ANALYSIS OF THE STEGANOGRAPHY IN IMAGE WHIT MOBILE COMPUTING

Stoyanova V. T, PhD
National Military University, Faculty of Artillery, AAD and KIS,
1 Karel Shkorpil Str., 9700 Shumen, Bulgaria

veselka_tr@abv.bg

АНАЛИЗ НА СТЕГАНОГРАФИЯТА В ИЗОБРАЖЕНИЯ С ПОМОЩТА НА МОБИЛЕН КОМПЮТИНГ

гл.ас. д-р инж. Стоянова В.Т.
Национален Военен Университет „Васил Левски”,
Факултет „Артилерия, ПВО и КИС” гр. Шумен
ул. „Карел Шкорпил”1
veselka_tr@abv.bg

Abstract: *The report examines the use of steganography as a method of hiding text, images or sound recordings in file-carrier for mobile devices, which may give the opportunity to keep the correspondence without awaking any suspicion. The information file is hidden in the file-carrier by the method Least significant bit (LSB) through various algorithms of coding. The experimental part compares mobile applications, which are using Steganography methods and compares their advantages. The experimental results show that the Ultra Mobile Steganography is realizing with fast pace, the applications have common static characteristics of the cypher image and are easy to use***.

Keywords: STEGANOGRAPHY, LSB, MSE, PSNR

1. Introduction.

The development of modern technology in our daily lives is evidenced by the wide distribution of the well-known smartphones. The statistics shows that the total number of smartphones users worldwide for 2016 already reached 2.1 billion users and also expects that by 2019 will exceed more than 2.71 billion users [1]. The high rates of users, which develop and use social networks, facilitate the dissemination of media files by sharing them to a wide range of people. Despite the convenience to share free images, audio and video files, the steganography transmission of messages through social networks is hampered by the policy of the most networks to compress the files, which are shared. With the reducing the size of the file, the embed message becomes destroyed. In that case the secret conversation becomes unavailable, due to lack of opportunity for discovering the secret message.

Mobile technologies have already entered our lives seriously and have become an integral part of it. Through them various types of activity can be carried out. From playing different types of games to managing your personal finances.

“Statista“ Figure 1 shows that from 173.5 million units in 2009, Smartphone sales to end-users have reached 1,432.9 billion units in 2016, which means sales have increased more than 8 times, expected in 2019. Sales to be over 1,862.3 billion. Total sales over the 10-year period will exceed 11.2 billion(see Fig.1).

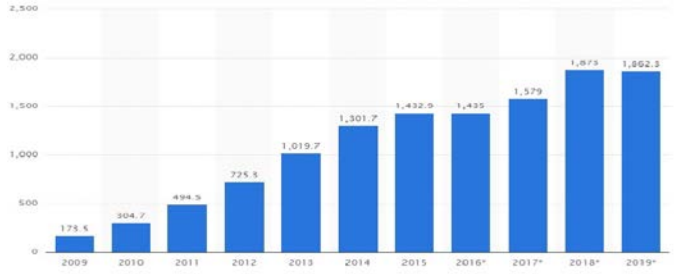
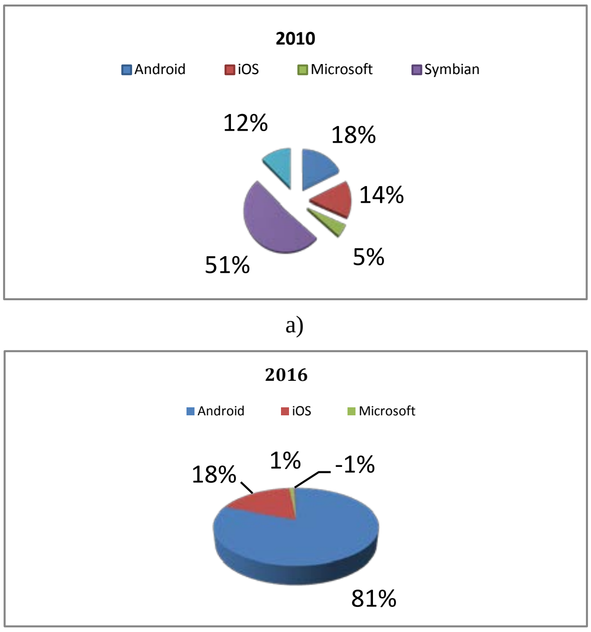


