Stealth Steganography in SMS

Mohammad Shirali Shahreza
Computer Science Department
Sharif University of Technology
Tehran, IRAN
shirali@cs.sharif.edu http://mohammad.shirali.ir

Abstract— **The short message service, abbreviated to SMS, is one of the services used in mobile phones and has been warmly welcomed by the public throughout the world, esp. in Asia and Europe. Using this service, individuals can write and send to each other short messages and also black and white pictures.**

On the one hand, considering the issue of information security and esp. establishing hidden communications, many methods have been presented for hidden communications, among which steganography is a relatively new one.

Combining steganography of data in picture and using pictures in SMS messages, this article proposes a method for hidden exchange of information. The main focus of this article is on steganography in B&W (black and white) pictures and making this possible on mobile phones considering the limitations in mobile phones.

After receiving a picture message containing hidden data, the decoder program extracts the data and immediately changes the steganography places. Therefore, the picture saved on the recipient's mobile phone will not contain any hidden information.

This paper has been implemented with J2ME (Java 2 Micro Edition) and has been implemented on a Nokia 6680 mobile phone.

Keywords—**Steganography, Stealth Text, Information Security, Binary Images, Mobile Phone, Short Message Service (SMS), Image Processing.**

I. Introduction

In 1985, Ernie made the first telephone call on the mobile phone in Britain. In less than two decades, however, the mobile phone has turned into a necessary device for people and now one out of every six individuals throughout the world has a mobile phone.

With the expanding use of mobile phones and the development of mobile telecommunications, telecommunication companies as well as companies manufacturing mobile phones decided to add additional features to their telephone sets in order to attract more customers. One of the services that were provided on the mobile phone was the SMS.

The SMS (Short Message Service) is the transfer and exchange of short text messages between mobile phones. The SMS is defined based on GSM digital mobile phones. According to the GSM03.40 standard [1], the length of the exchanged message is 160 characters at most, which are saved in 140 bytes depending to how information is saved according to the standards. These messages may be a combination of digits and letters or be saved in non-text binary form. Using the same binary messages, one can also send pictures as well. The pictures, however, are two-color and have a low quality.

SMS messages are exchanged indirectly and through a component known as the SMSC. SMS messages have the following advantages:

- Communication is possible when the network is busy;
- We can exchange SMS messages while making telephone calls;
- Sending offline SMS messages;
- Providing various services such as e-commerce.

One can also receive reports on the status of the SMS message or define a validity period for the SMS message [2].

In line with what was said above, the issue of information security and its importance has been increasingly important, esp. in establishing wireless communications in which there is the possibility of disclosure of confidential and personal information during exchange of information between various systems.

One of the important branches in information security is the issue of exchange of hidden information. To this end, various methods such as cryptography, steganography, coding, etc have been used.

The steganography method is one of the methods that have received attention in recent years. In implementation of this method, the main goal is to hide information in the cover of another medium, so that other persons will not notice the hidden information. This is a major distinction of this and the other methods of hidden exchange of information because, in the coding method for example, individuals notice information by seeing encoded information, yet they cannot comprehend the information. However, in steganography, individuals do not notice the existence of any information in the sources.

Most steganography jobs have been carried out on pictures [3, 4], videos [5], text [6], music and sound [7].

Nowadays, however, information security has improved considerably with the other mentioned methods. The steganography method, in addition to application in hidden exchange of information, is also used in such other fields as copyright, preventing e-document forging, etc.

Considering the wide use of the mobile phone and exchange of a large number of SMS messages on the mobile phone and, on the other hand, the possibility of sending B&W pictures in this service, an appropriate option for establishing hidden

1-4244-0340-5/06/$20.00 ©2006 IEEE

communications would be steganography in SMS messages [8]. In this paper I introduced a new feature to my proposed method. In this proposed method, after extracting hidden data, the received image is immediately filtered. This removes hidden data in the image.

In this paper, first related works on steganography in B&W pictures are examined. Then, in section 3, the used algorithm is described. In section 4, the advantages and disadvantages of the proposed method are studied. In section 5, the results are described and, finally, in section 6, the final conclusion is provided.

