A Comparative Approach of the Efficiency of Modern Steganography Techniques for Mobile Devices

Dominic Bucerzan
Department of Mathematics-Informatics
"Aurel Vlaicu" University of Arad
Arad, Romania
dominic@bbcomputer.ro

Crina Raţiu
Department of Engineering and Computer Science
"Vasile Goldis" Western University of Arad
Arad, Romania
ratiu_anina@yahoo.com

***Abstract*—Cryptography and Steganography are two commonly used techniques in modern era for ensuring confidential and private communication. These techniques complete each other offering multiple layers of safety, enhancing digital information security. In this paper we analyze Smartsteg, which is a project that implements cryptography combined with steganography on mobile devices that run Android and Windows. We evaluate the performance of this project in terms of: interoperability, security, payload capacity, speed and robustness against steganalysis.**

***Index Terms*—SmartSteg; LSB Steganography; Cryptography; Android; Windows; Performance Analysis.**

I. INTRODUCTION

The decreasing costs of hardware equipment, due to the modern era technological development, make possible the sharing of digital information more rapidly and economically.

Today industry produces smaller, faster and high-performance mobile devices, which can support a wide range of features and open source operating systems [1]. Based on Gartner studies [2] figure 1 shows the usage of mobile devices in 2014 and a prediction for mobile devices usage for the years to come.

In modern society, digital information has become an asset. In contrast with this high level of development digital information security threats persist. Today we have to face an ongoing and never ending process of ensuring privacy, confidentiality, integrity and availability of digital information. Securing digital information has become an interdisciplinary process that is constantly optimized and innovated.

In this article we approach two widely used techniques for securing digital information namely Cryptography and Steganography. Cryptography scrambles the information in such a way that it becomes indecipherable to unauthorized access. Steganography allows to create a communication channel in an undetectable way, without drawing suspicion to the very existence of the secret data transaction.

These techniques were compared and debated among researchers and the result was a method to enhance digital information security, namely the combination of the two techniques. This solution has been studied, developed and implemented generating complex algorithms in PC environment.

The open environment of nowadays available networks for communication is full of threats and risks. In order to enhance the security of digital information, specialists propose, as a method, the combination of the above mentioned techniques.

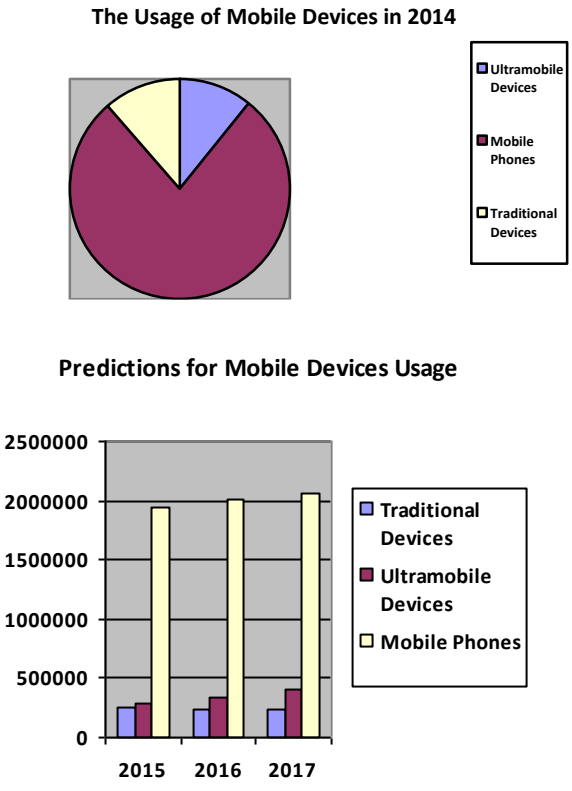


Fig. 1. Usage of mobile devices in 2014 and a prediction for the years to come [2]

II. SMARTSTEG DESCRIPTION

This paper is based on SmartSteg project [13]. SmartSteg is a robust solution for confidential and private communication. It proposes to transfer cryptography combined with steganography on mobile devices and to develop the opportunity of interoperability between traditional and mobile devices. All this in the following scenario: large quantity of embedded data, consuming minimal resources and minimizing the steganalysis detection.

SmartSteg allows to secretly transferring different types of files using devices that run Android and Windows. It uses secret key cryptography and steganography combined with a pseudo random selection function.

The programming language that we used for designing SmartSteg is JAVA within Eclipse environment.

