International Journal of Electronics Communication and Computer Engineering
Volume 7, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Employing The Use of Steganography for The Secured Transmission of Information In Mobile Devices

Bolude Oluwatosin Racheal, Dr.Olajide Olusegun Adeosun

***Abstract* – Individuals and corporate establishments alike are faced with threat from malicious attacks and infringement of their privacy over the internet or while using mobile devices. For this reason, there is a need for an enhanced means of information detection. Steganography is the practice of protecting files by hiding it within other files. This concept has been used by many businesses since its introduction. It has been applied in the field of communication most especially in the music industry. Information can be embedded in computer files like images, videos or audio. Hiding data in plain sight by encryption can draw unwanted attention to hidden messages thereby leading to high cases of attempts on decryption by unauthorized persons as such there is need to hide data in a form that will not be suspected by attackers. The aim of this research is to develop the possibility of using steganography mobile devices for the transmission of secured information. The system will be designed using UML (Unified Modeling Language) tools and android phone as the developing environment. The successful implementation of steganography can boost security for highly confidential files or messages that are meant to be kept in top secret forms in mobile devices.**

***Keywords* – Android, Encryption, Mobile devices Steganography, UML (Unified Modeling Language).**

I. INTRODUCTION

Growth in technology has resulted in wide spread use of different communication gadgets or mobile based devices for daily interactions and for conveyance of information personally between individuals or in an established corporate organization. With increased rate of data transmission comes the need for a secure system for transmission of confidential and proprietary information. Steganography is a technology that hides a message within an object, a text, or a picture. Steganography conceals not only the contents of the message but also the mere existence of a message (Alain, 2010). Steganography messages are often first encrypted by some traditional means, and then a cover text is modified in some way to contain the encrypted message, resulting in stegotext (Judge, 2001). Pure steganography uses no keyed system to embed cleartext or "null cipher" text into the cover data in order to hide the existence of a secret message. Pure steganography is the least secure method. It is only secure in two aspects which are, the fact only the sending and receiving parties know of the secret message's existence and which steganographic algorithm was used to hide the message. A stenographic messages contains three components; the secret message (hidden part) and the cover data (the container which bears the secret message) and the stego message (final product). Firstly, one must understand the components of a steganographic message. steganographic approaches convey the security level of protected information and include the use of pure steganography, public key steganography and private key steganography. The private key method uses a mutual key for encrypting then hiding the secret message within the cover data. As in traditional encryption the private key system is only as robust as the knowledge of the key. Since the private key system requires both parties to know the key, once it is compromised the entire stego message is non-secure. Public key encrypted steganography uses the key pair system to add a layer of robustness to the process. As in public key encryption, the public key of the recipient is used to encrypt the secret message and only that user's private key may decrypt it after extracting it from the cover data. This is the most secure type of steganography. This approach is recommended since it combines the benefits of hiding the existence of a secret message with the security of encryption (Alain, 2010). This paper proposes thedevelopment of the possibility of using steganography mobile devices for the transmission of secured information.

II. REVIEW OF RELATED WORK

Ashwini and Patil (2014) proposed the method of using SBR algorithm to hide the data into the JPEG Image. This paper presents a new Steganography technique in spatial domain for encoding extra information in an image by making small modifications to its pixels. The proposed method focuses on one particular popular technique. They used the Least Significant Bit (LSB) Embedding. Instead of using the LSB-1 of the cover for embedding the message, LSB-2 has been used to increase the robustness of system and protect the message against the external. They were able to hide a data up to 65536 bytes. The data was embedded in the LSB-2 of the cover to increase the robustness of the system and protect the message against the external influences such as noise, filter, compression…etc. The embedding process was very easy, which only replaces the permutated bits of the message by the LSB-2 set of the cover to obtain the new stego-image array. Using steganography (way of hiding data) and SBR algorithm, they were able to 100% detect the guilty agent in the leaks of a sports news from the BNN news channel which was the test area of study. The result shows that minimum distortions take place in data embedded image due to embedding small amount of data using proposed method. The results shows that the proposed method is much more secure than LSB. This method is essential for construction of accurate targeted and blind steganalysis methods for JPEG, BMP and PNG images.

Kamleshand Kiran (2005) proposed KVL Algorithm for image hiding in image using the LSB based algorithm.

In their research, least significant bit of cover image are used and secret image most significant bits of color components are hidden in them. 3 RGB Pixels were used to hide 8 bit information. This technique gives the image quality of high standards and with the necked eyes it is impossible to find the variations in the Stego image. The result comparisons also support the statement strongly. Experimental result shows the effectiveness of the proposed method. The results obtained also show significant improvement in PSNR with respect to image quality and computational efficiency.

