International Journal of Advanced Computer and Mathematical Sciences
ISSN 2230-9624. Vol 3, Issue 4, 2012, pp556-562
http://bipublication.com

A NEW STEGANOGRAPHIC TECHNIQUE: IMAGE HIDING IN MOBILE APPLICATION

Chandrakant Badgaiyan [1], Ashish Kumar Dewangan [2], Bhupesh Kumar Pandey [3], Keerti Yeulkar [4] and Kaushal Kumar Sinha [5]

[1]Communication Engineering, C.S.I.T. Durg, C.S.V.T.U Bhilai (C.G.), India,
[2]C.S.I.T. Durg,C.S.V.T.U. Bhilai, (C.G.), India,
[3,4]C.S.I.T. Durg (C.G.), India, [5]B.I.T. Durg (C.G.), India
[*]Corresponding author: Email: chandrakant.elex@gmail.com,

[Received-18/10/2012, Accepted-30/11/2012]

ABSTRACT:

Today's world has become fully digitalized. All data are available and stored in digital format. Critical data like E-Commerce or M-Commerce related data, user name, password of any personal account, medicine formula, product design prototype, defense and spying operation data is very sensitive from the point of view of data security. Keeping data in encrypted format always grab focus which may cause a brute force to decrypt it. Hence it is very important to hide data in such a way that it will not grab any attention of hackers. On the other hand, mobile device has become most used device and it is remain connected with network everywhere. Now Mobile devices are available with various features, sensors and a huge variety of application. Mobile application market has been so popular that in a single day millions of new application gets downloaded and installed by mobile users. In this paper we propose new technique to hide secret images of all formats into a mobile application which gives steganography field a new dimension for development and successfully overcome some challenges of old Steganographic techniques like limited payload capacity etc. A detailed discussion on proposed technique's comparison with previously available technique and about its advantage will be discussed. This project is implemented on J2ME (Java 2 Micro Edition) platform and target device for testing is Nokia C5 mobile phone and few other devices.

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 communication 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 mobile softwares 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).

On the other hand Steganography is a method of covert exchange of data, highlighted in recent years, chiefly aimed to hide data within a cover media such 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, in this 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].

There are five types of steganography technique exist like Text, Image, Audio, Video and Protocol [1]. The most important requirement is that a Steganographic algorithm has to be imperceptible. Any Steganographic technique is judged on basis of following criteria [1]:

1. Invisibility – Strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised [18].
2. Payload capacity – Information, Steganography requires sufficient embedding capacity [19].
3. Robustness against statistical attacks – Many Steganographic algorithms leaves a "signature" when embedding information that can be easily detected through statistical analysis. A Steganographic algorithm must not leave such a mark in the cover data as be statistically significant.
4. Robustness against cover data manipulation –The cover data may undergo changes by an active warden in an attempt to remove hidden information. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. It is preferable for Steganographic algorithms to be robust against either malicious or unintentional changes to the image.
5. Independent of file format –The most powerful Steganographic algorithms thus posses the ability to embed information in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.
6. Unsuspicious files – This requirement includes all characteristics of a Steganographic algorithm that may result in images that are not used normally and may cause suspicion.

Unfortunately hardly any algorithms fulfill these requirements. Thus a trade off will exist in most cases, depending on which requirements are more important for the specific application [2].

After literature survey of Steganography following problems are identified:

1. There no standard way to embed all type of data i.e. text, image, audio and video, in a single cover data [1].

2. Same algorithm cannot be used for all formats of data like for image PNG, BITMAP, JPEG [1].
3. Amount of data being embedded is limited because of cover size dependency.
4. Huge Processing power and time is required for existing algorithms.
5. Dependency of PC or laptops is there, for reproduction of secret data which is not available in all places.

[II] LITURATURE SURVEY

In this section, we will discuss different Steganographic technique implemented on mobile phones. Various mode of steganography on mobile phones are SMS based and MMS based steganography which are basically based on text steganography and image steganography.

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] METHODOLOGY

In all Steganographic technique whether it is various types Text steganography, Image steganography, Audio steganography, Video steganography or Protocol based steganography Secret Data is hidden into some Cover Data based

on some algorithm. Since these methods change at least some properties of Cover Data to hide Secret Data based on particular Steganographic Algorithm.

In our proposed technique, we are going to hide image into a mobile application with its resources in such a way that it cannot be recovered from any other means except by using Mobile Application. The proposed technique is implemented using J2ME platform and. Run & Tested on device Nokia C5 phone.

