INTERNATIONAL JOURNAL OF ADVANCED STUDIES
IN COMPUTER SCIENCE AND ENGINEERING
IJASCSE VOLUME 5 ISSUE 11, 2016

11/30/2016

Enhance Mobile Phones Privacy Based on Steganography

Mohammed Alaa Al-Hamami
MIS Dept., Applied Science University
Manamah, Bahrain
mohammad.alhamami@yahoo.com

Alaa. H. Al-Hamami and Salwa AlSharif
CS Dept., Amman Arab University,
Amman 11953, Jordan
alaa_hamami@yahoo.com

***Abstract*- In recent years, Internet and mobile are widely used for communication. Short Messaging Service (SMS) and Multimedia Messaging Service (MMS) are the popular services provided by the telecommunication companies. These services make the communication so fast and easy, the attention toward information security must be increased, and protection becomes a necessity because of the threats to the privacy and security.**

Steganography (Information Hiding) is used to hide the transferred secret information existence with other information. When data is hidden within text or image apparently may look the same for the naked eye of a person.

The Steganography software for mobile application is designed upon using the mobile phone messaging architecture system, and it will use Steganography to hide the secret messages into SMS and MMS covers. The LSB algorithm will be used to embed secret message into cover images, and it will generate Stego images for (MMS) and it will use the same menu for the messages of the mobile phone system. It is possible to extract directly the hidden secret message by the receiver. This software is implemented by using J2ME (Java 2 Micro Edition) programming language, and the dependence flexibility of the software load on all mobile types that have the property of the send messages.

Keywords- SMS; MMS; Steganography; Privacy; Secret Messages.

I. INTRODUCTION

The SMS method is connected to a number of characteristics that contributed to an increase in popularity. First, support the device to send and receive SMS messages in almost everywhere, ranging from low-end mobile phones to the Web interface phrases which are accessible via regular computers over the Internet. Furthermore, support plug and routing of SMS messages by most cellular networks throughout the world. Second, it follows the "push" model of operating and short messages are extradition to mobile devices in near real time, which makes SMS peer wireless Internet applications such as Instant Messaging like AIM, ICQ. Third, the consequence of the contact from store and forward like e-mail messages, which do not ignore the message if you cannot receive immediately by hand and alternatively are stored in the server interim and re-sent at a later date [1].

The MMS was evolved from the popularity of the SMS messaging system and uses the Wireless Application Protocol (WAP). WAP is a protocol that permits mobile devices to communicate with Internet servers via the mobile radio communications network. MMS Stenography is a combination of image and text Steganography. SMS Steganography is a combination of text and text Steganography.

While communication apps continue to be prime usage on smartphones among all the users, the types of communication apps adopted by each country differs from one another [2]. Although for the large number of communication apps, communicating in a secret way is still a big concern.

II. SMS and MMS

Mobile phones and wireless networks are being used widely now days, wireless networks are available in most public places, this encourage the unauthorized used for those networks and devices. WAP is the protocol that allows Internet access from wireless devices and as more subscriber's

demand WAP services, the need for wireless Internet security will continue to grow [3].

SMS is the abbreviation for Short Message Service and is the text communication service component of a phone or mobile communication system, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices. A standard SMS is usually 160 characters in length and can be sent from any regular mobile phone.

The MMS was evolved from the popularity of the SMS messaging system and uses the WAP. MMS is the abbreviation for Multimedia Messaging Service and is a standard way to send messages that include multimedia content to and from mobile phones. A standard MMS does not have a specific character limit. One can, however, send music, animation and other interactive media with a MMS from a specially designed cellular handset that is capable of receiving and sending multimedia messages [4].

III. Steganography Concept

Embedding information, which is to be hidden, into media requires two files. The first is the innocent-looking file that will hold the hidden information, called the cover media. The second file is the secret message that the information to be hidden as shown in Fig. 1.

