Journal of Computer Science 7 (11): 1626-1628, 2011
ISSN 1549-3636

Text Hiding in Mobile Phone Simple Message Service Using Fonts

Wesam S. Bhaya
Department of Information Network, College of Computer Technology,
University of Babylon, Iraq

Abstract: Problem statement: Hiding secret information in an ordinary mobile phone Simple Message Service (SMS). **Approach:** In mobile phones, there are two default types of fonts, System and Proportional fonts, which have similar figures to human vision and cannot recognized by human eye. The suggested method hides the information (0,1) in cover SMS message by changing the fonts of each character by one of those two fonts (0 represented by System font and 1 represented by Proportional fonts). After embedding secret information in cover message, the Stego message will look like an ordinary message but each character draw in one of these similarity fonts. Finally, at extract site, it must analyze each character font to retrieve secret information. This study has been implemented by J2ME (Java 2 Micro Edition) programming language to works in mobile (cellular) phones. **Results:** By using two similarity fonts, we can hide one bit in one character of mobile phone message. **Conclusion:** Good steganography depends on the human behavior and way of thinking. The most successful hiding method is the uncommon one. Although the proposed method is simple but it is unthinkable one and needs knowledge and experience to be discovered.

Key words: Steganography hides, text hiding, mobile phone, message service, proposed method, text steganography, proportional fonts, secret message

INTRODUCTION

Steganography is a Greek word which means "covered writing" and can trace its origins as far back as 440 B.C. (Petitcolas *et al*., 1999). Steganography, in today's electronic era, is the ability of hiding information in redundant bits of any unremarkable cover media, so nobody notice the existence of the secret information. Its objective is to keep the secret message undetectable without destroying the cover media. Steganography replaces unneeded bits in image, sound and text files with secret data. Instead of protecting data the way encryption does, steganography hides the existence of the data (Provos and Honeyman, 2003). Most of the steganography study has been carried out on pictures (Chandramouli and Memon, 2001; Shirali, 2005) video clips (Doërr and Dugelay, 2003; Doërr and Dugelay, 2004), music and sounds (Gopalan, 2003). Text steganography is the most difficult kind of steganography (Brassil *et al*., 1995) this is due largely to the relative lack of redundant information in a text file as compared with a picture or a sound file (Bender *et al*., 1996).

The information-hiding process in a steganography system begins by identifying a cove r medium.

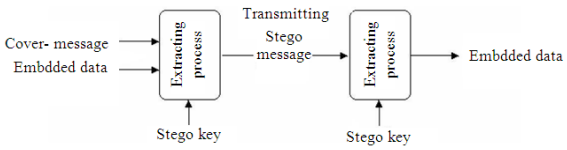

Fig.1: Steps of steganography

The embedding process creates a stego medium by hiding secret data in cover medium (for example, replacing the redundant bits) (Provos and Honeyman, 2003). Figure 1 shows the main steps of steganography.

The present study offers a new method for hiding information in text of SMS. We uses two default similar types of fonts FACE_SYSTEM and FACE_PROPORTIONAl which J2ME supplies in canvas class for implementing the hidden purpose in mobile phones.

The related studies in hiding text are line shifting (Low *et al*., 1995), Word Shifting (Kim *et al*., 2003), semantic methods feature coding (Rabah, 2004), Abbreviation (Bender *et al*., 1996), Open Spaces (Huang and Yan, 2000), Persian/Arabic Text steganography (Shirali-Shahreza and Shirali-Shahreza, 2006) and hiding dynamic and static text within a cover-text (Riad *et al*., 2009). The methods which study on hiding data in SMS are Stealth Steganography in

SMS, which steganography in the pictures of SMS messages (Shirali-Shahreza, 2006) and Text Steganography in SMS which use and develop abbreviation text steganography with the use of the invented language of SMS-Texting (Shirali-Shahreza and Shirali-Shahreza, 2007).

MATERIALS AND METHODS

Hiding (Embedding) Side: In order to hide text, there are many algorithms interest in texture inclusion. Hiding the information inside text is different from one human language to another, for example, the inclusion in Arabic language not necessary to be applicable on English sentence and the reverse is true. The example below simplifies one that used. Remember, the proposed method uses two types of fonts that the J2ME supplies it in "canvas class":

Example: Let the secret message is: run Which will represented as: 10001 10100 01101, this according to the position order of the character in alphabet (i.e., a = 0, b = 1, c = 2,….. z = 25).

Let the cover text is: this is my program notices that the cover text must consist of at least 15 letters; this depends on the number of bits that represent the secret message (run) (each secret letter represented by five bits). Figure 2 shows the result of proposed system when it implemented.

Fig. 2: Proposed hiding system

Fig. 3: Hide and retrieve the secret message

RESULTS AND DISCUSSION

The result is as the original text but the letter (T) painted in Proportional font type because it hides the bit (1) and other painted in System font type that hide the bit (0) and so on for the rest letters. Now the SMS of the sender is ready to be sent. When the legal receiver gets the SMS message, it must analyze the letters and extract the bits and collect them to retrieve the secret message, as follows:

Extract (retrieval) side: For the purpose of retrieving the secret message, we will use J2ME's function called get face () to analyze the font. The method of extract will be as follow:

Test each character of received text and return its font face using get face () function. If the font face for this character is System, this means that the bit of the hidden secret message character is (0). If the font face is Proportional this means that the another secret bit is (1) and so on for five characters to retrieve one hide character, since we are hides every character of the secret message in five characters of the cover message. After continue on the rest of the characters, we will get back the secret message. Figure 3 shows the result of implementation.