For achieving this, following flow of control figure (1) is implemented in a Mobile Application which can be any utility like Paint Brush and entertainment application like any Mobile Game. If we create an application in such a way that the whole application can work separately without showing secret image hidden in its resource as graphic file. Then we can assign a Secret Key or password key to user, in order to see hidden image and stop the Application's Normal Mode. Same Secret key will be used to hide image again and to enable normal application running. For making the retrieval of Secret Image more complex use of password can be fixed at a specific event or arena in mobile application.

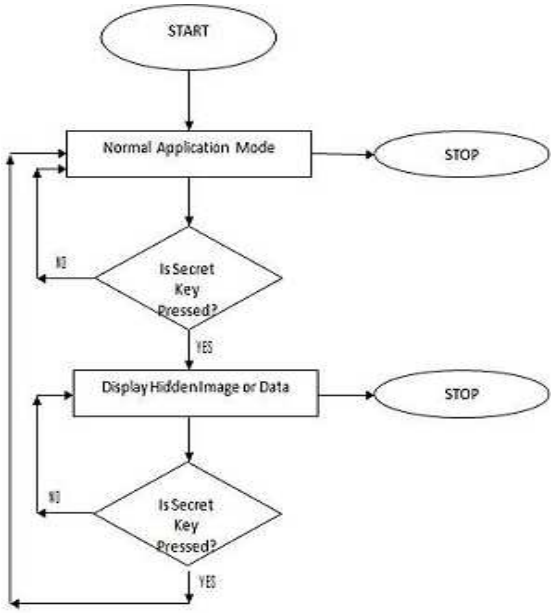

Figure1. Control flow diagram of technique

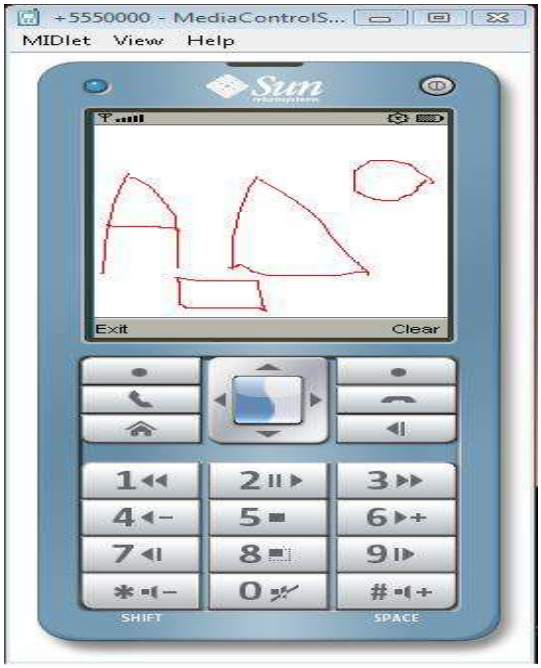

Figure2. Paint Brush App in Normal Mode

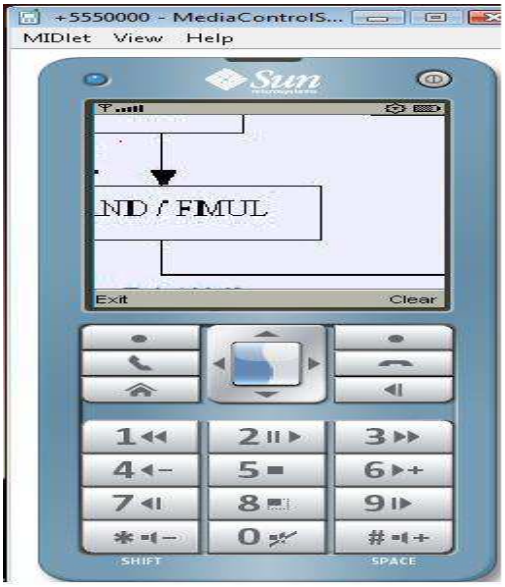

Figure3. After Applying Secret Key, Image Display Mode

[IV] RESULTS

	Image Format/ Mobile phones	PNG	BITMAP	JPEG
1	Nokia N97	YES	YES	YES
2	Nokia C5	YES	YES	YES
3	Nokia C6	YES	YES	YES
4	Samsung S5620	YES	YES	YES

Table 1.Testing various phones with different Image format

	Image Format/ Mobile phones	Bluetooth	Data Cable	OTA
1	Nokia N97	YES	YES	Not Performed
2	Nokia C5	YES	YES	Not Performed
3	Nokia C6	YES	YES	Not Performed
4	Samsung S5620	YES	YES	Not Performed