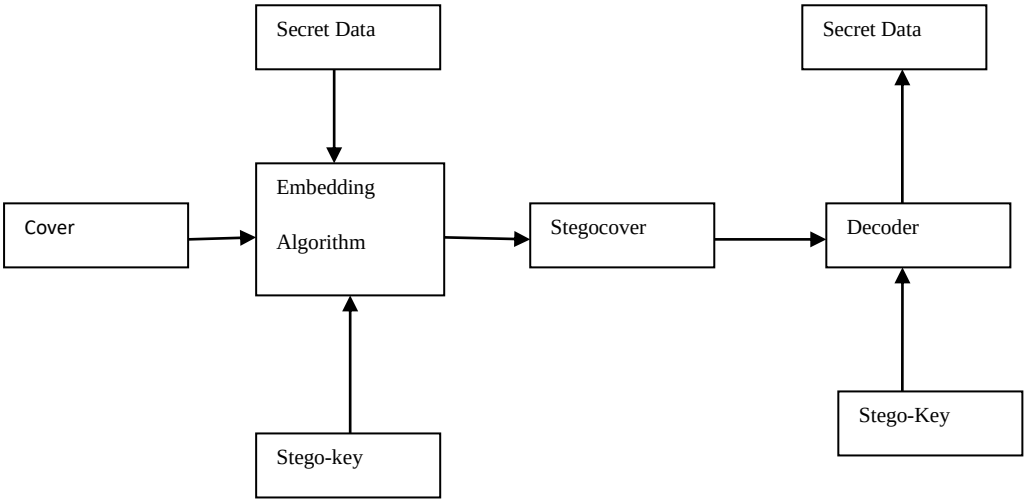

Fig. 1 The Main Steps of Data Hiding and Extracting.

The secret message may be plaintext, cipher text, images, or anything that can be embedded in various types of cover. If the data are embedded in a text file (cover text), the result is a stego-text (or stego text) object. Thus, it is possible to have cover image and stego image, cover audio and stego audio, cover video and stego video, etc. The most media use is an image for hiding information. When combined, the cover media and the embedded message this will form a stego-object product. A stego-key (a type of password) may also be used in hiding process and then later may be used to decode the message [3].

IV. The Proposed Hiding App

SMS and MMS are methods to send messages from one mobile to another. Steganography is securing SMS or MMS and it secures the exchange of information. Without having privacy of information there is no meaning of doing communication using extremely high end technologies like SMS or MMS. This can be achieved by using Steganography, which is the process of hiding secret information inside some carrier. SMS and MMS can be used as a carrier for hiding information in mobile devices. In this research we are trying to improve privacy and security to send subtle messages through the merge text in text or text in image, it is not a magnet for hackers to attack the message.

The following features are considered in this research.

- Embedding capacity: also known as payload which is the amount of data that can be hidden in a cover, compared to the size of the cover. This feature can be measured numerically in units of bit-per-bit (bpb).
- Invisibility: Any data hidden in a cover causes it to be modified. Invisibility (also termed perceptual transparency or algorithm quality) is a measure of the amount of distortion to the cover.
- Undetectability: An attacker may be able to detect the presence of hidden data in a given file by computing certain statistical properties of the file and computing them to what is expected in that type of file.
- Robustness: This is a measure of the ability of the algorithm to retain the data embedded in the cover even after the cover has been subjected to various changes as a result of lossy compression and decompression or of certain types of processing such as conversion to analog and back to digital.

The app is designed for mobile phones with J2ME language to hide text messages inside text and image. The result of the hiding process could be send by SMS or MMS.

The proposed app has the following specification:

• The hiding process doesn't require a secret key between the communication parties (sender and receiver).

• The process of sending the secret message is done by using the same way of sending SMS or MMS messages; this will allow the app user to send the secret message for one person or more by inserting a new contact, or select as many as desired from the stored contacts in the Mobile.

• The cover of the secret message can be chosen in two ways; either by selecting a cover stored in the mobile or by inserting a new cover to the mobile.

• The same algorithm is used in the hiding and in the extraction process.

