

Tap Based Pattern Locking System for Android Phone

Ms. Preetee K. Karmore¹

¹ Assistant Professor, Computer Science & Engineering Dept, DBACER, Nagpur, Maharashtra, India

ABSTRACT

The trend of the graphical passwords is rising and every year a number of new password schemes are being launched by researchers from the various parts of the world. Password patterns, as used on current Android phones, and other shape-based authentication schemes are highly usable and memorable. In terms of security, they are rather weak since the shapes are easy to steal and reproduce. Due to increased use of smart phones for every purpose including storing important personal data, they require a better security. Currently we are using pin lock, alphanumeric lock, pattern lock and some other locking applications. These days when talking about data security the applications currently being used somewhere lag to fulfil the requirement to some extents. This idea introduces a new innovation in the field of data security that is an application with improved features such as locking with the help of tapping some colours arranged in the circular pattern and shuffling every time when applied. In this work we are making more secured touch screen lock for android based systems by means of which user will get the facility to protect their password pattern guess by other people if the people monitoring while user unlocking their device in public place too.

Keyword : - Android, Security, Shuffling, Smartphone, Pattern Lock

1. INTRODUCTION

Now a days the smart phone users are increasing in huge manner most of android users. They perform all the activities or regular work by android smart phone. We can say the desktop or laptop is replaced with smart phones but the smart phone user must look on his security concern so the need arises how to gives security for his data [8]. Nowadays, passwords are integrated in people's routines. Humans authenticate themselves using keyboards, finger-print readers or touch screens. Smartphone's hold an important amount of information about the owner and for this reason people tend to lock them using the provided mechanisms. In most cases, phone lock mechanisms are implemented either as a PIN or a password. Contemporary smart phones using the Android Operating System adopt a type of lock mechanism different to traditional PIN codes. This approach, called 'pattern lock', is based on existing research on graphical passwords [9] and requires the user to form a pattern on the screen by drawing lines in order to unlock the device. Its interface consists of 9 nodes in a 3x3 grid formation. Users start by touching one of the dots to make it the start point and swipe their fingers to add dots and form a pattern [10]. Among these, pattern lock, PINs, and passwords are the most widely used locking features, but they are highly vulnerable to shoulder surfing and smudge attacks and therefore a new type of locking system is required. Therefore, the enhanced lock function is required to be processed multimedia content effectively due to increase in the popularity of smart devices [11]. In this paper, we proposed an application with improved features such as locking files/folders/app with the help of some colors arranged in pattern and the colour sequence of the pattern gets shuffled every time when the locked application is given an attempt to open. In this system user has to tap the colour instead of swipe or drag the pattern.

2. RELATED WORK

In this section, the pattern lock, face recognition, face and voice recognition, PIN, and password approaches, which are basic locking features embedded in multimedia smart phones, are briefly explained.

2.1 Pattern lock

This locking feature is the most widely used by the general public. The pattern locking feature consists of a 3×3 grid with simple user interface. The user selects the starting point and drags the pattern. However, the number of patterns provided is limited. This feature is vulnerable to smudge attacks by malicious attackers to unlock the pattern [11].

2.2 PIN Lock

It is most basic idea of security application. A PIN generally consist of a combination of 4-digit (from 0-9999) strong enough not to be guessed by anyone. It is very commonly used in smart phones to lock applications and even the screen of the phone. In order to unlock a locked application, the user applies the same no. sequence (4-digit PIN) which can easily be remembered by someone if once noticed [11].

2.3 Password

The password is the most widely used locking feature, not only for smart phones but also for logging in for email, home page, and SNS use. This locking feature can include a combination of various numbers, letters, and special characters. However, if the password chosen is the same as one which has been previously used, it may be exposed easily. In addition, password syndrome might occur if different passwords are used in situations where a login is required [11].

2.4 Bio-metric lock

Biometrics needs the biological information of the user such as thumb-finger impression, face structure, voice pitch and toning and retina size and colour. All these need an external hardware and a big database to manage a successful secure application. The hardware needed is very costly and needs a very high maintenance [12].