Table 2.Testing on various phones with different Modes

4.1 ADVANTAGES

1. This proposed method can carry huge amount of data. There is no dependency on cover file size.
2. A variety of data can be embedded into Jar file. Like text, image, audio files and video files.
3. This proposed method has no restriction of specific file format of data to be embedded. All file format supported by target device will be acceptable.
4. 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.
5. It does not require much processing and can be run on small devices and machines with limited resources.
6. Each day millions of J2ME applications are downloaded and installed throughout the world. Therefore, it is hardly likely to identify JAR containing hidden information.
7. Cost of Mobile phone as compared to PC is very low. Therefore, benefiting from this method for sending hidden images is very cost-effective.
8. This method can also be used on all J2ME supported devices in the world such as PDAs and Pocket PCs.
9. The mobile phone is a public facility and most individuals have mobile phones. On the other hand, mobile network has improved. Therefore, our proposed method covers many users.

4.2 LIMITATIONS

1. In our proposed technique data is hidden with Mobile Application resource data, though it does not catch any attention but it can be recovered by extraction of Mobile Application package file or executable file. This problem can be resolved by Binarization of secret data file.
2. As in our proposed technique, hidden image can be recovered by only means of Password and that Password is used in source code module of image recovering hence this password can be recovered by reverse engineering of source code file. Obfuscation of source code is one solution of this problem
3. Above both situation comes when user device goes in the hand of some hackers but this require not only large time and a communication media between user mobile and PC but also requires special type of software for analyzing.

4.3 APPLICATIONS

1. This Proposed Technique can be used by all spy agencies like RAW, CBI, FBI, CIA etc because this implemented on mobile phones.
2. This technique can be used for covert interactive communication like chatting and others services.

Since technique has no limitation related to file format, type of data and data size, this can be used with almost all type Steganographic application.

[V] PERFORMANCE EVALUATION

S.N.	Judgment Criteria	Performance Evaluation
1	Invisibility	Secret data is secured inside application with secret key and remain completely invisible till the application of key.
2	Payload Capacity	Payload capacity is flexible with respect of secret data. In this case 51 kb size image is hidden inside 6 kb of application size.
3	Robustness against Statistical attack	As secret data is hidden inside mobile application installation file, after installation hidden image cannot be accessed by user in any way except from our application that is too only with our secret key. Hence no risk of statistical attack.

4	Robustness against Secret Data manipulate-on	If mobile application file gets tempered by some hackers then too there are chances of recovering secret data.
5	Independent of file format	• Any file format supported by native mobile and J2ME API can be hidden by this technique. • All type of data like text, image, audio and video can be hidden. • For image PNG, JPEG and BITMAP format have been tested.
6	Unsuspicious file	Mobile applications are very common and downloaded using WAP or internet from Mobile Apps Store daily in huge numbers and there is no way to find out whether it is malware or not.

Table 3.Based on various judgment criteria of Steganography

[VI] CONCLUSION

In this paper, by embedding various formats of images as secret data into a mobile application, a new Steganographic method is proposed for hiding images into a completely new cover data i.e. a mobile application. The payload capacity in our proposed technique is not dependent on the size of Cover data. One additional advantage of the technique is that it works equally well for all type of image formats like PNG, Bitmap or JPEG.

As our technique is a real time application for mobile phones user can access and use this at anywhere on his mobile phone, mobility is one of the prominent feature with this technique which was not available in others techniques used for Steganography. Proposed techniques has limitation that secret image can be exposed to hacker when he has clue that mobile application has contain a embedded secret image into it. Recovering image file from any unfair means will require media connection of mobile phones to PC and specialized software. It has also threat from code reverse engineering. Both of these limitations can be overcome by using Obfuscation in coding and Binarization of resource data.

The proposed Steganographic technique has more advantages as compare to other existing techniques and the limitation of this can be overcome by adopting specialized solution mentioned above. Many mobile phones support Java platform, and approximately all mobile phones can download mobile application, so this method can be implemented on wide range of mobile phones. This method has real time applications for all spy agencies.

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 project work and for their kind support.

REFERENCES

[1] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee, Poulami Das," A Tutorial Review on Steganography", International conference 2008 at JIIT

[2] Ahsan, K. & Kundur, D., "Practical Data hiding in TCP/IP", Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002

[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

[18] Zenon Hrytskiv, Sviatoslav Voloshynovskiy, Yuriy Rytsav., "Cryptography and Steganography of Video information in modern communication", Electronics and Energetics, Vol 11, No. 1, 115-225

[19] Dean Lewandowski, Mike Palmisano., Steganography