An Improved Method for Steganography on Mobile Phone

MOHAMMAD SHIRALI SHAHREZA
Allameh Helli Pre-University
Ghafari Street, South Kargar Street
Tehran, Iran
http://mohammad.shirali.ir

Abstract - In this paper I introduce an improved method for hiding data in images or steganography. This method is used for secure data transfer from a computer to mobile phones. In this method a message can hide in an image on a PC using a password.

The user can download this image from the computer to his mobile phone. The decoder program running on his phone will extract the hidden information by a Java program. The decoder program was installed on a Nokia 6600 mobile phone and tested by posting the students' grades over it.

Key-Words - Steganography, Watermarking, Mobile phone, Wireless communication, PNG image format, J2ME, Security

1 Introduction

The development of digital devices, introduces a rapid growth in the wireless communication systems. One of the areas of communication in which the growth is significant includes the mobile phone industry. A mobile phone is not only a phone but also a small and portable computer. It can connect to the internet, produce or show digital images, generate and play movies and music. It can be used as electronic cash or a game playing system, etc. People, especially young people, like mobile phones very much. On the rapid use of these systems, the security is a big issue.

Many hackers try to attack mobile phones. The extensive use of these systems increases the possibility of the intrusion. Therefore the security of the information transferred into these devices becomes a major issue for users and developers.

A new approach for protecting the information is to use steganography. In this paper I introduce an improved method for hiding data into image for mobile phones. Because sending and receiving images are common on the mobile phones, the hackers are not attracted to attack the system. Other advantages of this method are its simplicity and wide range of application. I used this method for announcing students' grades via internet to mobile phones.

2 Method

In this project I hide information in the least significant bits (LSB) of pixels colors. In this method each byte of information is hidden in two pixels. For hiding the information a byte is divided into eight bits. By using a password, two pixels are selected in which a byte of information is hidden. I introduce an algorithm to select the pixels in the next section.

After selecting the pixels we hide a byte within them. Each pixel has three colors (RGB), and the information is stored in the LSB of these colors.

The changes of LSB may not be detected because of the imperfect sensitivity of the human eyes. It seems that the human eyes are less sensitive to blue colors, so more significant changes may be applied to blue colors, before the changes be recognized. Therefore each byte of information is hidden into two pixels. The number indicating the size of information is stored in the image as well. Knowing the size of the information is necessary for decoding correctly the information.

In order to select the pixels in which data will be hidden a new algorithm is developed. Since the pixels containing the information are not sequential, it is difficult for stegano analysis software to detect the stegano images.

The PNG format is used to represent images. This format is common for representing images on mobile phones and the Java language supports this format. The PNG format is lossless. It uses compression therefore the size of the image is relatively small.

The decoding algorithm is the same as the coding algorithm. The coding and decoding algorithms are written in Java language. Because the decoding must run on a mobile phone, I used a special version of Java for the mobile phone called “Java 2 Micro Edition” or J2ME.

3 The Coding Algorithm

In the usual steganography algorithms, information is hidden in the sequential pixels. Therefore anyone with the knowledge of the coding algorithm can extract the hidden information from the image. In this paper I used a new approach for selecting pixels according to a password. Using the password would cause to select the pixels in a random manner.

In the usual steganography algorithms, if the size of the information is small in comparison with the size of image, the attacker can find the pattern of altered pixels and extract the hidden information. But in this method, information is in random order pixels in each block, and extracting the hidden information is difficult.

On the other hand if the size of the information is large, the algorithm reaches the end of image. For solving this problem, it has to return to the beginning of the image and hide information in an empty pixel (an empty pixel is defined as a pixel of original image that has no hidden data). This process needs a large amount of memory to remember all empty pixels, but in the mobile phones we have a limited amount of memory. After all, finding an empty pixel needs a lot of time in coding or decoding phases.

The new method for hiding information is described here:

In this method the image is segmented into n blocks of m pixels. Then according to the password, a block is selected and the information is hidden in an empty pixel of this block.

The algorithm for selecting a block and an empty pixel in that block is as follows: if the selected block starts with the pixel number k and has m pixels then the number of the last pixel is k+m-1.

This algorithm uses an array of size m+1 for remembering empty pixels of current block. This array contains the number of pixels having no data. The last cell of the array is the total empty pixels in the current block. According to the password, an empty pixel is selected and the last empty pixel number is copied to this array cell. After this operation the total number of empty pixels on the block decreases by one.

This method is also used for selecting a block to hide the information in itself. The figure-1 shows the array before and after selecting a pixel.

k	k+1	k+2		k+i-1		k+m-2	k+m-1	m
1	2	3	…	i	...			

