INT J COMPUT COMMUN, ISSN 1841-9836
8(5):681-688, October, 2013.

SmartSteg: A New Android Based Steganography Application

D. Bucerzan, C. Ratiu, M.J. Manolescu

Dominic Bucerzan
Aurel Vlaicu University of Arad
Department of Mathematics and Computer Science
Romania, 310330 Arad, Elena Dragoi, 2
dominic@bbcomputer.ro

Crina Raţiu*
Vasile Goldis Western University of Arad
Department of Computer Science
Romania, 310414, Arad, Liviu Rebreanu, 91-93
*Corresponding author: ratiu_anina@yahoo.com

Misu-Jan Manolescu
Agora University of Oradea
Romania, 486526 Oradea, Piata Tineretului, 8
mmj@univagora.ro

Abstract: With the development of mobile devices the security issue migrates from the PC platform to this new technology. Securing confidential information on the mobile platforms has been, is and will be a topical issue for the specialists. In this paper we propose a new solution in order to provide security of digital data that is transferred through today's available platforms for communication.
We developed SmartSteg application that works on Android platform and it is able to hide and fast encrypt files using digital images of MB dimension as cover. LSB steganography is combined with a random function and symmetric key cryptography to transfer digital information, in a secure manner between smartphones that run under Android.
Keywords: Least Significant Bit (LSB), steganography, cryptography, android, SmartSteg.

1 Introduction

Communication and digital technology has changed society's daily activities, using information in all spheres of its existence, having a major economical 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. Figure 1 shows briefly today's techniques widely used to secure digital information.

Cryptography and steganography are two techniques used to ensure information confidentiality, integrity and authenticity. Cryptography uses encryption to scramble the secret information in such a way that only the sender and the intended receiver are able to reveal it. Steganography hides the secret information in different carriers in such a way that it becomes difficult to detect. Commonly the carriers are media files (like images, audio, video) or other supports like communications protocols; an example is network steganography [6].

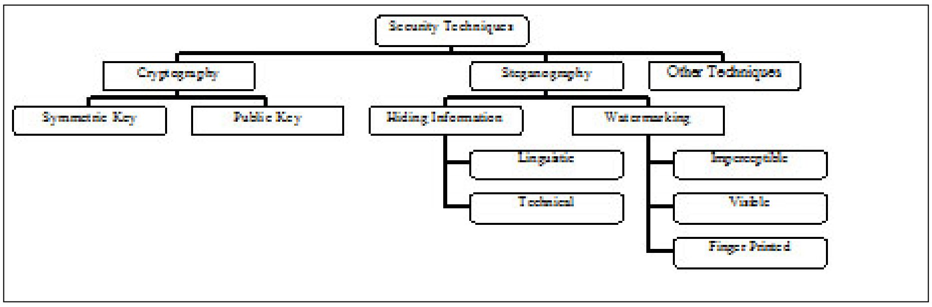


Figure 1: Security techniques

Both technologies have their limitations and this is why most of the specialists sustain that a good solution for securing the digital information is to combine the two techniques [9].

In this paper we propose a new application named SmartSteg developed to transmit secret files through Internet and Mobile Networks using a smart phone that run Android operating system. It involves technical steganography combined with symmetric key cryptography and a pseudorandom selection of the bits.

We chose to work on Android because:

- it is an open source software designed for mobile phones,
- it is well spread between mobile phones manufacturers as shown in Table 1 and Table 2,
- we have not find any reliable steganography application for Android phones that work with large files.

Company	1Q13 Units	1Q13 Market Share (%)	1Q12 Units	1Q12 Market Share (%)
Samsung	64,740.0	30.8	40,612.8	27.6
Apple	38,331.8	18.2	33,120.5	22.5
LG Electronics	10,080.4	4.8	4,961.4	3.4
Huawei Technologies	9,334.2	4.4	5,269.6	3.6
ZTE	7,883.3	3.8	4,518.9	3.1
Others	79,676.4	37.9	58,537.0	39.8

Table 1. Worldwide Smartphone Sales to End Users by Vendor in 1Q13 (Thousands of Units). Source: Gartner (May 2013) [10]

Operating System	1Q13 Units	1Q13 Market Share (%)	1Q12 Units	1Q12 Market Share (%)
Android	156,186.0	74.4	83,684.4	56.9
iOS	38,331.8	18.2	33,120.5	22.5
BlackBerry	6,218.6	3.0	9,939.3	6.8
Microsoft	5,989.2	2.9	2,722.5	1.9
Bada	1,370.8	0.7	3,843.7	2.6
Symbian	1,349.4	0.6	12,466.9	8.5
Others	600.3	0.3	1,242.9	0.8

Table 2. Worldwide Smartphone Sales to End Users by Operating System in 1Q13 (Thousands of Units). Source: Gartner (May 2013) [10]

Android may be considered a software stack for mobile devices that includes an operating system, middle ware and key applications [8]. Android architecture includes five layers, as shown in figure 2: applications layer, application framework layer, libraries, Android runtime, Linux kernel.

