ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

# Text Stenography Using Computer Fonts

Nirmatha T.M[a], and Amaresan.S[b]
[a]Research Scholar, Department of Computer Science, PRIST University, Thanjavur.
[b]Research Supervisor, Department of Computer Science, PRIST University, Thanjavur.

**Abstract**: Steganography along with cryptography is used and offers suitable amount of privacy and security over the communication channel. This proposed method describes a detailed study of SMS based Steganography. 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. Stenography is a new concept for transformation of secure data. The proposed method hides the secret data into ASCII 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 computer text fonts). After embedding secret information in cover message, the Stego message will look like a common message but each character draw in one of these fonts. In extraction side, it must analyze each character font to retrieve secret information.

**Keywords**: SMS, Secure data, Stegomessage, ASCII, cryptography

## I. INTRODUCTION

Steganography is derived from a finding by Johannes Trithemus (1462-1516) entitled ―Steganography and comes from the Greek words meaning ― covered writing. Steganography is the art and science of hiding a message inside another message without drawing any suspicion to others so that the message can only be detected by its intended recipient. Cryptography and Steganography are ways of secure data transfer over the Internet.

Cryptography scrambles a message to conceal its contents; steganography conceals the existence of a message. It is not enough to simply encipher the traffic, as criminals detect, and react to, the presence of encrypted communications. But when information hiding is used, even if an eavesdropper snoops the transmitted object, he cannot surmise the communication since it is carried out in a concealed way.

Limitation of cryptography is that the third party is always aware of the communication because of the unintelligible nature of the text. Steganography overcomes this limitation by hiding message in an innocent looking object called cover. Steganography gained importance because the US and the British government, after the advent of 9/11, banned the use of cryptography and publishing sector wanted to hide copyright marks.

Modern steganography is generally understood to deal with electronic media rather than physical objects and texts. In steganography, the text to be concealed is called embedded data. An innocuous medium, such as text, image, audio, or video file; which is used to hide embedded data is called cover. The key (optional) used in embedding process is called stego-key.

A stego-key is used to control the hiding process so as to restrict detection and/or recovery of embedded data to the parties who know it. The stego object is an object we get after hiding the embedded data in a cover medium.

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 transferred message is 160 characters at most, which are saved in 140 bytes dependent on how information is saved according to the standards. The SMS has such advantages as low costs, offline SMS sending, exchanging SMS instantaneously with establishing telephone contacts, etc.

## II. RELATED WORKS

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

or protected", and graphei meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographic, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible between the visible lines of a private letter. Seemingly harmless messages, Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen. An encoded message just screams you're using encryption, which may attract unwanted attention to your activities even if snoopers cannot read the text of your messages.

Steganographic invented the word steganography and the word is derived from two Greek words steganos, meaning ―covered‖, and graphein, meaning ―to write‖. The first written evidence about steganography being used to send messages is the Herodotus story about slaves and their shaved heads. The modern representation of steganography can be given in terms of the prisoner„s problem. In the general model for steganography, illustrated in Fig., let a sender wishing to send a secret message S to an intended receiver. To do so, the sender embeds S into a cover media C to obtain the stego-object ´C. This stego-object„s carrying the secret message is then sent through the network. In a pure steganography framework, the technique for hiding the message is unknown to the warden and shared as a secret between sender and receiver. In compared to other steganography such as on images video files, audio files, etc., due to the lack of large-scale redundancy of information in a text file, text steganography seems to be the most difficult kind of steganography. To overcome the difficulties, like attacking, with the existing linguistic approaches, without replacing the original.

## III. Existing Approaches in Text Steganography

A few works have been done on hiding information in texts. Following is the list of different methods of the works carried out and reported so far.

In general, the Text Steganography methods can be categorized into two groups:

- Changing the text format
- Changing the meaning of the text

The methods which are based on the changing the meaning of the text are limited. Some examples of these methods are as follows:

### 3.1 Syntactic method

By placing some punctuation marks such as full stop (.) and comma (,) in proper places, one can hide information in a text file. This method requires identifying proper places for putting punctuation marks. The amount of information to hide in this method is trivial.

### 3.2 Semantic method

In this method, synonym words substitution for hiding secret message bits on the analogy form. This method uses the synonym of certain words thereby hiding information in the text. The synonym substitution may represent a single or multiple bit combination for the secret information. A major advantage of this method is the protection of information in case of retyping or using OCR programs.

### 3.3 Text abbreviation or acronym

Another method for hiding information is the use of abbreviations or acronym. In this method, the use of substitution of words with their respective abbreviations or vice versa is used to hide bits of secret message.

### 3.4 Change of spelling

In this method, a method to exploit same words which are spelled differently in British and American English for hiding secret message bits. The concealment methodology elaborated below, where the words spelled in British and American English is arranged in separate columns; is identical to that explained in preceding sub-para.

