Journal of Engineering and Applied Sciences 12 (17): 4448-4452, 2017
ISSN: 1816-949X

Combining Steganography and Cryptography on Android Platform to Achive a High-Level Security

[1]Sarkar Hasan Ahmed, [1]Aram Mahmood Ahmed, [2]Omed Hasan Ahmed and [3]Wrya Karim Kadir
[1]Department of Computer Science, Sulaimani Polytechnic University, Sulaimani, Iraq
[2]Department of Information Technology, University of Human Development, Sulamiani, Iraq
[3]Department of Mathematics, College of Science, University of Sulaimani, Sulaimani, Iraq

Abstract: These days, using Smartphone is getting more common in the world and they are provided with powerful hardware resources and variety of communicating methods. A robust security model is applied to develop android operating systems that works on Smartphone and tablets. But it does not satisfy some users, especially whom with confidential and delicate data transmission and whom who keeps these kinds of data on their devices. At this time, users may turn to use third party applications to archive this satisfaction. In this research, a combination of Steganography and Cryptography techniques is proposed to design a third-party application for devices that run android platform to solve this issue. Also, resource limitations of different Smartphones and tablets is assessed to test whether this new technique can be handled by these devices or not as mobile devices has resource limitations if it compared to personal computers. Least Significant Bit (LSB) Steganography algorithm is used for hiding the texts and enhanced playfair algorithm as a Cryptography algorithm is used for encrypting the texts. It seems that through considering the attitudes to clean energies and their efficiency through inspiring past experiences in a combination of past and present time can not only show response to the coming problems but also it can cover some parts of economic considerations.

Key words: Steganography on android, Cryptography on android, data hiding, security on android platform, playfair, LSB

INTRODUCTION

Now a days, Smartphone and tablets have dominated a large part of human's life. And, about three out of four of the users are using Smartphone, it is according to pew-research center's survey in 2015 (Smith, 2015). Some of the most crucial specifications in the Smartphone are using different approaches of communication and having a massive capacity of storage for instance network social media, e-mail, Multimedia Message Service (MMS), Short Message Service (SMS) and Bluetooth. Correspondingly, we can say that Smartphone is a way and handy for communication in general, nevertheless it still needs enhancing and developing more tools and techniques to do data transferring securely. However, phone calls can be hacked easily with simple tools as witnessed in the UK phone hacking scandal article (Library, 2016). Also, the variety of email hacking techniques are growing rapidly by the anonymous groups (Anonymous, 2017). It gives us the feeling that communicating by phone call and e-mail are not secure and robust enough particularly in the case of sending sensitive information.

There are various methods used to secure and hide secret data for example Cryptography, Steganography and water marking (Hardikkumar *et al*., 2012). In this study, we propose applying two layers of security that are Steganography and Cryptography. Enhanced playfair algorithm is used encrypt the plain text and changed to a crumbled text that cannot be read by unauthorized user. Also, Least Significant Bit (LSB) is an algorithm of Steganography that is used as a second security layer in this work to hide the encrypted text inside an image file. In addition, we evaluate different Smartphone's hardware capabilities to know if they able to process these tasks or not.

Literature review: There are various methods of securing electronic communications. Usually these methods are techniques of Cryptography and Steganography (Song *et al*., 2011). Cryptography can be defined as way of changing information to a form so that only those who the data is intended for can understand the data.

Corresponding Author: Sarkar Hasan Ahmed, Department of Computer Science, Sulaimani Polytechnic University, Sulaimani, Iraq

Seemingly, the benefits of Steganography are hiding sensitive information and it can avoid attracting attacker's attention for itself. This approach is not only simple but also holds good aural or visual quality. Security researchers believe that combination of the two techniques increase the security to data storing and data transmission. They also said this combination can satisfy the requirements of the users and it causes to develop of several techniques in the combination of Cryptography and Steganography. One of the approaches that suggested by Khalil Challita and Hikmat Farhat (Atafar *et al*., 2013) includes embedding a secret plain message in the cover file without changing. They also mentioned that the message can be hidden in multiple file formats. However, the main drawback of this research is using multiple object (Ibrahim and Kee, 2012). As Steganography is about modifying pixel values of images, Smartphones would need to access and do low level operations on image files. And android gives developers this capability. Furthermore, computing power in Smartphones is on the increase.