Linux kernel is the basis of Android architecture and it supports security, memory management, process management, network stack, and device driver model. Android's libraries are written in C/C++ and include: standard C system library, media libraries including MPEG4, H.264, MP3, JPG, and PNG, surface manager for display subsystem, LibWebCore as a web browser engine, 2D graphics engine SGL, 3D graphics libraries, FreeType for font rendering and SQLite, a lightweight relational database engine [8]. Android runtime is the engine which authorizes the applications. It includes Dalvik virtual machine and core android libraries [4]. The application framework layer includes the application manager, which allows developers to use the features of Android operating system. The application layers include all native and third party applications.

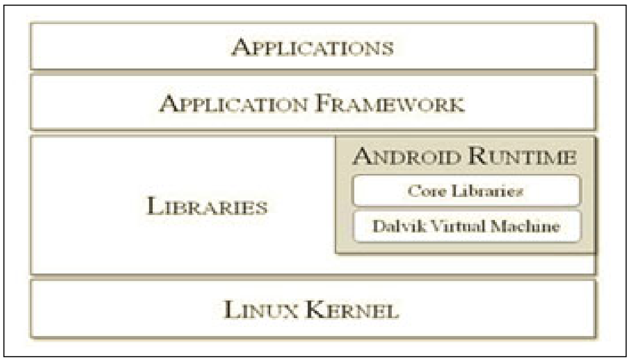


Figure 2: Android architecture [8]

2 Related Works

Image steganography has drawn attention of researchers because of its applicability in today's digitalized world. There are many applications in this direction mainly developed on computers running different operation systems.

A new approach in steganography that drawn our attention is the project developed by Mazurczyk, Karas and Szczypiorski on Skype steganography. The researchers method lies in how Skype manages silence sequences. The application encrypts the secret data and embeds it in a silence package when ones appear [3].

An interesting idea of a robust algorithm of steganography resistant to steganalytic attacks is presented in the research made by Mare [2].

Regarding Android for mobile phones, there are few reliable projects on steganography. In the following we discuss some of them.

Most of the applications that exist on Android smart phones, embeds only short sequence of characters, none of them embeds entire files. This excludes the possibility to traffic secretly images or large documents.

White and Martina developed an application Android based that uses steganography to hide a short text message in an audio message recorded by the user and then share that message [7].

MoBiSiS is an application that implements a steganographic algorithm Android based. It is able to send the image that covers the secret message via the Multimedia Messaging Service

(MMS). The cover image can be retrieved from the device's message inbox. The disadvantage of this application is the size of the cover image with the secret message embedded which must be less than 30 KB [1].

Similar applications with MoBiSiS having the same limitations, are MobiStego [12] and Pixelknot [13] both available on Google Play.

Rughani in his work [5] regarding the limitation of implementing steganography on smart phones sustains some ideas that we do not agree with:

- There cannot be a common algorithm - since there are many smart phone manufacturers. It is almost difficult to develop a common algorithm for steganography.
  - Our opinion - there are three main players (see Table 3) in the operating systems market for smart phones (Android, IO's, Windows 8) and we extend our project to all these operating systems.

- "Smart phones are small computing devices - even though smart phones are smarter than mobile phones they are not as efficient as traditional computer like desktop or laptop".
  - Our opinion - smart phones support complex, efficient and fast algorithms, fact sustained by the present work.

Operating System	1Q13 Shipment Volume	1Q13 Market Share	1Q12 Shipment Volume	1Q12 Market Share
Android	162.1	75.0%	90.3	59.1%
iOS	37.4	17.3%	35.1	23.0%
Windows Phone	7.0	3.2%	3.0	2.0%
BlackBerry OS	6.3	2.9%	9.7	6.4%
Linux	2.1	1.0%	3.6	2.4%
Symbian	1.2	0.6%	10.4	6.8%
Others	0.1	0.0%	0.6	0.4%

Table3. Top Five Smartphone Operating Systems, 1Q 2013 (Units in Millions). Source: IDC (May 2013) [11]

We also considered in our research the steganography applications available on Google Play. Most of them treat steganography and the secrecy of the communication lightly. None of them offers the advantages of SmartSteg presented in this paper.