V. Hiding using SMS Messages

The first and most obvious aim of information hiding is simply to hide private, sensitive data in a cover. The data is embedded either as plain, raw format or encrypted. Since the amount of data to be hidden may be large, it makes sense to compress it prior to its encryption and embedding. This enables several parties to exchange messages without communicating directly. The proposed method which is used in this research is very simple one and it depends on the spaces between the words in the text. If there are two spaces between the words followed by one space, it means a zero bit. If there is one space between the words followed by two spaces, it means a 1 bit. If there are two spaces followed by two spaces or one space followed by one space, it means there are no hidden bits.

To send a secret message by using SMS, we follow the following steps:

- Step 1: Select or insert a text to be used as a cover.
- Step 2: Write the secret message that will be hidden in the cover.
- Step 3: Use the proposed method: put two spaces for the Zero and one space for the One of the text message.
- Step 5: Hide the secret message in the text cover by using the proposed method.
- Step 6: Send the SMS to the destination.

To extract the hidden message, user must use the same sequence in reverse order.

IV. Hiding using MMS Messages

The app provides the ability to use a single or multi covers to hide the secret text message in MMS.

To send a secret message using a single cover by MMS, we need to use the following instructions:

- Step 1: select image that will be used as a cover.

- Step 2: Write the secret message that will be hidden in the cover.
- Step 3: Hide the secret message into cover image using Least Significant Bit method (LSB).
- Step 4: Send the MMS message, this message will include the stego-image (cover with the secret text message).

To send a secret message using multi-covers by MMS, we need to use the following instructions:

- Step 1: Select the first cover image.
- Step 2: To write the secret message that will be hidden in the cover.
- Step 3: To hide the secret message into cover1 using Least Significant Bit method (LSB).
- Step 4: To select the second cover image.
- Step 5: To hide the result of step 3 into cover 2 using Least Significant Bit method (LSB).
- Step 6: To send the MMS message, this message will include the stego-image (the result of the second hiding process).

V11. The Experimental works

The Steganography software for mobile application is designed identical to the mobile phone system; we use the same menu of the messages for the mobile phone (SMS, MMS) to send messages to one user or more. The developed Steganography software designed for mobile phones using J2ME language to hide information in covers (text, image).

Taking into account the developed Steganography software design to meet the following requirements:

- It doesn't need a secret key between the parties' connection (the sender and receiver) to send a secret message.
- The Process of sending secret messages is done by using the same facility of the mobile system, and this allows us to send a message for one person or more, insert a new contact, or select as many contacts as wanted from the stored contacts list in the Mobile.
- The covers for the two types (SMS, MMS) are either a stored cover in mobile, or they are being input using mobile camera.
- Extraction process is adversely embedding process, so it must contain the same algorithm in both of the sender and receiver mobile.
- The developed software storage does not need any modification in mobile architectural or in its software.

Fig. 2 shows the selection of the steganography type on Mobile device.

Fig. 2. Shows Steganography in mobile application software (SMS, MMS).

The cover form for MMS _single for the sender will be as the following:

- Image box “cover image”: this image use to select the cover image from existing folder.
- Text field called “secret text”: this textbox to write secret message and fill selected template.
- Embedding command: to embedding the text message into cover image 1 using LSB.
- Send button: to send result of embedding MMS.

The sender selects single cover, and after the sender is selected the cover message; thereafter be able to write the secret message. The selected image is done through a collection of images that stored in a mobile device. The selected image is not the only one which is stored, but the sender can select another image that stored in a mobile device.

Fig. 3 shows the option send to help the sender in sending the secret messages "result" to one receiver or several receivers at the same time.

Fig. 3 Show process sends to the result.

MMS _Double cover: MMS _double cover sender form will be as the following:

- Image box “cover image1”: this image use to select the cover image from existing folder.
- Select cover 1: to embedding the text message into cover image 1 using LSB.
- Text field called “secret text”: this textbox to write secret message and fill selected template.
- Image box “cover image2”: this image use to select the cover image from existing folder.
- Select cover 2: to embedding the result of process button1 into cover image2 “LSB”.
- Send button: to send result of embedding MMS.

Fig. 4 shows the screen display when the sender selected double cover "double images ". The first option is to select cover1, and the next step is the selection of cover2.

Fig. 4. shows mine screen MMS _double, and select cover1.