Ibrahim and Kee (2012) represented an application in their study that applies Steganography on android devices. The application can only hide secret messages and also retrieve the hidden message. The stego image can only be transferred via e-mail and MMS. On the other hand, Thomas and Jean proposed another method of Steganography on android devices that is hiding messages inside an audio file. Both of the studys has a weakness point that is directly hiding a readable text without encryption inside a file. And in Ibrahim and Ke's research the Stego file can only be transferred via e-mail and MMS however there are variety of ways to share the file for example social networks, e-mails, Bluetooth and cloud services.

In this study, the given weaknesses in the mentioned studys has been solved in our proposed system, a Cryptography algorithms is combined with a Steganography algorithm rather than using one of them alone. Also, in our system the stego image can be transferred via all exists techniques in Smartphones such as social network media, clouds, e-mail, Bluetoot, etc.

MATERIALS AND METHODS

Problem definition: To design and implement an android application and provide a secure communication for users that includes the following two sections:

- Encrypt and hide a text inside an image file-this will be done by a sender
- Retrieve and decrypt the scrambled text from the image file this will be done by a receiver
- To assess Smartphone's hardware ability

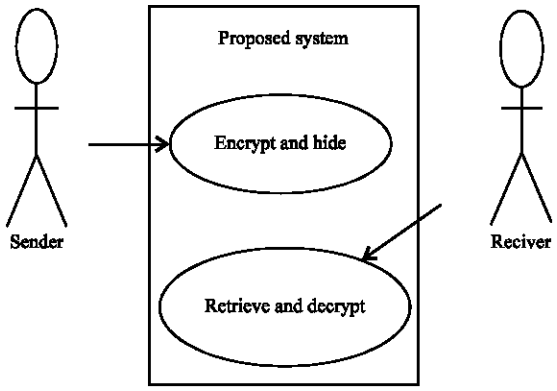

Fig. 1: The use-case diagram of the system

Algorithm: First, specifying requirements is initial point to start from by the requirements, we mean the problems that should be fixed by the proposed system. In general, the system consisted of two functions that shown in Fig. 1.

Encrypt and hide the plain text: Usually, the scenario is like this, a person has a confidential text and wants to transfer to the destination in a secure way. The sender use the proposed system then enter the sensitive message and a password then choose an image from gallery. Finally, the processes flow through two phases.

Phase 1 (Encrypting the plain text): The password is used to encrypt the plain text and changed to a scrambled text that is not readable by unauthorized person. To complete this task, an enhanced playfair algorithm is used that can support unicode characters. This algorithm uses 256×256 matrix instead of the default 5×5 matrix which holds all unicode values for all languages in the world. This massive matrix has two advantages that are holding all the unicode values and make the algorithm stronger against brute force attack (Hassan *et al*., 2015).

Phase 2 (Hiding the encrypted text): The second stage, is embedding and hiding the encrypted message inside a cover image file. It is archived by using least significant bit Steganography algorithm. That changes the least bit of each color pixel of the image. The data flow diagram illustrates the flow of data on sender side.

Decrypt and retrieve the secured text: After transferring the encrypted and hidden data over the internet, the receiver gets the image. Then, it passes through the following two phases.

Phase 1 (Retrieve the encrypted text from the image): After loading the received image from the sender in to the system and entering the key, the software start retrieving the encrypted text that was hidden inside the image. It is done, using the same algorithm that used for the hiding.

Phase 2 (Decrypt the retrieved text): In this stage, the encrypted text will be decrypted using the password and the same algorithm that was used for the encryption. The following figure shows data flow diagram for this function.

Challenges: These are the challenges and solutions that faced us during the development of this application. Resource limitations like, limited amount of RAM and limited amount of CPU is the biggest problem that faces developers of this type of devices. However, variety of solutions always exist for most of the problems.

Problem 1 (Exception (java. lang. out of memory error))
Description: Because of resource limitation in Smartphone android as an operating system limits a specific amount of resources for each application. This is the cause of this exception when a user loaded an image >3 mega bytes.