3 The Proposed Solution

Based on Kerckhoff's principle we choose to work with secret key stegano algorithm because in this case no unauthorized person should be able to extract the secret information even the specifications of the algorithm are public.

Our proposed application, SmartSteg, works on Android smart phones. We select BMP Bitmap format for the cover images because it is a lossless format and allows embedding large quantity of information. The designed programming language for mobile application that runs Android Operating Systems is JAVA using Eclipse environment.

In our study due to Android's support of multiple devices we have encountered some problems regarding how Android manages stored images both on SD card and internal memory of a device and on different versions of Android.

Most of the applications developed in this domain are using an image view tool to obtain the cover image. The image view tool does not access directly the original image file. It makes a copy of the original image file and transforms it in an (.png) image type no matter the type of the original image. This technique reduces very much the dimension of the cover image and this is not proper for LSB because it reduces the quantity of secret information which is to be hidden. SmartSteg is able to manipulate carrier images of MB dimensions usually transferred through Internet and Mobile Networks.

This is the main reason why we worked to find a way to access the original digital image file stored on SD card or in phone's memory. This is quite a challenge on Android platform because the way to access the system root folder is different depending on Android's edition and is not widely spread among programmers.

To process the data SmartSteg follows these steps:

- Cover image, secret file, and the secret key are loaded into application.
- SmartSteg verifies the dimension of the two files (cover image and secret file) to see if they are suitable.
- The secret file, its dimension and its execution are encrypted by means of a stream cipher algorithm using the secret key. The encrypted bits are stored in a temporary array.
- LSB algorithm starts to embed secret bits inside the cover image file using the pseudo random function completed with modulo 3 operations. The purpose of this random algorithm is to spread the secret message over the cover in a rather random manner. The purpose is to create confusion for the possible steganalitic attack. Since the secret message will normally not cover the entire support file the embedding process will continue until end of cover.
- The cover image with the secret file embedded is saved and can be transmitted to an intended receiver via e-mail.

4 Design and Implementation

The characteristics of smart phones used for testing:

- Samsung GT-S5670, Android: v 2.3.4, Processor: 600 MHz
- Samsung Galaxy Nexus I9250, Android: v4.0, Processor: Dual-core 1.2 GHz Cortex-A9

The characteristics of the cover image:

- Type: BMP file
- Dimension: 4.03MB
- Pixel arrangement: 1372x1029

Types of secret files:

- txt file: 400 kb that is approximately 100 printed A4 pages
- JPG file: 402kb, 3000x1682 shown in figure 5
- different image files: BMP, JPG; archives; pdf.

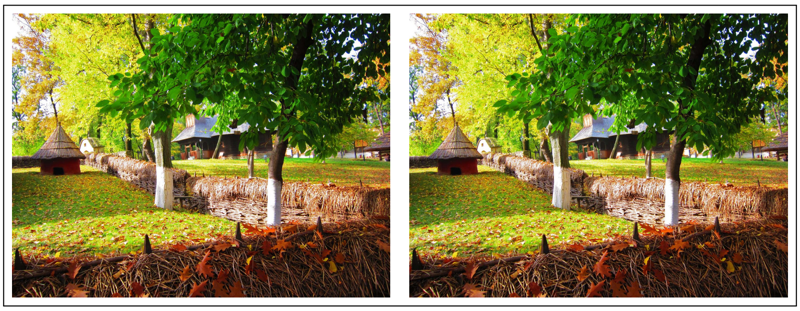
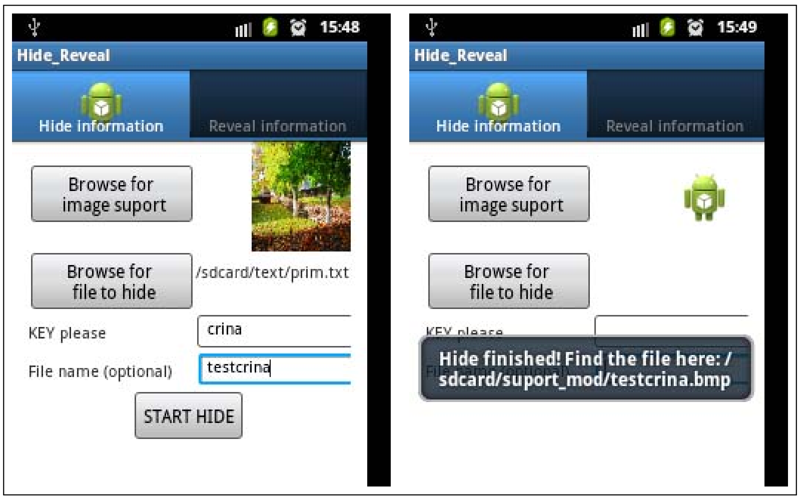


