Secure Transmission Of Sensitive Data Using System Fonts Technique

R.Bhuvaneshwari[1],P.Archana[2], S.Mahalakshmi[2].

**[1,2&3]Department of Information Technology,
Sivakasi,Tamilnadu, India**

Abstract

SMS is one of the mostly used services in mobile phones throughout the world. Using this service, individuals can write and send short messages to each other. Information security is a critical issue in this digitalized world. Stegnography is a new concept for transformation of secure data. In mobile phones, two default types of fonts are used. They are System and Proportional fonts, which have related figures to human visualization and cannot recognized by human eye. The proposed method hides the secret data(0,1) in cover SMS message by changing the fonts of each character by one of those two fonts (1 represented by Proportional fonts and 0 represented by System fonts). After embedding secret information in cover message, the Stego message will look like an common message but each character draw in one of these fonts. In extraction side, it must analyze each character font to retrieve secret information.Most of these techniques are executed on J2ME (Java2 Micro Edition) platform.

***Keywords**:Stegnography,SMS(Short Message Service), J2ME (Java 2MicroEdition), Proportional fonts, System fonts, information security.*

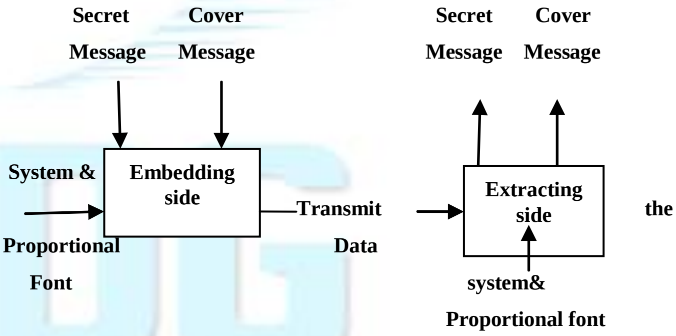
1.Introduction

After the presence of mobile phone in 1985, it has become a very important accessory in a way six men uses a mobile phone. Initially mobile phones were only 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 companies have added additional features to their mobile phones.

The SMS (Short Message Service) is used for transfer and exchange of short text messages between more than one mobile phone.The length of the transfered message is 160 characters at most, which are saved in 140 bytes dependent on how information is saved according to the standards[2]. The SMS has such advantages as low costs, offline SMS sending, exchanging SMS instantaneously with establishing telephone contacts, etc..

Steganography is a word which means "covered writing"[3].Steganography is the ability of hiding information in redundant bits of any unremarkable cover media, so that other persons will not notice the existence of the secret information., for example, in the method of cryptography, folks see the encoded data and notice that such data exists but they cannot comprehend it[1].However, in steganography, individuals will not notice at all that data exists in the sources [4]. Some Steganographic model with high security features has been presented in [13], [14], [15] and [16].

The application of steganography is, copyright protection, preventing e-document forging etc[6].The present study offers a new method for hiding information in text of SMS. We uses two default types of fonts FACE_SYSTEM and FACE_PROPORTIONAL which J2ME supplies in canvas class for implementing the hidden dedication in mobile phones[5].



The embedding process creates a stego medium by hiding secret data in cover medium[8]. SMS based steganography is used in improving mobile banking security for transfer of important information [11].

Existing System

2.1 Cryptography

Crptography is the secure communication in the presence of third parties(called adversaries)[12]. It achieve the confidentiality, Integrity, Availability, Authenticity, Non-reputation. The art of protecting information by transforming it (encrypting it) into cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text.

Cipher text is encrypted text,it is in unreadable form.Plain text is decrpted text, it is orginal message. Plain text is the most portable format because it is supported by nearly every application on every machine. It is also called clear text.

2.2 Image Steganography

As stated earlier, images are the most popular cover objects used for steganography[10]. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image.It is the ability of hiding secret information in any cover media, so that nobody notice the existence of the secret information. Transmit binary/color images and use this image as cover data for hiding secret data using image steganography algorithm.

The Drawbacks of Existing Systems are,

1. In cryptography, third parties can understand about the transmission of secret message by viewing ciphertext.
2. In Image steganography is the Complex processing.
3. In Image steganography,limited size of data can be embedded.

Proposed System

In this paper, a detailed study of SMS based Steganographic methods and their advantages will be discussed. A SMS can be in text format or in a binary images. Hence SMS based steganography techniques are basically example of texts and image steganography. Because SMS services are accessible on mobile phone, this type of steganography provides user mobility, all time connectivity for real time transfer of secret data and it does not take any attention as it is new in field of all type of steganography[7].

