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. 3, Special Issue 19, April 2016

Retrieval of Original Password Using Multi Levels of Security in Mobiles

V.Priyanga[1], V.Saranya[2], J.Frank Vijay[3]

[1,2]Final year, Department Of Information Technology, KCG College of Technology
[3]HoD, Department Of Information Technology, KCG College of Technology
[1]mailtopriyanga95@gmail.com,[2]saranyaveeramani@yahoo.com,[3]hodit@kcgcollege.com

***Abstract*–Mobile is a widely used device all over the world. For privacy and security, password/pattern lock method of authentication is most widely used for all of the applications that are already built-in or installed by the user. So there may be chances of forgetting the password that tends the user to uninstall an application. If most of the applications in the mobile resemble the same password then that becomes the major problem. To address these authentication problems, a new alternative authentication method have been proposed. This can be accomplished through two-levels of security such as image authentication and pattern/pin lock without compromising the privacy and security of mobile. Along with image authentication, Steganography algorithm is applied that includes mapping (hiding data behind the image) and unmapping(reveals the data from the image) process. It is not just retrieval of original password rather than uninstalling an application.**

***Keywords* – Steganography, Mapping, Unmapping, image authentication.**

I. INTRODUCTION

One of the most important topics in data protection or information security today, is user authentication. The most common computer authentication method is setting alphanumerical usernames and passwords. It has got some significant drawbacks. For instance, a user tends to pick a password that can be easily guessed. If password is hard, then it is difficult to remember. Even some of the confidential application can be protected with a password/pattern lock for privacy and security. Usually if user forgets their password, then they may go with reset or help. Why user can think of retrieving the application lock password? Is that resetting is more secure? Due to these confidential data loss problems, a novel new steganography algorithm has been applied in order to implement the retrieval of original password.

Steganography refers to the hiding of secret messages in communications over a public channel so that an eavesdropper (who listens to the communications) cannot even tell that a secret message is being sent. Early works of authentication has been done on single file media. This is sometime easy to analyze and find out the secret message. Even in steganography there may have a chance of attacks in the image which is embedded. In the current work the image is used as a top secret, pattern/pin lock as a data where data embedded inside the image by using the efficient algorithm called novel new steganography [1]

In the proposed paper both the data and the image is inserted for security and reliability purpose. As in this method the message is embedded with the picture in a manner depending on the user selected picture and also the message is scrambled with image to obtain the original password.

II. EXISTING SYSTEM TECHNIQUES

Still now there is no way proposed for retrieving the password. But they were some software tools to retrieve the password, which are a big process and more time consuming. So the simple techniques which have been followed now are resetting the lock screen password. The methodologies followed here are resetting, rebooting, master reset.

A. Factory Resetting / hard resetting

A hard reset will perform the factory data reset on the device. This will give back a mobile as a brand new phone. See Figure1.The main drawback of this method is that the information currently on the phone is lost. Some amount has also been charged for the service of hard resetting. Hard reset performed by the customer care see the Figure 1.

- *UPSIDE:* Get back the phone as such in initial format.
- *DOWNSIDE:* The information currently on the phone is lost.

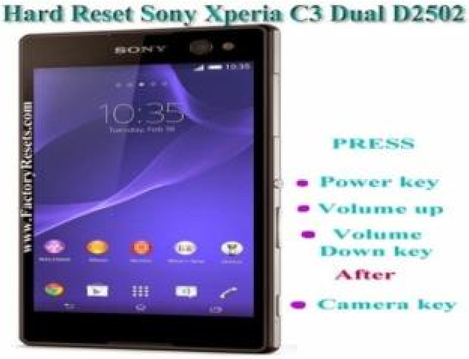


Figure 1: Hard resetting [2]

B. Rebooting [3]

Rebooting is the process by which running computer systems is restarted, either intentionally or unintentionally see the Figure 2.

- STEPS:

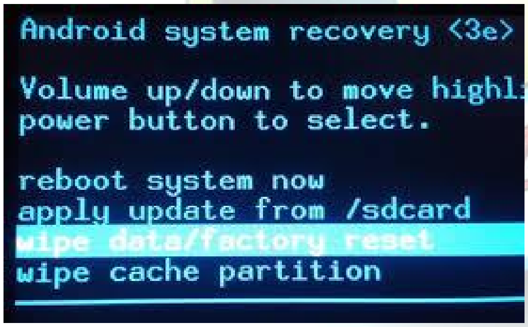
1) Set any password.

2) Power off it...

3) Then at a time press power button + volume button.

4) Some phone options are displayed. In that press wipe/system button and then press delete all the data.

5) Then select reboot/system option.



```
Android system recovery <3e>

Volume up/down to move highl
power button to select.

reboot system now
apply update from /sdcard
wipe data/factory reset
wipe cache partition
```

Figure 2: Rebooting

C .Master Reset Code

The Master Reset code is the code which restores the phone to its factory settings without deleting any of the user data.

- STEPS:

1) Switch off your mobile phone.

2) Remove the battery, sim card and the memory card.