Fig. 1. *Sales of smartphones [1]*

With the increase in production, the market shares of smartphone operating systems sharply change (see Fig. 2a and 2b). In 2010 Android-17.2%, iOS-14.1%, Microsoft-4.9%, Symbian - 50.2% and others - 12%, while in 2016 Android OS reached a record 80.7% ,iOS-17.7%, Microsoft-1.1% and other OSs - 0.5%, and Symbian is not even produced.



a)

b)

Fig. 2. *Market Share in a) 2010[2] and b) in 2016 [2].*

With this impressive development, the involvement of the technologies in our lives also arises with the issue of the security and protection of the personal data of the mobile user. When it comes to security issues, smartphone users scamperly believe that the phone is safer than the computer.

According to Martin Hack, vice president of the NCP, who says that if you have access to some information on your smartphone, the hackers will have it too.

There are many of definitions for the Steganography as science, which describe it like a hidden method or art, which is used for hiding a secret information in unsuspicious file-carriers [3], [5], [6]. Steganography as part of the science Steganology, which includes both Steganography and Steganalysis, is divided into two main types. Conventionally speaking, the first type we call classical steganography, which was established with the sole purpose to summarize the set of historically evolved methods, systems, techniques and applications, and the other type - high-tech steganography. The high-tech steganography on the other hand can be divided into IT-steganography, biological-steganography and etc.

Object of our attention is the IT-steganography, which consists the computer steganography, linguistic steganography and network steganography in itself. The computer steganography has two main ways to hide the information. The first one is using the special properties of the computer formats, and the second one is using already converted into discrete form signals, which are having continuous analog nature (images, video, sound).

2. Steganography methods

2.1. Steganography in mobile computing

It is possible to counteract the compression process by using files of smaller sizes, which do not require interference with the compression algorithms from the site, in which the information is shared.

Due to the rapid pace with which the smartphones market is growing, the developers of software applications for mobile devices have developed numerous applications that can hide information and a certain portion of them are free [3]. Media files that are used by mobile applications for hiding the information, for the most of the part, are images, but there are a large number of applications that are using for a file-carrier audio or video files.

Examples of free Steganography applications are the applications: "Hide it in", "Acoustic Picture Transmitter Pro", "Stegais", "DaVinci Secret Image";

To be successful the transmission of hidden information prerequisite is the consumers who share it to use the same application on their mobile devices, because each application is coding in its own method of embedding the message in a carrier file and require the same application to decode this same file carrier.

2.2. Exploring the possibilities of the programs:

Stego-image 24-bit format file storage using *RGB* (Red, Green, Blue) color model [7] is a prerequisite for the presence of a large excess of information that can be used for the purpose of steganography. Steganography synthesized algorithm for embedding information in images uses up to three of the last significant bits in each color channel pixels

"Stegais" and "Da Vinci Secret Image", as mentioned above, are free mobile applications which services are for hiding information by steganography methods. The information that can be transmitted in Stegais can be text or sound, and in Da Vinci Secret Image is text only. There is a possibility for both of the applications the messages they transmit to be encoded by the method *AES* (Advanced Encryption Standard), which is one of the most widely used cryptographic algorithms, another possibility for the secret text is to be written in both Cyrillic and Latin, since both applications support standard *UTF-8* (Universal Transformation Format 8-bit.). The main advantage in both applications is the relatively simple and easy to use interface consisted of a few simple steps:

- Create a secret message;
- Select the image file from the library-media or create an image through the camera of the device;
- Select on / off option for encoding;
- Select the button "Hide" to use the algorithm to hide;
- Save the file carrier carrying a hidden message in the device memory or send it by an e-mail to the receiver;

As a major disadvantage can be noted the fact that in both applications the carrier-file that is used to transmit data can be only image file.