II. RELATED WORKS

Most steganography work so far carried out on pictures has been on color or grayscale pictures and little work has been done on B&W pictures, because B&W pictures are sensitive to changes and, for example, change in one pixel of the picture in a white area would be quite visible while, in color pictures, if the color of a pixel is changed slightly, this would not be tangible. In this section, we study work carried out on steganography of B&W pictures.

A. Using Dithered Images

In this method, data are saved in dithered images. In old newspapers, the dithered method in the form of B&W dots were used for printing color or grayscale pictures and the pictures looked grayscale from a distance. The problem with this method is that it cannot be used for normal two-color pictures and, on the other hand, a small number of data can be saved in the picture [9].

B. Method to Displace Words and Lines

In this method, by displacing the text or changing the distance between words, data are hidden in the printed picture of a text. The problem with this method is that it can only be used for pictures of text and cannot be used for regular pictures [10].

C. Changing two bits in each block

In this method, the input picture is divided into m×n blocks. Then each block is changed by apply XOR with a key on that block, so that the block is encoded. Considering the weight matrix, at most 2 bits of each block are changed. In this method, if the block dimensions are m×n, each block can hide $\log_2(mn+1)$ bits of data. The main advantage of this method is the high stegano capacity of this method. However, its major drawback is the tangible changes in the output picture [11, 12, 13].

D. Changing one bit in each block

In this method, the B&W pictures are first divided into m×n blocks and then, in each block, at most one bit of information is hidden. For each block, the possibility of saving is calculated and, if the possibility exceeds a certain limit, the middle point in that block is changed according to the data in question. The major advantage of this method is the intangible changes in the resulting pictures. The drawback of this method is the low steganography capacity of the pictures. The more the edges of the picture, the higher the steganography capacity will be [14, 15].

III. PROPOSED ALGORITHM

This is a summary of the algorithm used for steganography in the pictures of SMS messages in mobile phones: After converting the picture into the B&W color and a suitable format for the mobile phone, the picture is divided into 3×3 blocks. Information is encoded by the password. The possibility of steganography in each block of the picture is considered. If the result is positive, one bit of information is hidden in the picture by maximally changing one block cell. What follows is an elaboration of this algorithm.

First the received picture is converted to B&W. As the size of the SMS picture message must be 72×28 pixels, a 72×28-pixel conversion of the picture is created. The saving format of the SMS picture is OTA. The structure of this format is as follows [2].

The header of this format containing 4 fixed bytes is as follows:

Byte 1) 0000 0000 (→ 0)
Byte 2) 0100 1000 (→ 72)
Byte 3) 0001 1100 (→ 28)
Byte 4) 0000 0001 (→ 1)

As you can see in the above header, the second and third bytes indicate the height and width of the picture.

The structure of the body of the picture contains the pixels in 0 and 1. The amount of each pixel is saved in one bit. In each bit, 0 indicates the black and 1 the white color. Thus, every 8 pixels are saved in one byte. The order of saving of the pixels is from the left to the right and from the top to the bottom of the picture. Considering the size of the picture, the entire size of an SMS picture message is 256 bytes (Fig. 1).

Image Size: ((72×28 bit) ÷ 8) byte + 4 byte = 256 byte

Fig. 1. Size of an SMS picture message

Now, one should have B&W picture steganography. The main idea in B&W picture steganography is changing pixels of the image that are less noticeable because, in color and grayscale pictures, information can be hidden by making a slight change in the color, which does not apply to B&W pictures. For example, a black point put in an area of the picture that is fully white will be noticeable. As a result, the first action to be done is to identify areas of the picture that would not be noticeable by anyone in case of hiding information and changing pixels. In my algorithm, first the picture is divided into 3×3 blocks, and then the percentage of proportion of each block is calculated for steganography in it which is called flip-ability. To calculate the flip-ability, a table containing all the possible models is prepared for B&W coloring of a 3×3 block and the flip-ability of each of the modes is calculated for steganography. Now, by searching the table and finding the corresponding mode of the selected block, the flip-ability of the block is determined for steganography.