2.5 Alphanumeric lock

Alphanumeric password is somehow similar to PIN but provides a higher level of security with a combination of numbers and alphabets and hence the name given to it. But when technically speaking it becomes more risky as the users apply the passwords related to their real lives such as their date of birth, pet name, name and many more which becomes very easy for the shoulder surfers or someone known to the user to guess the password [2].

2.6 Face and Voice Recognition

In order to overcome the vulnerability of face recognition, face with voice is used as a locking feature. For its setup for locking, it follows the face recognition method along with a voice recording of the repeated pronunciation of set words. However, problems similar to those related to face recognition exist, where a similar face or photo can be used for facial recognition. Voice recognition can also be unlocked using Voice modulation or a recorded voice. Thus, the usage frequency of this method is very low. Furthermore, if face or voice recognition does not work on the first attempt, the user has to attempt to unlock the device multiple times, which is inconvenient.

3. PROPOSED SYSTEM

As the App lock starts, it accepts the pattern as an input from the user, then confirmation of the pattern will be asked. Then the user will be asked about which applications you want to lock? Then confirmation will be done. When the pattern is applied on the applications then for next time to unlock the app, applied pattern will get reshuffled. So user only needs to remember the sequence of the color code instead of the actual pattern applied. If the user enters the pattern, it will be crosschecked from the database and if pattern is correct then permission will be granted to the user to enter the application and perform the task which user want with this application. If the pattern is incorrect then user will be asked to retry the pattern.

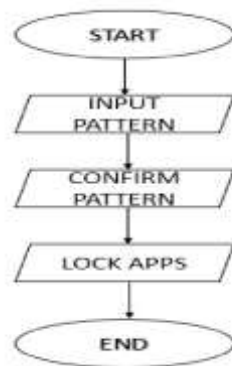


Figure 1: Pattern Lock Process

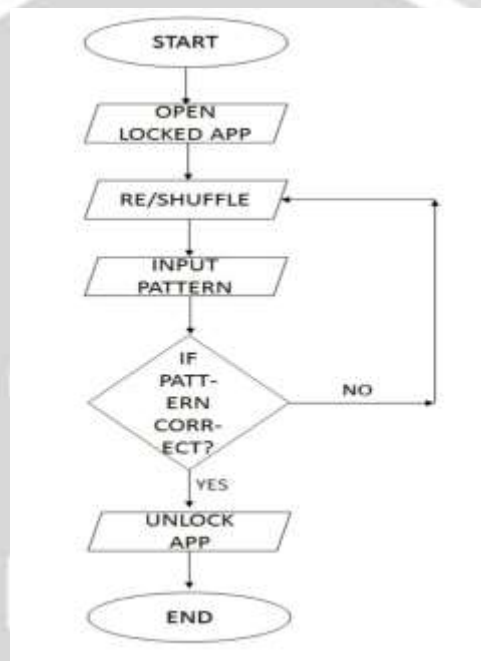


Figure 2: Opening of Locked Application

4. IMPLEMENTATION DETAILS

Step 1: Design view of pattern lock

In color code pattern lock system, we are providing color patterns of 3X3 blocks in colors. In this, we are creating nine buttons in nine colors which are stored. For showing the entered pattern, four buttons are there on top with two buttons for backspace and insertion.

Step 2: Password Creation and Confirmation

After installing the application, the user need to save the password by tapping on pattern for 4 times so the password is created then user need to tap the pattern again for confirming the pattern. This pattern is saved in session file. This session is valid till uninstalling the application.

Step 3: Applying the Lock on Applications in mobile device

The next part of application is to lock and unlock the applications in the android device. Applications from android device are stored in the database so whenever user wants to lock/unlock the applications, all the applications are on the app lock system so that user can lock/unlock the application.

5. RESULTS & DISCUSSION

This module describes exactly what the user interface is doing, how it looks like, and how the user interacts with an application.

Setting new password

In first step we have to set a new password. This step can be applied on various applications for locking purpose. Snapshot for the same is shown in figure 3.



Figure 3: Setting a new password

Password Confirmation:

In this step we have to re-enter the same password then it matches with the password which were set in first step. If it matches then the next step will be executed. Snapshot for the same is shown in figure 4.



Figure 4: Password Confirmation

Applying on various applications:

After setting a password, the application allows us to apply it on the various applications. In this way data can be secured. This application is use to maintain the privacy. Snapshots for the same is shown in figure 5.