Solution (Follow these two steps to solve this problem): Image scaling: for example, if the image size is 4288×3216 pixels, after the scaling its size will be reduced to 1500×1125 pixels based on the following calculation: lets assume h = height in pixel, w = wide in pixel and h = (1500×3216)/4288; result: w = 1500 and h = 1125; changing heap size: the application can ask the O.S to provide extra resources especially the amount of RAM by changing the heap size in the Manafest.xml file.

Problem 2 (Image pixel values cannot be changed)
Description: In android when an image file is loaded into the application by default it is in immutable mode, it means the pixel values is kept and cannot be changed.

Solution (The problem can be solved in two ways): The problem can be solved with ease for Smartphones that run Android API level 14 or newer easily by changing the option (bitmap. mutable = true) during loading the image. For api levels older than 14 file based technique should be used to solve this problem. That is about reading the image file from the SD card or local memory as any other files.

Problem 3 (Avoid using image filtering for the stego image during transferring)
Description: Any changes like image cropping, adding filters, image compression on the image will change the pixel values of the image may cause to lose all hidden data inside the stego image file.

Solution: To avoid image compression in our system, during the stego file creation, there is an option to specify the compression rate of the image and 100 should be assigned that means the quality of the image is hundred percentage as shown below. (bitmap.compress (Bitmap.Compress Format.PNG,100, out).

Problem 4 (Android App Not Responding (ANR) problem)
Description: Most of the time, the GUI of the application is frozen while running a longtime process that interacts with an image.

Solution: Using background threads or multi-threading techniques can solve this problem. It can be archived by putting the longtime processes into a different threat than the default one. At that time, the GUI thread will be busy only with the GUI handling. For example async Task, intent service with result receiver or worker threads in general.

RESULTS AND DISCUSSION

The result of this research is a fully functioning application that can run on Smartphones and tablets that runs android platform. In this application, techniques of Steganography and Cryptography are used to encrypt and hide crucial information inside an image to provide relabel and secure way of data transferring. Cryptography and Steganography are used for the same purpose, however they are totally different in the way of working.

Using Cryptography alone is not secure enough to transfer confidential data because the scrambled text is a prove to emphasize for having a sensitive information and attracts attentions to itself. At the same time, applying only Steganography alone is not enough to secure a vital information as well because Steganography is embedding a readable text inside an image file. If an attacker reveals the hidden information in the image by any chance, getting back and reading the secret information will not be impossible.

Overall, the data transmission can be protected by applying the techniques of Cryptography and Steganography. The role of Cryptography in our system

Fig. 2: The image before and after applying Steganography: a) After and b) Before

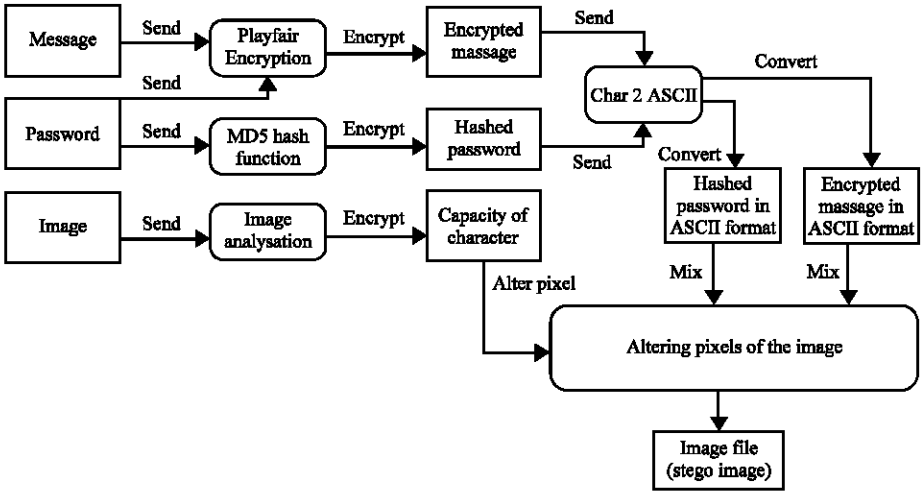

Fig. 3: The DFD diagram of encrypting and hiding the text

is converting a readable confidential message to a scrambled message. Then another security layer is applied that is Steganography. This technique hides this scrambled message inside an image file. The output of the system is an image that kept its original quality and keeps the sensitive message as well. However, changes happened to pixel values of the image but it is too small and human eye cannot detect this changes (Fig. 2).