3) Insert the battery and switch on the mobile.

4) Phone will ask the option to start mobile without sim card. Just allow it.

5) After the phone is on, type the code"*2767*2878#" [5].

6) Phone will be restarted automatically.

7) After the phone restarts, insert the sim card and memory card. As a result there will be no password stored in the mobile.

III. PROPOSED SYSTEM

A password retrieval technique has been implemented in this proposed paper. When the lock screen password and the application that are installed in the mobile shares the same password, then the retrieval of password would be more useful than just resetting the mobile. In this technique the user, select their preferred image and pin as password. Along with this password, a secret key is being entered to hide the user password. Then the password has been embedded behind the image through the new steganography algorithm. At last the hidden password is stored in the database. Unfortunately, if the password is lost then the following hidden message has been unhidden. This can be achieved with the three basic modules listed in the TABLE I.

TABLE I: Basic modules

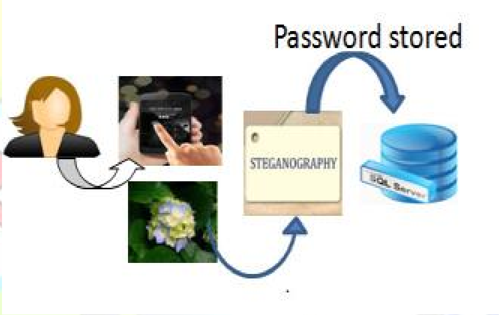


Figure 3: Module 1- Setting the password

MODULES	MODULE-1 SET UP THE PASSWORD	MODULE-2 FORGOT PASSWORD	MODULE-3 RETRIEVAL
STEP 1	Enter password	Select image	Password and image storage
STEP 2	Entering password	Password matching	Display error message
STEP 3	Select image	Image matching	Display original password

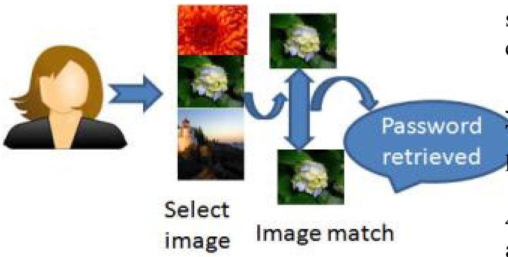


Figure 4: Module 3- Retrieving password

Figure 3 and Figure 4 explains the password setup and the retrieval of user original password. Figure 5 explains the detailed framework of the system which includes password as first level of security and steganography as second level of security to retrieve the user original password.

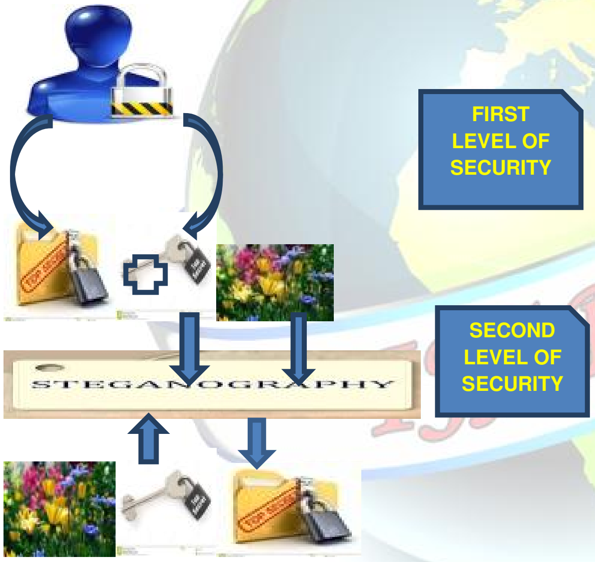


Figure 5: Framework of the system

IV. STEGANOGRAPHIC TECHNIQUE

A) Terminology

1) Cover-Image: It is an image in which the secret information (password) is going to be hidden. The term "cover" is used to describe the original, innocent message, data, audio, still, video etc. The cover image is sometimes called as the "host".

2) Stego-Image: The medium in which the information is hidden. The "stego" data is the data containing both the cover image and the "embedded" information. Logically, the processing of hiding the secret information in the cover image is known as embedding.

3) Payload: The information which is to be concealed. The information to be hidden in the cover data is known as the "embedded" data.

4) Secret key: This is the key which is used to map and unmap the cover and stego respectively in order to extract the hidden message.

B) Block Diagram Representation

The technique of steganography can be well explained using the following block diagram see the Figure 6 [4].

A piece of data that is the secret data is communicated between users (sender) and receiver. As this is a secure communication, a secret key is used for mapping (encoding) and unmapping (decoding) the data. This reduces the risk of hacking the data or third party attacks.

