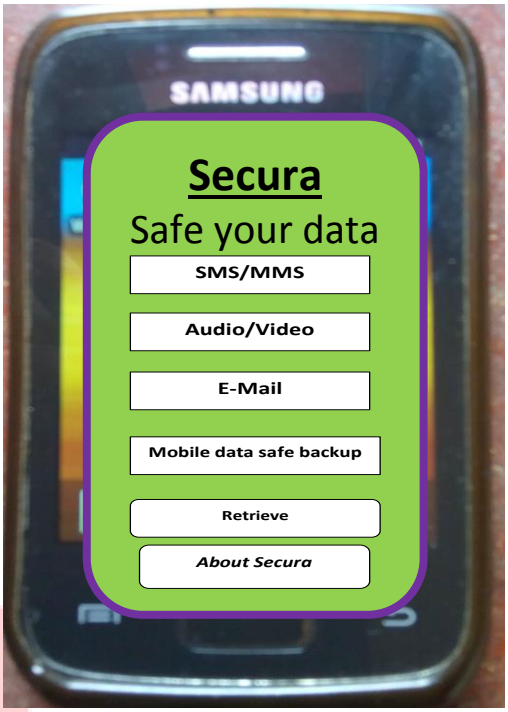
Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter

The use of Steganography in Android mobiles

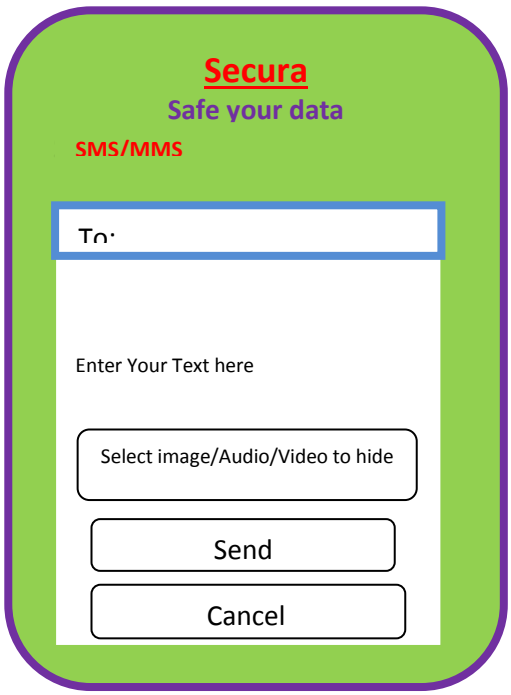
1. The development of an attractive Graphical User Interface that allows the user to send the text/image/Audio/Video to the receiver Securely
2. The engine will even enable to extract embedded information from loaded images.
3. To give an option of compression of contents [within the image/audio/video] to the user.
4. User can keep the files/Folder securely within the mobile
5. Data Present in the Mobile can be backup securely



Sequence diagram for SMS Sending



Proposed Frontend of a Secura Application



Sample SMS Sending Module:

How Secura work for SMS Sending

Image of a tree with a steganographically hidden SMS.

The hidden SMS is revealed by removing all but the two least significant bits of each Letter and a subsequent normalization. The hidden SMS is shown below.

Your Bank Account Number is XXXXX005749XXX and the ATM password is 0015

SMS is extracted from the tree image above. The application allows embedding a message to an image which can be compressed and encrypted by specifying a password to send the message to the receiver. The receiver required password to decrypt the message from the image

Embedding data in a JPEG Image

Because the JPEG file format is compact and does not significantly degrade the quality of an image it is in frequent use on the internet. The JPEG format uses a discrete cosine transform (DCT) to identify 64 DCT coefficients in successive 8x8 pixel blocks. Of these quantized coefficients, the least significant bits are used to embed data. Because modifications to these bits affect pixel frequency as opposed to spatial structure (as in GIF images where image structure information is present at every bit layer), no obvious distortion is present.

V.CONCLUSION

Android is a mobile Application designed primarily for touch screen mobile devices. While data transferring in android enabled mobile from one to another the data maybe insecure, secura will resolve this problem .By using Secura application the user can send/receive all types of data in an android Mobile securely, it uses steganography method to secure the data. Steganography provides better security to the android phones while transferring the data

VI. REFERENCES

[1] "Philosophy and Goals". Android Open Source Project. Google.