A. Encryption

We choose to work with stream cipher for encoding the secret file. We used stream ciphers because they are characterized by [5]: small size, high speed, minimal consumption of computational resources, these properties making them proper for running on mobile devices. Encryption is accomplished by combining plaint text secret file with the secret key. Usually this is done using the bitwise operation XOR.

In the literature there is a large variety of stream ciphers proposed algorithms, yet the majorities are proprietary and confidential. SmartSteg uses a symmetric stream cipher secure and fast algorithm.

B. Pseudo Random LSB Selection

Pseudo Random selection function aims to remove the major risk raised by least significant bit (LSB) technique. Its role is to remove the possibility that an attacker may select and unify the last bits of the bytes of the cover file, in order to get the secret information.

In developing this function we had the following objectives: easy implementation, high security, simple and fast, minimal time consuming and hardware, creating as much confusion and diffusion, string generated numbers to be unpredictable, producing numbers as vague correlation.

Pseudo Random selection function result is within the range of modulo 3 values: 0, 1 or 2. These values are used to settle the number of least significant bits of a byte from the cover file that will embed secret information. A byte of the cover file may contain zero, one or two bits of secret information. This process continues until the end of cover file is reached, to obfuscate the length of secret file.

C. Embedding

In the embedding process, the encoded secret file is integrated in the cover file. We choose to work with bitmap image files (BMP) as cover because they are proper for LSB technique, they can support large quantity of embedded data and it is a device independent format.

SmartSteg proposes to use randomly the LSB 3 bits of every color to embed the encoded secret file. According to the proposed pseudo random selection function a byte of color can contain 0, 1 or 2 bit of secret information. This alteration of the LSB does not produce any visible changes to the cover file. In our study we have some results regarding LSB alteration, namely, if some changes are made to the values of the last five bits of a color byte, the human visual system cannot distinguish the original image from the altered one.

SmartSteg can process cover files up to 16 megabytes (MB) dimension and secret files up to 2 MB dimension. It keeps the tradition LSB ratio of embedding 1 bit of secret information to 8 bits of cover file. The proposed solution reaches a good speed.

III. PERFORMANCE ANALYSIS FOR SMARTSTEG

In this study we evaluate the performances of SmartSteg project on mobile devices in terms of: interoperability, security, payload capacity, speed and robustness against steganalysis. We compared the obtained results with the values of performances reported by other steganographic solutions. These steganographic systems are presented in [6], [7], [8], [9] and [10]. We do not have access to the source cod of these solutions to perform the measurements we need to compare with SmartSteg performances. This is the reason why we compare SmartSteg tests results with the reported ones of these techniques.

A. Interoperability

SmartSteg is a project that offers interoperability between devices that run Android and Windows. In the literature, most steganographic system are designed only for a specific operating system. This means that the sender and the receiver must have devices that run the same operating system.

For example: 4-LSB [6] [7], MoBiSiS [9], MobiStego [10], Android-Stego [8], are some proposed steganographic systems for Android. In the literature there are some proposed solutions especially designed for PC, from which we choose as relevant: the project developed on Skype steganography [11] and the researches made in [12] and [14].

In this paper we analyze SmartSteg performances especially from the point of view of Android devices. We consider it's interoperability an important feature that highlights it from the other steganographic systems. In the same time we are aware that there are steganographic systems that run Windows and reach higher performances.

B. Security

Today the majority of steganographic systems offer double layer of security. First the secret information is encrypted and only then the encrypted information is embedded in the cover environment.

SmartSteg keeps this feature and provides two layers of security for the secret information. First the secret information is encrypted using a proprietary algorithm HENKOS that is based on symetric key (see encryption process II.A.). Second the encrypted information is embedded in the cover file using

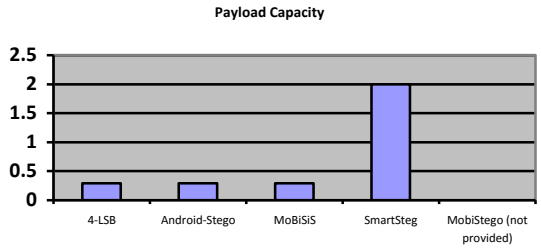
an improved LSB algorithm, based on the pseudo random selection function (see embedding process II.C.).