The possible modes for B&W coloring of a 3×3 block is $2^9 = 512$ modes. However, it is not necessary to calculate the flip-ability of all the modes. Simply by calculating a limited number of modes, one can find the flip-ability of all the modes because one can find the coloring modes of a 3×3 block by such conversions as rotating the picture, mirroring the picture or complementing the picture. Figure 2 shows the flip-ability value for a number of different coloring modes of a 3×3 block. In this figure a larger value indicates that the change of center pixel is less noticeable hence the change is more likely to be made for hiding information. The remaining modes, as already mentioned, are calculated according to this figure and by making the conversions. This lookup table has been developed by improving and correcting the table proposed by reference [15].

After calculating the flip-ability of each block, if the value exceeds a certain limit and the block can undergo steganography, one bit of information is hidden in the block.

For steganography of one bit of information in a block, first the white cells in the block are calculated. For steganography of one bit with value of 1, the number of white cells must be an even number. Therefore, if the number of white cells of the block is an odd number, by reversing the middle cell of the block, the number of white cells in the block will be an even number and, therefore, bit 1 will be hidden in this block of the picture (Fig. 3).

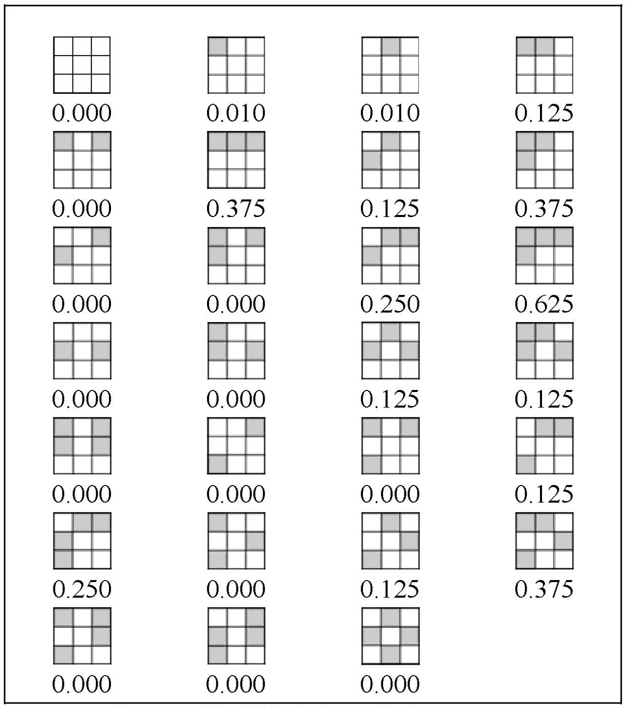


Fig. 2. My flip-ability lookup table for 3×3 patterns.

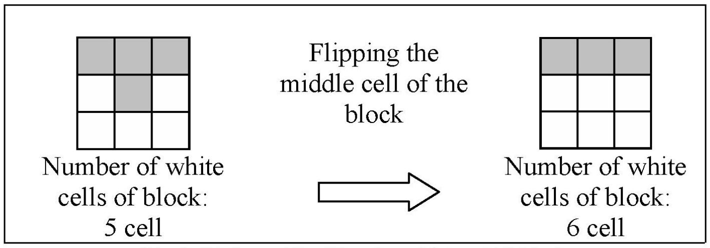

Flipping the middle cell of the block
Number of white cells of block: 5 cell
Number of white cells of block: 6 cell

Fig. 3. Hiding a bit with value of 1 in a 3×3 block

To hide one bit with a 0 value, the number of white cells in the block must be an odd number. Therefore, if the number of white cells in the block is an even number, by flipping the middle cell of the block, the number of white cells changed into an odd number and, thus, bit 0 will be hidden in this block of the picture.

As it is not possible to carry out steganography definitely in all the blocks, the maximum size of data that can undergo steganography in an SMS picture is 27 bytes (Fig. 4).

$$(72\times28 \text{ bit}) \div 9 = 216 \text{ bit} \qquad 216 \div 8 = 27 \text{ byte}$$

Fig. 4. Maximum capacity of an SMS picture for hiding data

Indeed, before steganography, information is encoded by a password received from the user and then it is hidden in the picture.