Another feature is that images that are used as files-carriers must be of format .jpg or .png, which are widely distributed and used by photographic and complex images or as stored images, that are created with the most of the types of smart phones.

For the experiment is used the base image for comparison - "monkey.bmp" (see Fig. 3), which is converted into formats .jpg and .png. To track the changes in the image and the embed hidden text, the carrier-images of Stegais and DaVinci Secret Image are compared sequentially by Mathlab software.

Fig.3. *Test imege, Monkey.bmp*

To obtain the most objective data for both applications, their images are tested in all possible cases of embedding text.

The tests consists in a study of the mean square error after changing the image - MSE (Mean Squared Error), study of the signal - noise -SNR (Signal-to-Noise Ratio), the peak of the signal - noise - PSNR (Peak Signal- to-Noise Ratio) and the entropy. The calculating of the MSE is a standard static method for objective measurement of the level of difference between two images. The low value of MSE means that the average level of difference between the images is low. In case of two equal images, the MSE value is zero. Unlike MSE, higher value of PSNR means that the quality of the image is higher. In case of two equal images the PSNR value is near infinity. The main idea of all of the steganography methods is to minimalize the MSE and maximize the PSNR

The studied characteristics are represented with the formulas (1) and (2), where *PSNR* is based on the values of *MSE*:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2, \quad (1)$$

where *m* and *n* are width and height of the image*; l (I, j)* and *K(I, j)* are respectively pixels with coordinates (I, j) in the original and the steganography-image.

$$PSNR = 10.\log_{10}(\frac{max^2}{MSE}) = 10.\log_{10}(\frac{max}{\sqrt{MSE}}), \quad (2)$$

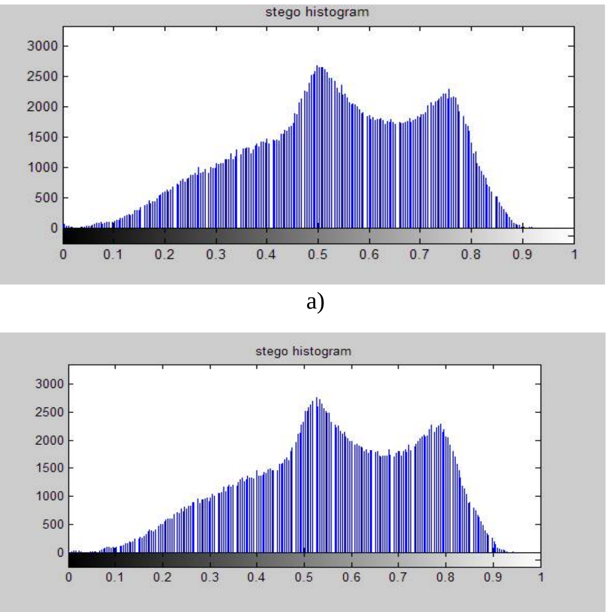
where *max* = 255 for 8 bit images.

The degree of similarity of the images before and after the process of embedding of data, valued with *MSE* and *PSNR*, define the quality of the steganography image. When the similarity between the studied images is low, is accepted that the quality of the steganography image is also low [4].

3. Experimental results.

By implementing a programs for embedding/ extracting text messages many tests with different size messages and images have been carried out. The studied algorithm is based on the *LSB* method applied and tested on *BMP* image formats. Test results of the qualitative characteristics *MSE*, *SNR* and *PSNR* are analyzed. Visual analysis of the compared images shows lack of visual differences in visual control. Histogram analysis and the results of the qualitative characteristics are obtained by MATLAB. Table 1 presents the results of the qualitative characteristics of embedded text files in English and Bulgarian with a size of 6 B to 15 B and cover digital image *Monkey.bmp* is used.

