International Journal of Advanced Computer and Mathematical Sciences
ISSN 2230-9624. Vol 3, Issue 4, 2012, pp 441-445
http://bipublication.com

A SURVEY PAPER ON SMS BASED STEGANOGRAPHY

Chandrakant Badgaiyan[1], Ashish Kumar Dewangan [2], Bhupesh Kumar Pandey [3]

[1]M.Te.ch Scholar in Communication Engineering, C.S.I.T. Durg, C.S.V.T.U
[2,3] Assistant Professor, C.S.I.T. Durg (C.G.), India
*Corresponding author: Email: chandrakant.elex@gmail.com, Mob: +91-9926656599

ABSTRACT:

After the advancement in mobile phone industry now mobile phones are available with huge variety of sensors, utility software, entertainment application and services like video conferencing and video call. Mobile phones has become ubiquitous and a general purpose device. SMS is one of the mostly used services in mobile phones throughout the world. Using this service, individuals can write and send to each other short messages and also binary pictures. On the one hand, information security is a critical issue in this digitalized world. For establishing hidden communications, a variety methods have been proposed for covert communications, among which steganography is a relatively new concept. As in mobile phones one can send text messages and binary picture messages both. In this paper, a survey work of all type of Steganographic techniques performed through mobile phone's SMS services esp. text steganography and image steganography and its future scope will be discussed. Most of these techniques are implemented on J2ME (Java 2 Micro Edition) platform.

Keywords: SMS (Short Message Service), IMEI (International Mobile Equipment Identity), J2ME (Java 2 Micro Edition), MMS (Multiple Part Message Service), PDAs (Personal Digital Assistant)

[I] INTRODUCTION

After the appearance of mobile phone in 1985, it has become a very important accessory in a way that one out of six men uses a mobile phone and many families have more than one mobile. Initially mobile phones were merely a device for talk with each other but due to its availability everywhere and every time, mobile phones' features have increased and the mobile phone manufacturers have added extra features to their mobile phones.

Because of the development in mobile phone field especially after the appearance of smart phone, the manufacturers of software using the new capabilities of mobile phones enjoyed a lucrative market. These software are written by languages which are specialized according to the specifications and limitations of the mobile phones. Some of the most famous mobile phone programming languages are C++ and J2ME (Java 2 Micro Edition), which is a special version of Java language for small devices such as mobile phones and PDAs (Personal Digital Assistant).

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. These pictures are named SMS picture message. The picture messages, however, are two-color and have a low quality [2].

The SMS has such advantages as low costs, offline SMS sending, exchanging SMS simultaneously with establishing telephone contacts, etc.

Steganography is a method of covert exchange of data, highlighted in recent years, chiefly aimed to hide data within a cover media so that other individuals fail to realize their existence [3]. The word steganography is a Greek word that means "hidden writing". While implementing this method, the main purpose is to hide data in a cover media so that other persons will not notice that such data is there. This is a major distinction of this method with the other methods of hidden exchange of data because, for example, in the method of cryptography, individuals see the encoded data and notice that such data exists but they cannot comprehend it. However, in steganography, individuals will not notice at all that data exists in the sources [4]. Most steganography jobs have been performed on images, video clips, text, music and sound [5]. It has also been implemented on such varying systems as computers and mobile phones [6]. Nowadays, however, information security has improved considerably with the other mentioned methods. The steganography method, in addition to application in cover exchange of information, is also used in other fields such as copyright protection, preventing e-document forging, etc [7].

[II] LITURATURE SURVEY

2.1. Methodology

In this paper, a detailed analysis of SMS based Steganographic methods and their advantages will be discussed. A SMS can be in text format or it can be a binary images. Hence SMS based steganography techniques are basically example of text steganography and image steganography. Because SMS services are available on mobile phone, this type of steganography provides user mobility, all time connectivity for real time transfer of secret data and it does not grab any attention as it is new in field of all type of steganography. One more thing which is quite prominent about any mobile based steganography technique is as mobile has limited processing power and run time memory any bulky algorithm will not work on this or it will take more time to recover secret data and embed secret data.

Following approach is used in almost all type of Steganographic technique using SMS on mobile phones and application development platform used is J2ME (Java Micro Edition).