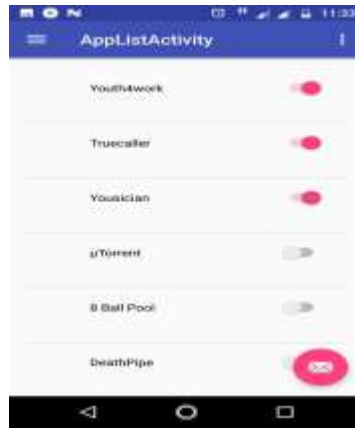


Figure 5: Applying password on applications

Enter password to open the application:

To open the application, we have to enter the correct password. So that the application which was locked can be opened. Snapshot for the same is shown in figure 6.



Figure 6: Enter the password while opening an application


6. CONCLUSION

Typically the inbuilt features and various locking systems are providing security to the applications in the smart phones, but they are not up to the mark. They are vulnerable to smudge attacks and shoulder surfing, where the passwords can be easily determined. By using the concept of pattern locks, we implemented the system having square shaped UI of colour blocks for pattern formation. This scheme provides a higher level security with the help of random shuffling of the colour blocks whenever the locked application is given an attempt to open. By providing shuffling of the colour blocks, it improves security and users convenience.

7. REFERENCES

- [1]. Adarsh Singh, Ankit M. Digraskar, Krutika R. Fulkar, Megha B. Murkute, Nikunj A. Prajapati, Mr. S. B. Lanjewar, "Color based android shuffling pattern lock", International Reasearch Journal of Engineering and Technology(IRJET), Volume: 03 Issue: 02 Feb-2016.
- [2]. Prof. V. J. Kadam, Taj Mohammad A. Raheman, Ajinkya Ajagekar and Sushant B. Patil, "Shoulder shuffling free graphical locker for android graphical pattern lock with text support for android devices", IJARCH, Volume 4, Issue 3. 2013.
- [3]. Deepika Jyoti and Dr. Amandeep Verma, "Enhancement of the security of pass-go pattern password using shuffling grid-shapes", IJIRCCE, Volume 2, Issue 11. 2014.
- [4]. Anand Bali, Saud Ansari, Kalim Khan, Wasif Shaikh, "Securing Informative Text using Color Visual cryptography", February 2016.
- [5]. Savita Patil, Jyoti Rao, "Extended Visual Cryptography for Color shares using Random Number Generators" of August 2012
- [6]. Devyani Patil, Vishakha Nayak, Akshaya Sanghavi, Aparna Bannore, "Cryptography based on Color Substitution", April 2014.
- [7]. Dinesh Sharma, Rohit Prasad, Gunraj Bedi, Archita Dad, "Colour Based Cryptography" Jan 2017.
- [8]. Kajale Bhushan M, Jambhale Prajakta S, Bairagi Ketan A, Randhir Sagar S, "Smart Color Locking System For Android Smartphones Users", International Journal of Research In Engineering And Technology, Volume: 04 Issue: 09, September 2015.
- [9]. R. Biddle, S. Chiasson and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years", ACM Computing Surveys, August 2012.
- [10]. Panagiotis Andriotis, Theo Tryfonas, George Oikonomou, "A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks", ACM 978-1-4503-1998-0/13/04, April 17-19, 2013.
- [11]. Ms. R. Srilekha, Mr. D. Jayakumar, "A Secure Screen Lock System for Android Smart Phones using Accelerometer Sensor", International Journal of Science Technology & Engineering Volume 1 Issue 10 April 2015.
- [12]. Kwang Il Shin, Ji Soo Park, Jae Yong Lee and Jong Hyuk Park, "Design and implementation of improved authentication system for android smart phone users", 26th International Conference on Advanced Information Networking and Applications Workshops 2012.

BIOGRAPHIES (Not Essential)

	<p>Ms. P. K. Karmore is working as an Assistant Professor in Computer Science & Engineering in DBACER, Nagpur, Maharashtra.</p> <p>She received M.E. degree in year 2011 from Nagpur University Nagpur, Maharashtra.</p> <p>She received a grant of Rs. 1.3 from AICTE under the scheme "Seminar grant" for conducting National Level Workshop. Her research interest is Networks & Network Security.</p>
---	---