[2] "When and where to get Android 5.0 Lollipop". CNET. CBS Interactive. October 15, 2014. Retrieved October 16, 2014.

[3] "Updated Android Lollipop Developer Preview image coming to Nexus devices in a couple of days". Phone Arena. Retrieved October 16, 2014.

[4] "MIPS get sweet with Honeycomb". Eetimes.com. Retrieved February 20, 2012.

[5] Shah, Agam (December 1, 2011). "Google's Android 4.0 ported to x86 processors". Computerworld. International Data Group. Retrieved February 20, 2012.

[6] Wayner, Peter (2002). Disappearing cryptography: information hiding: steganography & watermarking. Amsterdam: MK/Morgan Kaufmann Publishers. ISBN 1-558-60769-2

[7] Wayner, Peter (2009). Disappearing cryptography 3rd Edition: information hiding: steganography &

watermarking. Amsterdam: MK/Morgan Kaufmann Publishers. ISBN 978-0-123-74479-1.

[8] Petitcolas, Fabien A.P.; Katzenbeisser, Stefan (2000). Information Hiding Techniques for Steganography and Digital Watermarking. Artech House Publishers. ISBN 1-580-53035-4.

[9] Detecting Steganographic Content on the Internet. 2002 paper by Niels Provos and Peter Honeyman published in Proceedings of the Network and Distributed System Security Symposium (San Diego, CA, February 6–8, 2002). NDSS 2002. Internet Society, Washington, D.C.

[10] Recent Advances in Steganography, By Hedieh Sajedi, Published by : InTech

[11] Steganography in digital media, principal, algorithm and application by Jessica Fredrich Published by Cambridge University Press New York.

[12] Digital Watermarking and Steganography By Ingemar Cox, Professor, University College, London, U.K. Matthew Miller, NEC, Princeton, NJ, U.S.A.Jeffrey Bloom, Thomson, Princeton, NJ,U.S.A. Jessica Fridrich, SUNY Binghamton, Binghamton, NY, U.S.A.Ton Kalker, Hewlett-Packard Labs, Palo Alto, CA, U.S.A.

[13]

[14] **AUTHORS PROFILE**

Nirupadi Tidigol received B.E in CSE,SJMIT,Chithradurga and 1995. M.Tech in CNE,NIE,Mysore,2011.

He is working as an Assistant Professor and Head, Department of Computer Science and Engineering in EIT,Ummathur, Chamarajanagara, India, 4Yrs. Experience as a Head,Department of CS&E VVET,Mysore, 1Yr. of Experience as a Head, Department of computer Science and engineering VVCE, 9 Yrs. Experience as Head/Lecturer Dept. of CS&E,SLN. Presented, and attended the number of Conferences and workshops. His area of interests is Computer Networks and its Security , Data Mining, Cloud Computing ,wireless communication and Image Processing

Thrilochana Kumara Y.P received B.E in CSE, JVIT, Bangalore and 2005.& M.Tech in IT, KSOU, Mysore, 2010.

He has 3Yrs. Experience as a Lecturer,Department of CS&E VVET,Mysore, 2Yr. of Experience as a System Administrator VET,Bannur .He Presented, and attended the number of Conferences and workshops. His area of interests is Computer Networks, Data Mining and its Security, Cloud Computing, wireless communication

T.P.Lokesh received B.E in Electronics and Communication, M.Tech in Computer Network and Engineering and he is working as a Assistant Professor, Department of Electronics and Communication in VVET, Mysore. He has 8 years of teaching experience. He presented, attended the number of Conferences and workshops organized at various organizations.

Srinivas PS received B.E in SIT,Tumkur. . & M.Tech IT, in KSOU, Mysore, 2010.

He has 15 Yrs. Of Experience in teaching, presently working as a Head of the department in IS&E Santhinikethan Polytechnic Ramanagar. He Guided many projects and his area of interests are DBMS, Operating System,System Software and .NET

International Journal of Combined Research & Development (IJCRD)
eISSN: 2321-225X;pISSN:2321-2241 Volume: 4; Issue: 8; August -2015

Secure Data Transfer in Android Enabled Devices through Steganography (Secura)

Nirupadi Tidigol Thrilochana KumaraY.P
T.P.Lokesh Srinivas.P.S

Research Paper Received : June – 2015

Acceptance Notification : July 2015

Publication of Research Paper : August – 2015