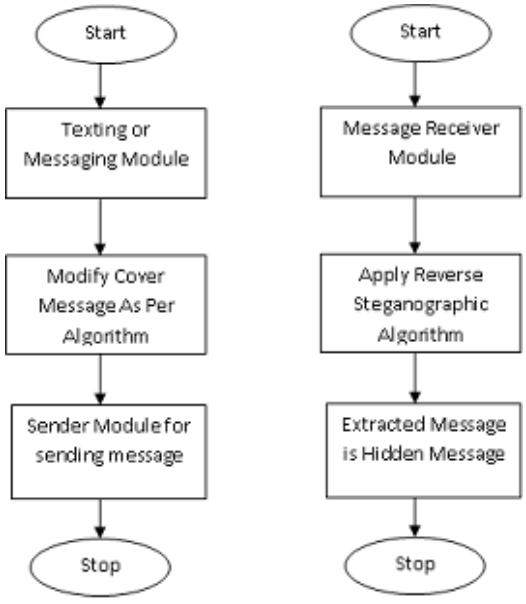

Fig: 1. Sender Side Approach Receiver Side Approach

2.2. Literature Survey

When SMS is used for sending text messages it utilizes the various algorithm of text steganography. Text steganography is most difficult type of steganography because there is no redundant information in text file as compared to the image and audio files [16]. We can send binary images through SMS and use this image as cover data for hiding secret data using image steganography algorithm [11]. This method has advantage of hiding text data into SMS which is a new concept in steganography but has disadvantage of limited size of embedded data. One of application of this method is in text steganography using SMS where message is typed using abbreviation text steganography with the use of the invented language SMS-Texting [12].

Further an enhanced method for SMS steganography using SMS-texting language, by removing the static nature of word-abbreviation list and introducing computationally light weighted XOR encryption. The dynamic arrangement of 'word-abbreviation list', if used alone, provides moderate level of security and makes it difficult for an adversary to instantly extract zeros' or ones' out of the SMS-text by knowing only the algorithm [15].

SMS based steganography technique using binary images can be used to send important information like Mobile software Activation key code to the user directly and software extracting the activation code from the picture and compare it with code which is generated natively [13]. This method has advantage of extra security while transferring activation code using SMS to the respected user as code is hidden inside the SMS image.

One more interesting way to send secret data using SMS was discovered in form of Sudoku game [14]. In this method, a Sudoku puzzle is send to the user then user solve this puzzle. After solving the puzzle, the numbers of specified row or column of the puzzle are computed. These numbers are given to decoder software and the decoder software will extract and display the coded data (maximum 18 bits) in accordance with order of numbers 1 through 9 and during a process conversely to coding stage. And a two-digit number is considered as a key. The first number of the key displays row and the second number indicate a column of the puzzle in which the data has been hidden. Of course one of these two digits must be 0. Number 0 indicates the fact that no data has been hidden in that row or column. For example number 50 means that the data is hidden in the 5th row or number 07 indicates the fact that the data has been hidden in the 7th column.

Finally SMS base steganography is also used in improving mobile banking security for transfer of important information [17]. In this method, instead of direct sending of the information, it is hidden in a picture by the password and is put on a site. Then the address of the picture is sent to the user. After receiving the address of the picture through SMS, the user downloads the picture by a special program. After entering the password, the user can witness the information extracted from the picture if the password is entered correctly.

[III] RESULTS

3.1. Advantage

Some advantages of SMS based Steganographic methods are as follow:

1. The cover media is in forms of SMS either text or binary image is very cost effective service hence wide range of people can use it.
2. Since SMS is available on mobile phone which provides the facility of mobility to application. Hence these Steganographic techniques can be used anywhere and anytime.
3. Each day millions of SMS messages are exchanged throughout the world. Therefore, it is hardly likely to identify SMS containing hidden information.
4. These methods can also be used on other devices such as PDAs and Pocket PCs.

5. The mobile phone is a public facility and most individuals have mobile phones. On the other hand, the SMS is a popular service. Therefore, SMS based steganography method covers many users.

6. Because of not using sophisticated technologies, this method can be implemented on simple mobile phones as well and there is no need to use advanced mobile phones and costly PC.

7. It does not require much processing and can be run on small devices and machines with limited resources.

8. All mobile phones, even black and white models and old-fashioned ones are capable to send and receive SMS so this method covers a lot of users.

3.2. Limitations

1. As all these techniques are implemented on mobile phones, it has a limited processing power.
2. SMS services can carry a limited amount of data only in a single time hence cover file size is limited in all SMS based Steganography.
3. In case of SMS texting method, as number of words increases, the time required to search and replace also increases.
4. SMS services can carry only binary images, no color images are allowed in case of SMS hence algorithm used to embed secret data can be recovered with brute force easily.