During extraction of information from the picture, first the SMS picture is divided into 3×3 blocks. Then the flip-ability of each block is calculated with the method described in the steganography section. If the block can undergo steganography, one bit of information from that block is extracted. To do so, if the number of white cells in the block is even, the value of the hidden bit in the block is 1. If the number of white cells in the block is odd, the hidden bit in the block is 0. After full extraction of the entire hidden bits in the picture, information is decoded with a password received from the user.

The main idea of my project is to stealth the hidden information. To do this, the decoder program, after extracting hidden information from the SMS picture, removes the information from the picture and saves the picture without any data on the recipient's mobile phone. Morphological methods are used for removing hidden data from the picture. The method used in this project is smoothing the borders of the picture [16].

The size of the hidden information is hidden at the beginning of the picture in one byte so that a proper quantity of the information can be extracted from the picture.

IV. Advantages And Disadvantages

A. Advantages

1. Little processing and a small memory are needed for this method of steganography. Therefore, there was no need to a computer and the entire process of steganography as well as extraction of information from

the picture can entirely carried out on a mobile phone.

2. Stealth-Text is a new SMS function recently provided in Britain and welcomed by the public [17]. In this method, the SMS message is automatically destroyed 40 seconds after being viewed by the recipient. However, this requires subscription of both the sender and the recipient to this system and the recipient of the message must have access to WAP (Wireless Application Protocol) functions. However, in our proposed method, there is no need to either the sender's or the recipient's subscription to a special service or having access to WAP. On the other hand, our method only destroys hidden data of the picture but the picture itself is maintained. Therefore, it is less likely to be noticed by others.
3. This method is compatible with many types of mobile phones.
4. Steganography methods are usually carried out on color or grayscale pictures and little work has been done on steganography in two-color pictures. Therefore, using the existing two-color pictures in SMS messages for steganography is less noticeable.
5. In the proposed method before steganography in the picture, information is encoded by a password. Therefore, if the person manages to extract information from the picture, he will not be able to decode it without having the password.
6. Each day millions of SMS messages are exchanged throughout the world. Therefore, steganography in SMS pictures has attracted less attention and it is hardly likely to identify pictures containing hidden information.
7. Costs of SMS message esp. compared to services such as the WAP is very low. Therefore, benefiting from this method for establishing hidden communications is very cost-effective.

B. Disadvantages

1. As it was described in the suggested algorithm section, maximum SMS message capacity for hiding information in an image is 27 bytes, and because of the blocks of the image that cannot undergo steganography, the capacity is usually less than 27 bytes. As a result, information that can undergo steganography in SMS messages is very little and is appropriate mostly for steganography of short letters in the picture.
2. Two-color pictures are much more sensitive than color and grayscale pictures. Therefore, steganography in these pictures is more tangible.
3. Since two-color pictures only contain pixels with two black and white values, they have a low degree of resistance and, in case of creation of noise, additional information may enter the picture and it is quite likely that false information would be extracted from the picture.
4. The size of SMS picture message is 72×28 pixels. There are few pictures with this size, esp. black and white pictures. Therefore, there are few options for selecting the pictures intended for steganography.

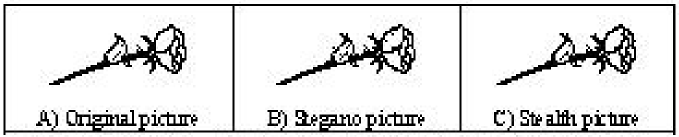
V. Experimental Result

This project uses the described algorithm to hide messages and phrases in SMS picture messages. Therefore, several messages and several pictures were selected. Then, the steganography program was run on a Nokia 6680 mobile phone. The program was in the J2ME (Java 2 Micro Edition) language, which is a kind of Java language for small machines such as pocket PC, mobile phones, etc.

The steganography program first receives the picture, the message and the password from the user. Then the picture is converted to a B&W image suitable for the mobile phone. If the image is larger than OTA valid resolution, the image is reduced to 72×28 pixel resolutions. Then the message is coded by using the password, and coded message is hidden in the picture. Finally the resulting picture is sent to the recipient as an SMS picture message.

On the receiver side, first the hidden information is extracted from the received SMS picture message, then the information is decoded by the entered password and finally by smoothing the image, the hidden information is destroyed (stealth information). Now the resulting image is saved on the mobile phone (Fig. 5) and the extracted message is shown to the user.