The results obtained from the study are filled in table 1, and the test histograms visualizing images are proposed in fig. 4.



a)

b)

fig. 4*. Histogram of stego-image, which has 15 kB of embedded information whit a) Stegais and b) Da Vinci Secret Image*

Table 1: *Qualitative characteristics of Monkey image in embedding a different size of the secret message*

Text	Format type of the image	Application	Size of text [bit]	AES pass	MSE aver	SNR	PSNR
Cyrillic	.jpg	Stegais	15	-	10.9720	23.3884	28.7094
Cyrillic	.jpg	Stegais	15	+	10.9721	23.3884	28.7094
Latin	.jpg	Stegais	6	-	10.9717	23.3885	28.7094
Latin	.jpg	Stegais	6	+	10.9717	23.3884	28.7094
Cyrillic	.png	Da Vinci Secret Image	15	-	9.8509	22.8895	28.2105
Cyrillic	.png	Da Vinci Secret Image	15	+	9.8508	22.8895	28.2105
Latin	.png	Da Vinci Secret Image	6	-	9.8510	22.8895	28.2105
Latin	.png	Da Vinci Secret Image	6	+	9.8509	22.8895	28.2105

In Figure 5 can be seen histograms of original and stego-image obtained by embedding of 15 B information at base settings of the steganography algorithm whit Stegais, i.e. successively embedding in the three color components of pixels without using protection by stego-key in a pepper.bmp cover image

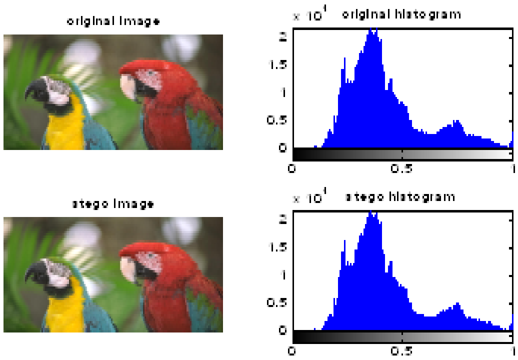


fig. 5. *Histogram of original and stego-image, which has 15 B of embedded information whit Stegais*

Difference in the histograms is hardly observed. This result can be attributed to the fact that the embedded message is not particularly large.

4. *Conclusion*

From the results it can be deduced that the applications do not establish substantial modification of the basic image by embedding text and that there is a minimal difference in the data as the presence of a key, and in his absence. But with -Low levels of entropy and noise that are expressed in the form of the hidden text in the image, the app that is distinguished is the Da Vinci Secret Image application.

Even the popular free distributed applications for steganography transmitting data are sufficiently reliable and secure to be able to send important information without raise suspicion at anyone.

- The used cryptographic algorithm ensures additional security during transmission and recovery of the stego-message.
- In embedding in the same image of equal length messages in Cyrillic and Latin, the stego-images obtained have approximately 0,0001 difference in the values of the parameters examined

References:

[1] Statista, http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/, reviewed on 30/03/2017

[2] Statista, http://www.statista.com/statistics/263441/global-smartphone-shipments-forecast/, reviewed on 30/03/2017

[3] Greene T., Network World, http://www.networkworld.com/article/2291708/security/130370-15-FREE-steganography-apps-for-mobile-devices.html#slide1 reviewed on 30/03/2017;

[4] Stoyanova V, Tasheva Zh. PhD, “Research of the Characteristics of a stenography algorithm based on LSB method of embedding information in images” National Military University, Faculty of Artillery, AAD and KIS, Shumen;

[5] Zhelezov S. Paraskevov H., S. Stanev, Hristov H. "Manual exercises steganography" University Publishing House "Ep. Konstantin of Preslav" Shumen, 28.02.2015;

[6] Kessler D., Forensic Science Communications, http://www.garykessler.net/library/fsc_stego.html reviewed on 31/03/2017

[7] Cox I. J., Miller M. L., Bloom J.A., Kalker T., Fridrich J. „Digital watermarking and steganography“. Second Edition, Burlington, MA, USA: Elsevier Inc., 2008.