The ease in use and abundant availability of steganography tools has law enforcement concerned in trafficking of illicit material via web page images, audio, and other files being transmitted through the Internet. Methods of message detection and understanding the thresholds of current technology are necessary to uncover such activities. Max (2004) discussed the method of embedding data in a JPEG Image. Because the JPEG file format is compact and does not significantly degrade the quality of an image it is in frequent use on the internet. The JPEG format uses a discrete cosine transform (DCT) to identify 64 DCT coefficients in successive 8x8 pixel blocks. Of these quantized coefficients, the least significant bits are used to embed data. Because modifications to these bits affect pixel frequency as opposed to spatial structure (as in GIF images where image structure information is present at every bit layer), no obvious distortion is present (Max, 2004). Ongoing work in the area of Internet steganography by Dunigan (2001) investigates embedding, recovering, and detecting information in TCP/IP packet headers and other network transmissions. Development in the area of covert communications and steganography will continue. Research in building more robust digital watermarks that can survive image manipulation and attacks continues to grow. The more information is placed in the public's reach on the Internet, the more owners of such information need to protect themselves from theft and false representation. Success in steganographic secrecy results from selecting the proper mechanisms. However, a stego-image which seems innocent enough may, upon further investigation, actually broadcast the existence of embedded information (Dunigan, 2001).

III. Real Work

The researcher's proposed mobile steganography tool will be used to enable the privacy and security of messages sent through the mobile communication network as they will be hidden in multimedia files.

The flowchart of the data hiding and data retrieval processes of the system are shown in Figure 1 below:

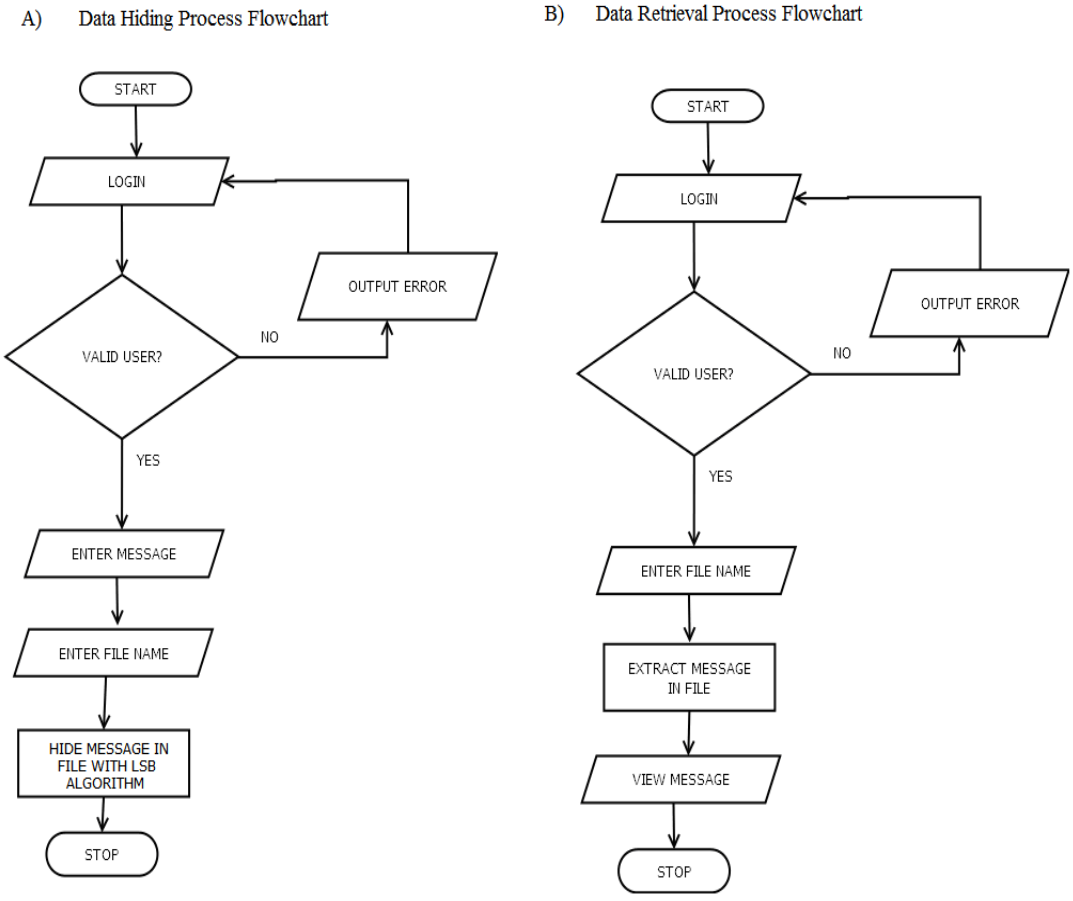

Fig. 3.1 System Process Flowchart

The mobile steganography tool was developed using the Java Programming Language and Eclipse Integrated Developer Environment on a system running the Android Development Toolkit.