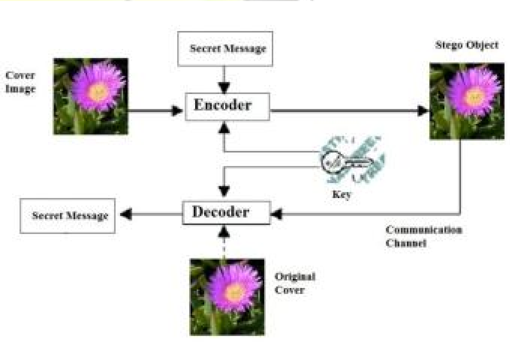


Figure 6: Block diagram of steganography

The secret data is mapped using a secret key and then embedded behind a cover image. This produces a stego image and it is stored to the database. While unmapping the same secret key is used to extract the information.

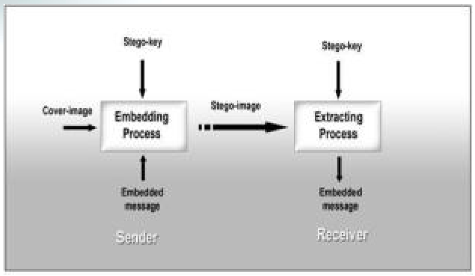


Figure 7: Framework of the image steganography.

In general, the basic framework of the image Steganography model is illustrated in the Figure 7. This model consists of two main processes, namely the embedding process and the extracting process. The main function of the embedding process is to hide the secret message, called embedded message, behind a selected image, called cover-image. In hidden communication techniques, the cover-image is no more than an innocent (unrelated to the embedded message) piece of information that is used to hide the secret information (password).

A secret key, called stego-key is used in the embedding process such that it makes the embedded message computationally infeasible to extract without possessing this key. The output of the embedding process is called stego-image, which is the original image holding the hidden secret message. This output becomes, at the other end, the input of the extracting process, in which the embedded message is extracted from the stego-image. Since the stego-key is used both in embedding and extracting process.

C) Methodology

Basic Principle

If the value of the pixel of an image is incremented /decremented by a value of '1' it does not change the appearance of the image. This fact helps us to for hiding data in an image.

1) Conversion of secret key into numbers

1. The secret key which is in the form of text is converted to numbers in base 26. Taking into consideration the fact that there are 26 letters in English alphabet, the conversion of the password into a number is carried out in `base 26.

2. An array initialized with letters of English alphabet. Taking the password as a string and checking each letter with the array, the corresponding position of the letter is identified.

3. The numbers of the letters of password obtained are assigned to another array. So the numbers are in base 26.

4. Convert those numbers into a decimal number using=n (0)*26^0 + n (1)*26^1 +n(2)*26^2 + ……

2) Transform the coefficients of image to odd numbers

Take the image and read the pixel values. An image consists of both even and odd pixels. The even pixels mean that there is some hidden information in it. Transform the even coefficients into odd numbers so that the bits in which the data is hidden are identified.

3) Generation of random length lines of text file and disordering it

The secret key is converted into a floating point number. Then generate an array of random sequence of numbers based on the floating point number obtained. The random number generation has to be done using a pre-defined algorithm which is known to both sender and receiver so that it could be useful in extracting process. The text file is split into rows and columns based on the random numbers of the array. Then a line of random length is obtained.

4) Converting text into binary numbers to embed in image

The disordered text is now converted into binary numbers, by using the ASCII values of the text. The converted numbers are vectorized and assigned to another array. Now subtract this array of binary numbers from the image coefficients which have been transformed into odd numbers, so that the pixel values change by '1' or '0', which has no effect in the appearance of image. Then the text is embedded into the image.

5) Extracting Process

At receiver side, the stego-image is received and a copy of it is made. Its coefficients are made into odd numbers. Now the pixel values of original and modified image are subtracted, in order to get the binary format of the disordered text. The secret key is already known to the receiver and generates the random number sequence in the same way as done at the sender's side. Then the binary format of the text received is converted in to ASCII, reordered using the random numbers and reverse operation is made to retrieve the original data.

V. RESULTS

The project proposed to overcome the method of resetting through two levels of security, image and data. Along with image authentication, new Steganography algorithm is applied to retrieve the original password without compromising the privacy and security of the mobile phones. Therefore, hacking the password is impossible and original password can be recovered accurately.

VI. CONCLUSION AND DISCUSSIONS

The original password of the application that is used to lock the built-in or the application that are added by the user is retrieved in case of password loss which helps the user not to uninstall an application by using the novel Steganography algorithm. The proposed paper deals with two level of security (password and image authentication). The future enhancement of this paper provides an additional level of security that deals with finger print authentication of the user.

REFERENCES

[1]Steganography Algorithm to Hide Secret Message inside an Image, Rosziati Ibrahim and TeohSukKuan, Faculty of Computer Science and Information Technology.

[2]http://growthstreet.in/android-mobile-tracker-password-reset/

[3]https://www.youtube.com/watch?v=VTdWFLbq52A,rebooting process.

[4]Improved information security using Steganography and Image Segmentation during transmission Mamtajuneja, Parvinder Singh Sandhu Computer Science and Engineering Department, Rayat and Bahra Institute of Engineering and Technology (RBIEBT)

[5]https://www.youtube.com/watch?v=hrlOPjZiT14