By comparing the hidden information and the extracted information, it was seen that both messages were the same and the program worked properly.



A) Original picture

B) Stegano picture

C) Stealth picture

Fig. 5. Hiding "Iran" message in an SMS picture message

VI. Conclusion

This paper presented a new method for Stealth Steganography in SMS on mobile phones. The SMS messages, in addition to creating a communication between two mobile phones, can establish a communication between a mobile phone and other computer networks. Therefore, by creating intelligent programs, dynamic SMS pictures containing hidden information appropriate for the recipient can be sent.

As mentioned under Section IV.B.3, these pictures has little resistance and stability. However, they can be further stabilized by methods such as multiple saving of a bit in several blocks of the image or changing two colors of each block for marking this method more powerful.

ACKNOWLEDGMENT

I would like to express my appreciation here for the valuable advices of Mr. Navid Hamed Azimi, my programming teacher at Sharif University of Technology, in carrying out this project.

REFERENCES

[1] GSM 03.40 v7.4.0, Digital cellular telecommunications system (Phase 2+), Technical realization of the Short Message Service (SMS), ETSI 2000, http://www.etsi.org

[2] Nokia, "Sending Content over SMS to Nokia Phones", Version 1.0, Forum Nokia, May 2001, http://www.forum.nokia.com

[3] R. Chandramouli, and N. Memon, "Analysis of LSB based image steganography techniques," Proc. of the International Conference on Image Processing, vol. 3, 7-10 Oct. 2001, pp. 1019-1022.

[4] M. Shirali Shahreza, "An Improved Method for Steganography on Mobile Phone," WSEAS Transactions on Systems, vol. 4, no. 7, July 2005, pp. 955-957.

[5] G. Doërr, and J.L. Dugelay, "A Guide Tour of Video Watermarking, In Signal Processing: Image Communication," vol. 18, no 4, 2003, pp. 263-282.

[6] N. F. Maxemchuk, and S. Low, "Marking Text Documents," Proceedings of the IEEE International Conference on Image Processing, Santa Barbara, CA, USA, Oct. 26-29, 1997, pp. 13-16.

[7] K. Gopalan, "Audio steganography using bit modification," Proc. of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03), vol. 2, 6-10 April, pp. 421-424, 2003.

[8] M. Shirali-Shahreza, "Steganography in SMS," Proc. of the 11th International CSI Computer Conference (CSICC'2006), School of Computer Science, IPM, Tehran, Iran, 24-26 Jan. 2006, pp.905-910 , (in Persian).

[9] K. Tanaka, Y. Nakamura, K. Matsui, "Embedding secret information into a dithered multi-level image", IEEE Military Communications Conference, 1990, pp. 212-220.

[10] S. H. Low, N. F. Maxemchuk, J. T. Brassil, L. O'Gorman, "Document marking and identification using both line and word shifting," Proc. of the 14th Annual Joint Conference of the IEEE Computer and Communications Societies, vol.2, 1995, pp. 853–860.

[11] Y. C. Tseng, Y. Y. Chen, and H. K. Pan, "A Secure Data Hiding Scheme for Binary Images," IEEE Trans. on Communications, Vol. 50, No. 8, Aug. 2002, pp. 1227-31.

[12] Y. Y. Chen, H. K. Pan, and Y. C. Tseng, "A Secure Data Hiding Scheme for Two-Color Images," IEEE Symposium on Computers and Communications, 2000, pp. 750-755.

[13] Y. C. Tseng and H. K. Pan, "Secure and Invisible Data Hiding in 2-Color Images," IEEE INFOCOM, 2001, pp. 887-896.

[14] M. Wu, E. Tang, and B. Liu, "Data hiding in digital binary image," in IEEE Int. Conf. Multimedia & Expo, New York, 2000.

[15] M. Wu and B. Liu, "Data Hiding in Binary Image for Authentication and Annotation," IEEE Trans. on Multimedia, vol. 6, no. 4, August 2004, pp.528-538.

[16] R. Haralick and L. Shapiro, Computer and Robot Vision, Vol. I, Addison-Wesley, 1992.

[17] StealthText, http://www.stealthtext.net, Accessed on 21 Jan. 2006.