C. Payload capacity and variety

Payload capacity and variety was a main target to achieve when developing SmartSteg. Other steganographic systems that run Android are developed to conceal only short text messages or small images. One of the reasons is because they use Multimedia Messaging Service (MMS) for transferring the cover file with embedded secret data. When using MMS the maximum size of a file that can be transferred is 300 kb, this means that the amount of secret data is small. Another reason is the fact that some steganographic systems use as a cover the icon created by the image view tool when the sender loads the cover file. This does not access directly the original cover file from the memory to use it as a cover file.

The applications that we analyzed reach the following performances: 4-LSB [6] [7] uses MMS and can embed an image, text or audio in an already transferred image using MMS; MoBiSiS [9] uses MMS and can embed text in an image, MobiStego [10] uses MMS and can embed text in an image; Android-Stego [8] uses MMS and can embed a file in an image.

SmartSteg stands out from the rest of the steganographic systems that run Android because it can conceal any type of file, up to 2 MB dimension. The application is able to access the cover file and the secret file directly from the device's memory or from the SD-card.



D. Speed

Considering the performances achieved by HENKOS on PC platforms, the processing of secret information of 2 MB with SmartSteg is done in a very short time. SmartSteg reaches a good speed value. It can process cover files up to 16 MB dimension and secret files up to 2 MB dimension. The process speed make viteza procesului in cazul SS o face folosibila pt utilizatorii de platform mobile seems quick for human perception.

We tested SmartSteg's speed on different types of devices (smart phones, tablets, laptops) and different versions of Android and Windows. For the same task the time used by the new generation of smart mobile devices (multi core processors) is less than half of time used by old generation o mobile devices (single core processors).

We made tests measurement using wall clock time in java. These test confirm that time used by operating system is minimal (between 0 and 100 milliseconds) and do not influence SmartSteg process.

The testing platform consists of four different mobile devices: Samsung Galaxy S6 edge, Sony Xperia Z3 Compact, LG Nexus 5 and Asus Fonepad. SmartSteg functionality is proper on all tested devices.

For a cover file of 2329 kb, time values (*in milliseconds*) for SmartSteg process varies:

- For the old generation of mobile devices between 1500 and 1800;
- For the new generation of mobile devices between 400 and 600.

Regarding the other application that we compared our result with (4-LSB, MobiSys, MoBiSiS, MobiStego, Android-Stego), none of them offers any information regarding the speed they reach.

E. Steganalysis

When doing Steganalysis we took into consideration the differences and the similarities between the cover file and the resulted file with embedded secret information. We select these indicators based on the data that we had about the performances reached by the application that we compared SmartSteg with.

Mean Squared Error (MSE) represents the difference between the original cover image and the resulted image with embedded information. See equation (1) where: MxN –image dimension, p –original image, q –image with hidden data.

$$MSE = \frac{1}{MxN} \sum_{i=1}^{M} \sum_{j=1}^{N} (p_{ij} - q_{ij})^2 \quad (1)$$

A low value of MSE means that there are unnoticeable differences between the two images. A high value of MSE means that there are distinguishable differences between the two images. MSE defines the Peak Signal to Noise Ratio (PSNR) indicator.

Peak Signal to Noise Ratio (PSNR) is measured in decibels and it is the similarity between two images. See equation (2) where: $C_{\max}^2$ is the maximum pixel value in the image.

$$PSNR = 10x\log_{10} \frac{C_{\max}^2}{MSE} \quad (2)$$

PSNR represents the ratio of the maximum possible value of a pixel and the intensity of distortion to the image. A high value of PSNR means unnoticeable changes between the original image and the resulted one after embedding.

Table 1 shows the values of MSE and PSNR recorded by SmartSteg and the application that we compared it with.

TABLE I. MSE AND PSNR VALUES

Steganographic system	Cover Image Size	MSE	PSNR
4-LSB [6] [7]	200 X 142	8.2693	38.9561
	200 X 142	6.2098	40.2001
	200 X 142	5.1030	41.0526
	150 X 203	4.9885	41.1511
	150 X 203	4.5364	41.5636
Android-Stego [8]	<= 300 kb impose by MMS	Not provided	Not provided
MoBiSiS [9]	<= 300 kb impose by MMS	Not provided	70.7586
		Not provided	69.0479
		Not provided	74.6493
		Not provided	72.6493
MobiStego [10]	Not provided	Not provided	Not provided
SmartSteg	1440X1080	3.8562	51.5229
	1155X679	3.0002	52.6131
	1613X1210	2.6401	53.4570
	2272X1704	3.0060	52.8933

Relation (1) and (2) show the fact that the dimension of the cover image is an important factor that influences MSE and PSNR indicators. Regarding this fact we consider these measurements irrelevant for small images. Also, we note that to conceal the size of the secret file, SmastSteg processes the entire cover file even if the secret file is much smaller.