In this case, if a malicious user reveals that there is an embedded information in the cover file then another layer defenses the confidential information that is the Cryptography algorithm.

After testing the application on multiple devices that use android operating system, we observe that these tasks can be handled by Smartphone resources and there are many functionalities in the operating system for developers to touch the modify image pixel values.

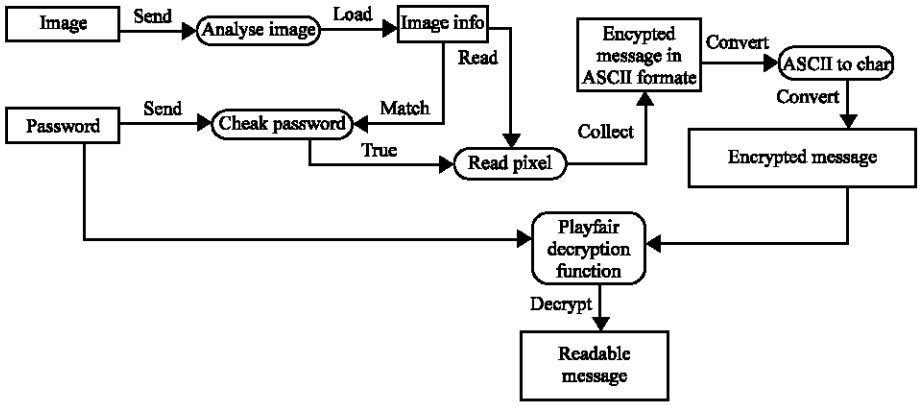

Fig. 4: The DFD diagram of retieving and decrypting the information

Techniques of software engineering were used to develop this application with the highest quality and the best performance. Then, different Smartphone types has been assessed to run this application, to observe the performance and response of them to the application requirement. The result of the observation tells us that android operating system with current device hardware limitations can handle the requirements in our application (Fig. 3 and 4).

CONCLUSION

In this research, a fully functioning and tested approach has been provided as a mobile application. The purpose of this application is to provide a way to archive a secure and robust data transmission in the android devices. To archive this goal, the combination of Steganography and Cryptography techniques are used. Least significant bit algorithm is used for hiding purpose and enhanced playfair algorithm is used to encrypt the message before doing the data hiding.

REFERENCES

Anonymous, 2017. Mobile hacking tools: The current top mobile device threats. InfoSec Institute, Illinois, USA.

Atafar, A., M. Shahrabi and M. Esfahani, 2013. Evaluation of university performance using BSC and ANP. Decis. Sci. Lett., 2: 305-311.

Hardikkumar, V., B. Pacheri and J. Distt, 2012. Steganography, cryptography, watermarking: A comparative study. J. Global Res. Comput. Sci., 3: 33-35.

Hassan, O., A. Mahmood and S. Hasan, 2015. Improving play fair algorithm to support user verification and all the languages in the world including Kurdish language. Intl. J. Eng. Comput. Sci., 4: 14058-14062.

Ibrahim, R. and L.C. Kee, 2012. MoBiSiS: An android-based application for sending stego image through MMS. Proceedings of the 7th International Multi-Conference on Computing in the Global Information Technology ICCGI, June 24-29, 2012, IARIA, Venice, Italy, pp: 115-120.

Library, C., 2016. UK phone hacking scandal fast facts. Turner Broadcasting System Inc, Atlanta, Georgia.

Smith, A., 2015. U.S. Smartphone use in 2015. Pew Research Center, Washington, USA. http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/

Song, S., J. Zhang, X. Liao, J. Du and Q. Wen, 2011. A novel secure communication protocol combining steganography and cryptography. Procedia Eng., 15: 2767-2772.