One more thing which is quite projecting 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 method is used in almost all type of Steganographic technique using SMS on mobile phones and application development platform used is J2ME (Java Micro Edition).

When SMS is used for sending text messages it uses the various algorithm of text steganography. Text steganography is most challenging type of steganography because there is no redundant information in text file as compared to the image and audio files [9].

The proposed system can be demarcated as a secret key steganography system.In this method, there is a secret key between the sender and the receiver. The stego key denoted by using two types of fonts in J2ME, for example "Proportional and System". Without knowledge of the stego key, the receiver cannot excerpt the original message. The connection between the cover text and stego text can be considered very well because using two appropriate types of fonts.

As SMS services are available using mobile Phones which main attribute is mobility and connectivity hence this technique can be used at anywhere. Since this field of Steganography is newer as compared to all other technique of Steganography, it catches very low attention[5].The suggested method can be apply in compute r 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.

Modules Specification

1. Stego medium creation
2. Embedding secret data
3. Transmit cover message to receiver
4. Extraction of cover message a.Stego Medium Creation

Assign five bit binary pattern for each alphabet ie. a – 00001, b - 00010…. .z -11011. Get the secret (stego) message from the user and convert stego message into five bit binary pattern. Find the length of the binary stream.Then read\create cover message of length equal to binary stream.

b. Embedding secret data

Embed stego message and cover message using System and proportional fonts.In binry stream 0 represent the System font and one 1 represent the proportional font.

c.Transmit cover message to receiver

In this module send SMS of embedded cover message to the corresponding receiver mobile.

d.Extraction of cover message

In receiver side receive the embed cover message.Convert each letter in cover message to binary form based on fonts.Divide the binary stream into group of five bits. Convert five bits pattern to alphabets using corresponding converstion.Then recover stego message.

IMPLEMENTATION METHODOLOGY

In order to hide text, there are several algorithms interest in texture inclusion. Hiding the secret information in side text is different from one human language to another language, for example, the inclusion in Arabic language not required to be applicable on English s entence and the reverse is true. The following Example simplifies one that used. Remember, the proposed method uses two types of fonts that the J2ME offers it in “canvas class”.

Example: Let the secret message is: word Which will be denoted as: 10001 10100 01101, this according to the position order of the character in alphabet like 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 20 letters; this depends on the number of bits that denote the secret message (word) (each secret letter signified by five bits).

a.Embedding Side:

Get the secret data from the user input and it is in the form of alphabet .And the alphabet converted into 0’s and 1’s. Each secret letter represented by five bits.To get the cover message from the user input and the cove r message is equal to the length of the converted message.Using the fonts like SYSTEM and PROPORTIONAL embed the secret and cover message.

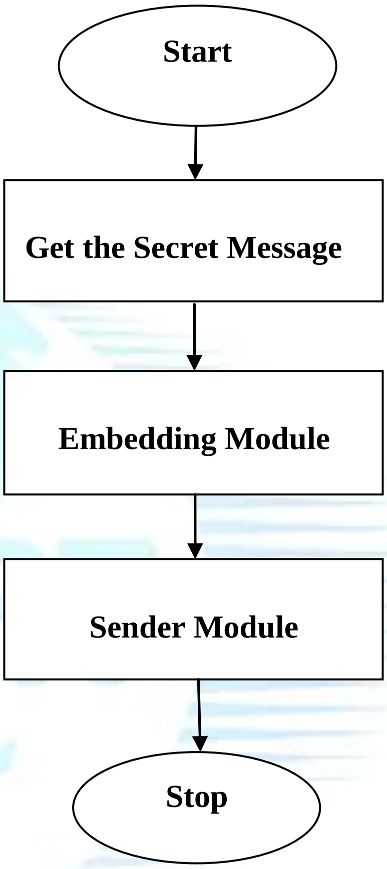


Fig.2:Sender Side Approach

b.Extract (retrieval) side:

For the purpose of extract the secret message, will use J2ME's function called get face () to analyze the font and extract secret data as follow:

Receive the message and test the each character of received message and return its font face using get face() function. If the font face for character is Proportional , this means that the bit of the hidden secret message character is (1). If the font face is System this means that the another secret bit is (0) and so on for five characters to retrieve one hidden 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 each character, we will get back the secret message.