### 3.5 Line shifting method

In this method, the lines of the text are vertically shifted to some degree (for example, each line is shifted 1/300 inch up or down) and information are hidden by creating a unique shape of the text. This method is suitable for printed texts.

### 3.6 Word shifting method

In this method, by shifting words horizontally and by changing distance between words, information is hidden in the text. This method is acceptable for texts where the distance between words is varying. This method can be identified less, because change of distance between words to fill a line is quite common.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

## IV. System Analysis

Hiding secret information in ordinary mobile phone Simple Message Service (SMS). 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 can be implemented using J2ME (Java 2 Micro Edition) programming language to works in mobile (cellular) phones.

The previous study offers a new method for hiding information in text of SMS. We use 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.

A. *Proposed System*

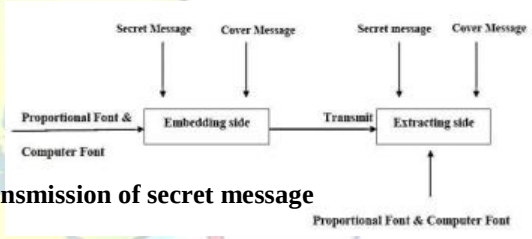
The proposed method describes a detailed study of SMS based Steganographic methods and their advantages will be discussed. A SMS can be in text format. Hence SMS based steganography techniques are basically example of texts. Because SMS services are accessible on mobile phone, this type of steganography 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.

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.

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.

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, 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. The suggested method can be applied 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.




**Transmission of secret message**

## V. Conclusion And Future Work

Thus the application for performing the steganography that is data hiding through the text in files is successfully completed. The input text is given and under various scenarios the effectiveness of the system is tested. The various further enhancements for reducing the small image distortions are need to make in the future. Further toughness for retrieving the images should be also done by means of any secret key lock in this system.

In future we can make this more effective by adding some extra feature. In future we will use indexing feature for storing the same letters used in secret message for reducing the low storing capacity of words and reducing the size of the cover message by the limited use of the null spaces in cover message and the scope of the project can be extended by turning the software into a web application and it can be extended by adding an e-mailing feature to the software where the encoded stream can be mailed to the receiver to get it decoded. This feature can make the software really efficient.

## References

[1]. Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay and Tai- hoon Kim, "Text Steganography: A Novel Approach",

International Journal of Advanced Science and Technology Vol. 3, pp. 79-86, February, 2009.

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

[3]. M. Hassan Shirali-Shahreza, Mohammad Shirali-Shahreza, ―Sending Mobile Software Activation Code by SMS Using Steganography‖, Intelligent Information

[4]. Hiding and Multimedia Signal Processing, 2007. IIHMSP 2007. Third International Conference on 2007, pp. 554-557

[5]. S.Changder, D. Ghosh and N. C. Debnath, "Linguistic Approach for Text Steganography through Indian Text", 20IO 2nd International Conference on Computer Technology and Development (ICCTD 2010), pp.318-322, 2010.

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

[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]. Mohammad Shirali Shahreza, ‖Improving Mobile Banking Security Using Steganography‖, ITNG _07, Fourth International Conference on 2-4 April 2007.

[9]. S. Changder, N.C. Debnath and D. Ghosh, "A New Approach to Hindi Text Steganography by Shifting Matra", 2009 International Conference on Advances in Recent Technologies in Communication and Computing, pp.199-202, 2009.

[10]. S. Changder, N. C. Debnath and D. Ghosh, "A Statistical Attack on a Kind of Word-Shift Text-Steganography", 2011 Eighth International Conference on Information Technology: New Generations, pp.30-35, 2011.

[11]. Mohammad Shirali-Shahreza, *Text Steganography by Changing Words Spelling*, ISBN 978-89-5519-136-3, Feb. 17- 20, 2008 ICACT 2008.

[12]. Mercan Topkara, Umut Topkara, Mikhail J. Atallah, *Information Hiding Through Errors: A Confusing Approach*, Purdue University.

[13]. Tsung-Yuan Liu, Wen-Hsiang Tsai,and Senior Member, *A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change Tracking Technique*, 1556-6013.

[14]. NeoByte Solutions, "*Invisible Secrets4*",http://www.invisiblesecrets.com/index.html

[15]. Mohammad Shirali Shahreza, *A New Method for Steganography in HTML Files*, Computer, Information, and Systems Sciences, and Engineering, Proceedings of IETA 2005, TeNe 2005, EIAE 2005, 247-251, Springer.

[16]. D. Parnas, ―On the Criteria to Be Used in Decomposing Systems Into Modules‖, *Communication of the ACM*, vol. 15, no. 12, December 1972, pp. 1053-1058.