(a) The array before selecting an empty pixel.

k	k+1	k+2		k+m-1		k+m-2	null	m-1
1	2	3	…	i	...			

(b) The array after selecting an empty pixel.

Fig. 1. Selecting the next empty pixels

The advantage of this method is that there is no need to search for an empty pixel in the block, because we have the empty pixel numbers of the current block in an array. On the other hand by dividing the image into small blocks, it only needs a small amount of memory. We indicate that the size of memory is a critical factor among mobile phones applications.

If the image is very large, it can be stored on the hard drive and only one of its blocks is transferred to the memory and after hiding the information on that block, it is stored back on the hard drive.

This method swaps the last cell of the array with the ith cell of the array. The advantage of this work is that the pixels are filled in a random order and can not decode without knowing the password.

This method for hiding information in images can be used for secure communication, copyright protection, preventing undesirable changes in digital documents, protecting from unauthorized copying and other applications.

4 Experimental Results

This method is used for announcing students' grades on the internet. Students can receive their grades by a mobile phone. In this implementation, the students' grades are hidden in arbitrary images in PNG format by the coder program using a password. We have posted the images on the course website.

The students can connect to this website by their mobile phones and download the image. After downloading the image, they use the decoding program and a password for extracting their grades.

If they download the right image and use the correct password, they can get their grades.

The grades of 30 students were hidden into 30 images with the coded program using a password, and put on a web site. Then the students connected to the computer with a Nokia 6600 mobile phone and downloaded their images. After entering the correct password they get their grades. Based on this experiment we wish to claim that our method would be acceptable for implementation.

5 Advantages and Disadvantages

The advantages of this method are:

1- The probability that one can detect a stegano image is relatively low, due to the high volume of images exchanged between mobile phones and computers.
2- As far as I am aware, this is the first time that this method is used on a mobile phone
3- The password is not stored in the stegano image; therefore it is difficult to detect the password.
4- Because the password is used, it is difficult to detect the information hidden in the image.
5- The decoding program uses a few kilobytes of memory.
6- The program is fast enough.
7- There is no limitation for selecting the password.

The disadvantages of this method are:

1- There is a variety of mobile phones on the market for which there isn’t a standard operating system, so it is not possible to produce a coder program for all of them.
2- The stegano image is sensitive to the size and other characteristics of the image; therefore changing the image could destroy the hidden information.

6 Conclusion

This paper introduces an improved method of hiding information in image for mobile phones. This method allows a secure transfer of information between a computer and a mobile phone.

In this implementation students connect to the course web site via internet with their Nokia 6600 mobile phone and get their grades. It can use other kind of wireless communication such as Bluetooth to transfer data between computer and mobile phone.

This method can be extended to hide data into video clips and sound clips that are common on new mobile phones.

7 Acknowledgment

The completion of this technical research is the result of elaborate guidelines and consultations provided by my teachers in Allameh Helli High School , to whom I am grateful very much.

I would like to thanks Dr. Mashaei and Mr. Shahram Abdoli from Yazd University for editing the final version of this paper.

I would like to thank my mother for her consistent care, support and encouragement during the process of performing this research.

References

[1] R.J. Anderson, F. A. P. Petitcolas, “On the limits of the steganography,” IEEE Journal Selected Areas in Communications, Vol. 16, No. 4, pp. 474-481, May 1998.

[2] N. Cvejic, T. Seppanen, “Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method”, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC’04), Vol. 2, pp. 533, 2004.

[3] M. Ramkumar and A. N. Akansu, “A Robust Scheme For Oblivious Detection Of Watermarks / Data Hiding In Still Images”, Proceeding of SPIE, Vol. 3528, pp. 474-481, Jan. 1999.

[4] L. M. Marvel, C.T. Retter and C. G. Boncelet, “Hiding Information in Images”, Proceeding of International Conference on Image Processing, 4-7 Oct. 1998, Vol. 2, pp. 396-398.

[5] S. Venkatraman, Ajith Abraham, M. Paprzycki, “Significance of steganography on data security”, Proceedings of the International Conference on Information Technology: Coding and Computing, ITCC 2004, 5-7 April 2004, Vol.2, pp. 347- 351.

[6] L. Ehsan, F. Edrisi, Digital Steganography using DCT, MS Thesis, IRIB University, Tehran, Iran, 2002.

[7] N. Samsonchi, An Approach to Steganography for digital images, MS Thesis, Tarbiat Modarres University, Tehran, Iran, 2000.