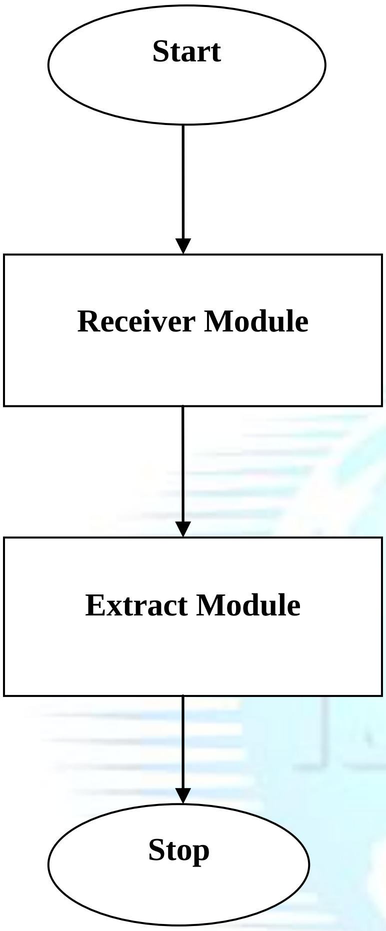


Fig.3: Receiver Side Approach

Advantage

Steganographic methods have some advantages. They are,
1. Steganography is very cost effective service Hence wide range of people also use it because the cover media is in forms of SMS either text or binary image.
2.Steganographic techniques can be used anywhere and anytime since SMS is available on mobile phone which provides the facility of mobility to application.
3. Each day millions of SMS messages are Interchanged throughout the world. Therefore, it is hardly likely to find SMS containing hidden information.
4. This method also be used on other devices such as PDAs and Pocket PCs.
5. SMS based steganography method covers many Users because most individuals have mobile phones and also SMS is a popular service.
6. Not using sophisticated method, this method can be executed on simple mobile phones as well and there is no need to use advanced mobile phones and costly PC.
7.It can be run on small devices and machines with Limited resources.
8. All mobile phones, even old models are also capable to send and receive SMS so this method covers a lot of users.

Limitations

1. It has a limited processing Power, so these techniques are executed on mobile phones.
2. SMS services can carry a limited amount of Data only in a single time the covered file size Is limited in all SMS based Steganography.
3. In SMS texting method, as number of words increases, at the same time required to search and Replace also increases.

I. RESULT AND DISCUSSION

From the result section of paper the process of the SMS based Steganography technique is clear. As SMS services are available using mobile Phones.The main characteristic of mobile phone is mobility and connectivity hence this technique can be used at anywhere. Steganography is newer as compared to all other methods and also, it catches very low attention.

The letter can be painted in Proportional font type, it hides the bit (1) and other painted in System font type that hides the bit (0) and so on for the rest letters. Now the SMS of the sender is ready to be sent. When the receiver gets the SMS message, it must analyze the letters and retrieve the orginal message.

CONCLUSION

This paper presented a Steganographic method in SMS on mobile phones and it's 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.

REFERENCES

[1] 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.

[2] Brassil, J.T., S. Low, N.F. Maxemchuk and

L.O'Gorman, 1995. Electronic marking and Identificatio techniques to discourage document Copying. J. Select. Areas Commun. 13: 1495-1504. DOI: 10.1109/49.464718.

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

[6] 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.

[7] 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

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

[9] 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.

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

[11] K. Moon Y. Kim and I. Oh. A text watermarking algorithm based on word classification and inter-word space statistics. In Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR'03), pages 775–779, 2003.

[12] Rivest, Ronald L. (1990). "Cryptology". In J. Van Leeuwen. Handbook of Theoretical Computer Science. **1**. Elsevier

[13] Souvik Bhattacharyya. And Gautam Sanyal. Study of secure steganography model. In Proceedings of International Conference on AdvancedComputing And Communication Technologies *(ICACCT-2008)*, Panipath, India, 2008.

[14] Souvik Bhattacharyya. and Gautam Sanyal. An image based steganography model for promoting global cyber security. In Proceedings of International Conference on Systemics, Cybernetics and Informatics, Hyderabad, India, 2009.

[15] Souvik Bhattacharyya. And Gautam Sanyal. Implementation and design of an image based steganographic model. In Proceedings of IEEE international Advance Computing Conference, Patiala, India, 2009.

[16] Geert Uytterhoeven Dirk Roose Adhemar Bultheel. Integer wavelet transforms using the lifting scheme. In CSCC Proceedings, 1999.