[IV] DISCUSSION

From the result section of paper the pros and cons of the SMS based Steganography technique clear. As SMS services are available using mobile phones which main characteristic is mobility and connectivity hence this technique can be used at anywhere. Since this field of Steganography is newer as compared to all other method of Steganography, it catches very low attention.

[V] CONCLUSION

This paper presented a detailed survey work of comparatively new Steganographic method in SMS on mobile phones and its various applications in critical data communication like mobile software activation key transfer and for sending user name and password in banking. The SMS can be used as text messages or for sending binary images and creating a communication between two mobile phones.

As mentioned under Section 3.1 and 3.2, these methods consume limited processing and memory which suits mobile phones. But because of small size cover data and low manipulation of cover data, secret data can be comparatively easily recovered. However, number of SMS sent in a day is so huge and common that it is difficult to keep a check. Using some other technique complexity of recovering data can be increased further.

ACKNOWLEDGEMENT

I would like to express my sincere thanks here for the valuable advices of Mr. Ashish Kumar Dewangan and Mr. Mangal Singh, my project guide and my project Coordinator respectively at C.S.I.T. Durg, in carrying out this survey work and for their kind support.

REFERENCES

[1] European Telecommunications Standards Institute (ETSI), *GSM 03.40 v7.4.0*, Digital cellular telecommunications system (Phase 2+), Technical realization of the SMS ETSI, 2000, http://www.etsi.org.

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

[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE*, Vol. 87, Issue 7, July 1999, pp. 1062-1078.

[4] J.C. Judge, "Steganography: Past, Present, Future," *SANS white paper*, 30 November, 2001, http://www.sans.org/rr/papers/index.php?id=552.

[5] N.J. Hopper, *Toward a theory of Steganography*, Ph.D. Dissertation, School of Computer Science Carnegie Mellon University, Pittsburgh, PA, USA, July 2004.

[6] M. Shirali-Shahreza, "An Improved Method for Steganography on Mobile Phone," *WSEAS Transactions on Systems*, Vol. 4, Issue 7, July 2005, pp. 955-957.

[7] F. Hartung and B. Girod, "Copyright Protection in Video Delivery Networks by Watermarking of Pre-Compressed Video," *Proceedings of Multimedia Applications, Services and Techniques - ECMAST '97', Springer Lecture Notes in Computer Science*, Vol. 1242, Milan, Italy, May 1997, pp. 423-436.

[8] M. Hassan Shirali-Shahreza, Mohammad Shirali-Shahreza," Sending Mobile Software Activation Code by SMS Using Steganography", Intelligent Information Hiding and Multimedia Signal Processing, 2007, IIHMSP 2007, Third International Conference on 2007, pp. 554-557

[9] Abbas Cheddad , Joan Condell, Kevin Curran, Paul Mc Kevitt ," Digital image steganography: Survey and analysis of current methods " 2010, Elsevier, Signal Processing , pp. 727-752

[10] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly1, Swarnendu Mukherjee1 and Poulami Das," A Tutorial Review on Steganography",2008, JIIT

[11] Mohammad Shirali Shahreza," Stealth Steganography in SMS", IEEE Wireless and Optical Communications Networks, 2006 IFIP International Conference

[12] Mohammad Shirali-Shahreza, M. Hassan Shirali-Shahreza, "Text Steganography in SMS", 2007 International Conference on Convergence Information Technology

[13] M. Hassan Shirali-Shahreza, Mohammad Shirali-Shahreza, "Sending Mobile Software Activation Code by SMS Using Steganography", Intelligent Information Hiding and Multimedia Signal Processing, 2007. IIHMSP 2007. Third International Conference on 2007, pp. 554-557

[14] M. Hassan Shirali-Shahreza, Mohammad Shirali-Shahreza, "Steganography in SMS by Sudoku Puzzle", Computer Systems and Applications, 2008. AICCSA 2008. IEEE/ACS International Conference , pp. 844-847

[15] Khan Farhan Rafat, "Enhanced Text Steganography in SMS", Computer, Control and Communication, 2009, IC4 2009, 2nd International Conference, pp. 1-6

[16] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding", IBM Systems Journal, vol. 35, Issue 3&4, 1996, pp. 313-336

[17] Mohammad Shirali Shahreza,"Improving Mobile Banking Security Using Steganography", ITNG '07, Fourth International Conference on 2-4 April 2007