Figure 3: Cover image: original and with secret message embedded

Figure 4: Secret image file embedded in the cover image



/sdcard/text/prim.txt

KEY please: crina

File name (optional): testcrina

Hide finished! Find the file here: / sdcard/suport_mod/testcrina.bmp

Figure 5: User interface of SmartSteg

5 Conclusions and Future Works

In our SmartSteg application, we used a sort of LSB steganography on BMP files. The proposed algorithm has reached a very good processing speed. This is significant result, considering that we manage files of MB dimension on smart phones. So far, the performance of mobile phones have exceeded our expectations concerning the execution time necessary to encode, to hide, to decode or reveal secret information even using files of MB size. The dimension of the carrier file must be approximately eight times larger than the one of the secret file.

Advantages of the proposed model:

- Combines LSB steganography with stream cipher cryptography and random algorithm on smart phone devices.
- Works with large files both the carrier BMP file and the secret file.
- Hides a large variety of files.
- Execution time practical immediately.
- The security of the proposed model lies in the usage of secret key.
- Works on different versions of Android operating system.
- The sender can take pictures with phone camera and then converts them into BMP files using them as image cover.

Future work in our research is to develop a new version of SmartSteg that is windows based. The purpose of this idea is to permit secret communication between computes and smart phones.

Bibliography

[1] I. Rosziati, L. C. Kee, MoBiSiS: An Android-based Application for Sending Stego Image through MMS, *ICCGI 2012 : The Seventh International Multi-Conference on Computing in the Global Information Technology*, 115–120, 2012.

[2] S. F. Mare, *Advanced Steganographic algorithms and architectures*, Teze de doctorat ale UPT, Seria 10, Nr.40, Editura Politehnica, 2012.

[3] W. Mazurczyk, M. Karas, K. Szczypiorski, SkyDe: a Skype-based Steganographic Method, *Int J Comput Commun*, ISSN 1841-9836, 8(3):432-443, June, 2013.

[4] D. S. Purkayastha, N. Singhla, Android Optimization: A Survey, *International Journal of Computer Science and Mobile Computing - A Monthly Journal of Computer Science and Information Technology*, 2(6):46-52, June 2013.

[5] P. H. Rughani, H. N. Pandya, Steganography on Android Based Smart Phones, *International Journal of Mobile & Adhoc Network*, 2(2):150-152, May 2012.

[6] K. Szczypiorski, Steganography in TCP/IP Networks. State of the Art and a Proposal of a New System-HICCUPS, http://www.tele.pw.edu.pl/krzysiek/pdf /steg-seminar-2003.pdf, visited on 01.09.2013.

[7] T. F. M. White, J. E. Martina, Mobile Steganography Embedder, 11 SBSeg Simposio Brasileiro Em Seguranca Da Informacao E De Sistemas Computacionais, Bsalia-DF, 6 a 11 de Novembro de 2011, http://www.peotta.com/sbseg2011/resources/downloads/wticg/91964.pdf, visited on 01.09.2013.

[8] H-J. Yoon, A Study on the Performance of Android Platform, *International Journal on Computer Science and Engineering*, 4:532-537, 04 April 2012.

[9] B. B. Zaidan, A. A. Zaidan, A. K. Al-Frajat and H. A. Jalab, On the Defferences between Hiding Information and Cryptography techniques: An Overview, *Journal of Applied Sciences*, 10(15): 1650-1655, 2010.

[10] ***, Gartner Press Release, *Gartner Says Asia, Pacific Led Worldwide Mobile Phone Sales to Growth in First Quarter of 2013*, 14.05.2013, http://www.gartner.com/ newsroom/id/2482816, visited on 01.09.2013.

[11] ***, IDC Press Release, Android and iOS Combine for 92.3% of All Smartphone Operating System Shipments in the First Quarter While Windows Phone Leapfrogs BlackBerry, According to IDC, 16.05.2013, http://www.idc.com/getdoc. jsp?containerId=prUS24108913, visited on 01.09.2013.

[12] MobiStego: http://play.google.com/store/apps/details?id=it.mobistego, visited on 01.09.2013.

[13] Pixelknot: http://guardianproject.info/apps/pixelkont/, visited on 01.09.2013.