IV. CONCLUSIONS AND FUTURE WORK

Table 2 presents a comparison between the performances achieved by the steganographic systems analyzed in this study. Of these, SmartSteg stands out with high speed, payload capacity, payload variety, interoperability and resistance against steganalysis. These features prove SmartSteg's capability to be robust and stable solution for steganography on mobile platforms.

We choose to design SmartSteg in modular way. This approach allows to expand new facilities or to improve performances. A model that we proposed in a further development of the project is an implementation of public key cryptography instead of existing solution that uses stream ciphers for symmetric key cryptography.

TABLE II. MSE AND PSNR VALUES

Stegano-graphic System	Security	Payload capacity variety	Speed	Stega-nalysis	Intero-pera bility
4-LSB [6] [7]	AES Encryption + Steganography	< 300 kb Text Message, Image Files	Not provided	Irrelevant	No
Android-Stego [8]	Public Key Cryptography+ Steganography	< 300 kb Secret Message	Not provided	Irrelevant	No
MoBiSiS [9]	Steganography	< 300 kb Text Message	Not provided	Irrelevant	No
Mobi-Stego [10]	Steganography	Not provided Text Message	Not provided	Not provided	No
SmartSteg	HENKOS Simetric Cryptography + Steganography	<= 2MB Any File Type	Test results in section III.D.	High	Yes

REFERENCES

[1] D. Bucerzan, C. Raţiu: Image Processing with Android Steganography, presented at the 6th International Workshop Soft Computing Applications (SOFA 2014), Timisoara, Romania, held on July 2014

[2] ***: Press Release, Gartner Says Global Devices Shipments to Grow 2.8 Percent in 2015, Egham, UK, March 19, 2015, available at: http://www.gartner.com/newsroom/id/3010017, visited on 25.06.2015

[3] D. Bucerzan, M. Gheorghiţă: HENKOS - A New Stream Cipher: Performance Analysis, WARTACRYPT 2004 The 4th Central European Conference on Cryptology, Bedlewo, Poland, held on July 2004.

[4] D. Bucerzan: A Cryptographic Algorithm Based on a Pseudorandom Number Generator, SYNASC 2008, Timisoara, Romania, held on October 2008

[5] D. Bucerzan, M. Crăciun, V. Chiş, C. Raţiu : Stream Ciphers Analysis Methods, Int. J. of Computers, Communications Control, ISSN 1841-9836, E-ISSN 1841-9844 Vol.V (2010), No. 4, pp. 483-489

[6] G. R. Kshirsagar, S. Kulkarni: Implementation of Hybrid Algorithm for Secured Multimedia Messaging Service System Using Android, Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering - CEEE 2013, ISBN: 978-981-07-6260-5 doi:10.3850/ 978-981-07-6260-28

[7] V. Jeswani, S. Kulkarni, M. Ingle: Android Application Development for Secure Data Transmission using Steganography, Transactions on Networks and Communications, Volume 3 No 3, June (2015), pp: 39-48

[8] A. Srinivasan, J. Wu, J. Shi: Android-Stego: A Novel Service Provider Imperceptible MMS Steganography Technique Robust to Message Loss, Accepted to appear in 8th International Conference on Mobile Multimedia Communications, May 25 - 27, 2015, Chengdu, People's Republic of China

[9] R. Ibrahim, 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, ISBN: 978-1-61208-202-8

[10] ***: Mobistego, available at: http://mobistego.sourceforge.ne t/index.html, vizited on 27.06.2015

[11] 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.

[12] Vinod K. Madan, Sunil H. Karamchandani, Krutarth J. Gandhi, Siddharth R. Gosalia, Shabbir N. Merchant, Uday B. Desai: PCA Encrypted Short Acoustic Data Inculcated in Digital Color Images, Int J Comput Commun, ISSN 1841-9836, 10 (5), 2015

[13] D. Bucerzan, C. Raţiu, M. J. Manolescu: SmartSteg: a New Android Based Steganogrphy Application. In: International Journal of Computers Communications \& Control, vol. 8(5), pp. 681-688 (2013) http://univagora.ro/jour/index.php/ijccc/article/view/642

[14] A. Majcher: The application of mobile devices in the system for carbon measurement in volatile ashes from power industry boilers, PROBLEMY EKSPLOATACJI – MAINTENANCE PROBLEMS, ISSN :1232-9312, 2013