As a result the cover text will be shown like the original one for the viewers but each character will be drawn in a particular font in a way that don't arouse suspicion.

CONCLUSION

The proposed system can be defined as a secret key steganography system. There is a secret key between the sender and the receiver. The stego key represented by using two types of fonts in J2ME, for example "System and Proportional". Without knowledge of the stego key, the receiver cannot extract the original message.

The similarity between the cover text and stego text can be considered very well because using two suitable types of fonts.

As a future work, the suggested method can be apply in computer text, which have many similar fonts in its figure and can hide more bits in cover message by using three or more fonts for characters.

REFERENCES

Bender, W., D. Gruhl, N. Morimoto and Lu, A., 1996. Techniques for data hiding. IBM Syst. J., 35: 313-336. DOI: 10.1147/sj.353.0313

Brassil, J.T., S. Low, N.F. Maxemchuk and L. O'Gorman, 1995. Electronic marking and identification techniques to discourage document copying. J. Select. Areas Commun., 13: 1495-1504. DOI: 10.1109/49.464718

Chandramouli, R. and N. Memon, 2001. Analysis of LSB based image steganography techniques. Proceeding of the International Conference on Image Processing, Oct. 7-10, IEEE Xplore Press, Thessaloniki, Greece, pp: 1019-1022. DOI: 10.1109/ICIP.2001.958299

Doerr, G. and J.L. Dugelay, 2004. Security pitfalls of frameby-frame approaches to video watermarking. Trans. Signal Proc., 52: 2955-2964. DOI: 10.1109/TSP.2004.833867

Doerr, G. and J.L. Dugelay, 2003. A guide tour of video watermarking. Signal Proc. Image Commun., 18: 263-282. DOI: 10.1016/S0923-5965(02)00144-3

Gopalan, K., 2003. Audio Steganography using bit modification. Proceeding of the IEEE International Conference on Acoustics, Speech and Signal Processing, April 6-10, IEEE Xplore Press, USA, pp: 421-424. DOI: 10.1109/ICASSP.2003.1202390

Huang, D. and H. Yan, 2000. Inter word distance changes represented by sine waves for watermarking text images. IEEE Trans. Circ. Syst. Video. Technol., 11: 1237-1245. DOI: 10.1109/76.974678

Kim, Y., K. Moon and I. Oh, 2003. A text watermarking algorithm based on word classification and inter-word space statistics. Proceeding of the 7th International Conference on Document Analysis and Recognition, Aug. 3-6, IEEE Xplore Press, USA, pp: 775-779. DOI: 10.1109/ICDAR.2003.1227767

Low, S.H., N.F. Maxemchuk, J.T. Brassil and L. O'Gorman, 1995. Document marking and identification using both line and word shifting. Proceedings of the 14th Annual Joint Conference of the IEEE Computer and Communications Societies, Apr. 2-6, IEEE Xplore Press, Boston, MA, USA, pp: 853-860. DOI: 10.1109/INFCOM.1995.515956

Petitcolas, F.A., P. Anderson, R.M.G. Kuhn, 1999. Information hiding-a survey. Proc. IEEE, 87: 1062-1078. DOI: 10.1109/5.771065

Provos, N. and P. Honeyman, 2003. Hide and Seek: An Introduction to Steganography. Securi. Priva., 1: 32-44. DOI: 10.1109/MSECP.2003.1203220

Rabah, K., 2004. steganography-the art of hiding data. Informa. Technol. J., 3: 245-269.

Riad, J., B. Ibrahim and H. Zoubiv, 2009. Information hiding: A generic approach. J. Comput. Sci., 5: 930-936. DOI**:** 10.3844/jcssp.2009.930.936

Shirali, S.M., 2005. An improved method for steganography on mobile phone. Allameh Helli Pre-University.

Shirali-Shahreza, M. and M.H. Shirali-Shahreza, 2007. Text steganography in SMS. Proceeding of the IEEE International Conference on Convergence Information Technology, Nov. 21-23, IEEE Xplore Press, Gyeongju, pp: 2260-2265. DOI: 10.1109/ICCIT.2007.100

Shirali-Shahreza, M., 2006. Stealth steganography in SMS. Proceeding of the 3rd IEEE and IFIP International Conference on Wireless and Optical Communications Networks, (WOCN 2006), IEEE Xplore Press, Bangalore, 5-5. DOI: 10.1109/WOCN.2006.1666572

Shirali-Shahreza, M.H. and M. hirali-Shahreza, 2006. A new approach to persian/Arabic text steganography. Proceeding of the 5th IEEE/ACIS International Conference on Computer and Information Science, July 10-12, IEEE Xplore Press, Honolulu, HI, pp: 310-315. DOI: 10.1109/ICIS-COMSAR.2006.10