The software was tested using on the PC using the Android SDK Emulator.

IV. Result

The mobile steganography tool was used to encrypt a message in a picture image file.

Figure 3.2 shows the image before the data was hidden in it.

Fig. 3.2

Figure 3.3 below shows the tool being used to hide the text in the selected image file.

Fig. 3.3

Figure 3.4 shows the image after the data was hidden in it.

Fig. 3.4

Figure 3.5 below shows the tool being used to view the text in the selected image file.

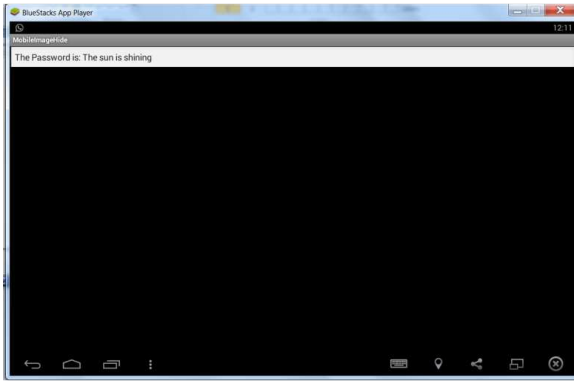

Fig. 3.5

V. Findings

The results of the test done with the mobile steganography tool revealed that visually there was no alteration to the appearance of the images before and after the steganography operation.

Also, the system was able to successfully retrieve the embedded information hidden in the file.

VI. Conclusion

Now that the majority of information takes on a digital form, it has become increasingly necessary to upgrade the means of protecting files by mobile phone users while making use of the World Wide Web. Private information can be leaked through download of malicious software, synchronizing the phones through insecure channels or loss of phones which can be picked up by questionable persons with bad intent. Whatever the source of intrusion, android phone users should have a more secure method of exchanging highly confidential messages without running risks of security breach which is the purpose of this research. Like every aspect of life, steganography also has its shortcomingsandvulnerabilities that still need to be addressed. Consequently, new steganography technologies will be released with increased efficiency.

References

[1] Ashwini Palimkar & Dr. S. H. Patil: Using SBR Algorithm To Hide The Data Into The JPEG Image. *International Journal of Security (IJS), Volume (8): Issue (2): 2014*

[2] Dunigan, T.: Work in progress on Internet steganography which involves hiding, recovering, and detecting info hidden in the TCP/IP packet headers. Oak Ridge National Laboratory, Oak Ridge, TN.

[3] J.C. Judge. (2001,November 30) Steganography: Past, Present, future Retrieved on http://www.sans.org/rr/papers/index.php?id=552

[4] Kamlesh Lakhwani and Kiran Kumari (2005): KVL Algorithm: Improved Security & PSNR for Hiding Image Using Steganography. *International Journal of Computational Engineering Research, Vol, 03, Issue, 10*

AUTHOR'S PROFILE

Bolude Oluwatosin Racheal was born in Ilesha Osun State, Nigeria, on September 16, 1987. She finished high school in 2002. For the next four years she pursued a degree at University of Ilorin, Nigeria between 2004 and 2008 where she obtained Bachelor in computer science. She received a Master Degree in Information Technology (MIT) from Obafemi Awolowo University in 2015. She worked as an Assistant lecturer at Interlink Polytechnic, Ijebu-Jesa in Osun State for Ten months before joining the Central Bank of Nigeria as an IT Support Staff in 2011.Presently, she is on working with West African Monetary Institute, Accra Ghana as an ICT Manager.

Miss. Bolude Oluwatosin Racheal is a member of Nigeria Institute of Management, APMG and Network Associate Member.

E-mail address: sayhi2tosin@gmail.com

Co-author: My Project Supervisor, **Dr.Olajide Olusegun Adeosun**, a lecturer from Ladoke Akintola University, Ogbomosho, Nigeria from Computer Science and Technology Department.

E-mail: ooadeosun@lautech.edu.ng