It is possible to store the final result in the mobile if the sender unwilling to send it to the other party.

VIII. CONCLUSIONS

The mobile is a personal device, and the hiding process stems from the natural human; therefore, we use Steganography in mobile. Given the importance of mobile in the daily life of users, and the importance of the messages and frequent used among users to its cheap price. For privacy, during the exchange of secret messages, it must not attract the attention of the intruders or their suspicion. Messages enable users to store sensitive information for a long time on the mobile and return them at any time possible. The developed software is to enhance security, increase privacy, and authorized access to sensitive information of the connected parties. This can be implemented through the use of steganography technology to hide sensitive information for mobile in the cover (SMS, MMS), reduce the detection and infiltration information to the intruders, and finally reduce all threats which threaten this information. The implemented system has been developed on Mobile with the attention to the following: **First**: No change for the SMS and MMS system to suit the developed system. **Second**: Use SMS and MMS system to send messages to take advantage of the characteristics of the service to be sent to several users. **Third**: To maintain the security or secret of the hidden messages and the lack of clarity to intruder during transmission. **Fourth:** Use SMS and MMS to send secret messages without any additions to the content or to the general form.

REFERENCES

[1] P. Zerfos, X. Meng, H. Starsky Y Wong, V. Sam anta and L.U. Songwu. A Study of the Short Message Service of a Nationwide Cellular Network., IMC'06, October 25–27, 2006, Rio de Janeiro, Brazil. Copyright 2006 ACM 1-59593-561-4/06/0010.

[2] M. S. Shahreza. An Improved Method for Steganography on Mobile Phone. Allameh Helli Pre-University, Ghafari Street, South Kargar Street, Tehran, Iran, http://mohammad.shirali.ir.

[3] T. Morkel, J. H. P, Eloff and M. S. Olivier. An Overview of Image Steganography. Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, 2002, Pretoria, South Africa.

[4] K. H. Zaidoon, A. A. Zaidan, B.B Zaidan & H. O. Alanazi. Overview: Main Fundamentals for Steganography. Journal of Computing, Vol. 2, No. 3, 2010, P. 40-43.

[5] Alaa. H. Al-Hamami and Mohammed. A. Alhammi. Information Hiding –Steganography and Watermark. Jordan, Dar Ithraa for Publishing and Distribution, 2008.

[6] E. A. Walia, P. Jainb and Navdeepc. An Analysis of LSB & DCT based Steganography. Global Journal of Computer Science and Technology, April 2010.

[7] W. S. Bhaya, Text Hiding in Mobile Phone Simple Message Service Using Fonts. Department of Information Network, College of Computer Technology (2011), University of Babylon, Iraq, Journal of Computer Science. Vol.7, No. 11, 2011, P. 1626-1628.

[8] B. Alrouh, A. Almohammad and G. Ghinea. Information Hiding in SOAP Messages: A Steganographic Method for Web Services. International Journal for Information Security Research (IJISR), Vol. 1, Issues 1/2, March/June 2011.

[9] S. Singh and G. Agarwal. Use of Image to Secure Text Message with the Help of LSB Replacement. International Journal of Applied Engineering Research, Dindigul Vol. 1, No1, 2010.

[10] P. Salhofer and F. H JOANNEUM. Mobile Application Programming Java Editions - IP-MAD. Mobile Application Programming. Java 2 Micro Edition, mad-ip.eu/files/J2ME.pdf.

[11] Shahreza M.H.S, and Shahreza M.S. "Text steganography in SMS", 2007 *Int*. Conf. on Convergence Information Technology, 2007, P. 2260-2263.

[12] A. H. Al-Hamami & S. H. Hashem. Escaping Information Using Unused Bits in the Internet Packets by secure sign., International Conference on Information and Communications Technology (ICICT2004) Cairo, Egypt, 2004, P. 167-180.

[13] A. H. Al-Hamami, Mohammed A. Alhamami and S. H. Hashem. A Strategy to Compromise Handwritten Documents processing and Retrieving using association Rules Mining. Ubiquitous Computing and Communication Journal, UbiCC Journal, Vol. 6, Issue 3, 2011, P. 901-906.