International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Android Notes using Finger Print Authentication

Vaibhav Garg[1], Siddharth Yadav[2], Rishabh Kamal[3]

[1, 2, 3]Information Technology Department, ABES Institute of Technology, Ghaziabad, India

[1]*gargvaibhav731[at]gmail.com*
[2]*yadavsid80[at]gmail.com*
[3]*kamalrishabh007[at]gmail.com*

Abstract: ***Android devices apps are secured using various mechanisms like pattern, pin, and password. Finger print Authentication technology accepted by various android apps manufactures for better security and with change in technology. Android Fingerprint APIs are bringing user authentication to a whole new level, making it fast and secure. Unlocking an app with a single touch is one of the favourite features in android devices. This application uses the fingerprint technology for authentication in which capacitive fingerprint scanners generate an image of the ridges and valleys that make up a fingerprint. But instead of sensing the print using light, the capacitors use electrical current. The sensor is made up of one or more semiconductor chips containing an array of tiny cells and that helps in the security of the data stored in these apps.***

Keywords: Android, Biometrics, Authentication, Security, Privacy, digital fingerprint processing, mobile integration, fingerprint recognition on Android platform

1. Introduction

Mobile phones vary from simple to smart phones, from cheap to the most expensive phones. Mobile devices are not only used for communication but also for storing sensitive data and credential information like username password, bank details, personal details and such information can be misused when mobile device gets stolen or lost. With increase in mobile theft, security plays an important role. Biometric Authentication is a technology adapted by many mobile manufactures for mobile security. Biometric authentication means authenticating a person based on their biological characteristics such as fingerprint, face, iris, voice, and retina. Biometric fingerprint recognition is used in majority of the smart phone's.

The advantage of fingerprint biometric authentication over other biometric authentication is the uniqueness, high performance. All the people in the world have their own unique fingerprint, two persons cannot have same fingerprint not even the twins. A standalone biometric security is unreliable because of device vulnerabilities. With support for fingerprint sensors becoming a native part of Android as of the Marshmallow release and fingerprint sensors rapidly becoming standard fare in flagship phones as a result it's easy to get spoiled by the ease of unlocking something with a touch of your finger. This release offers new APIs to let you authenticate users by using their fingerprint scans on supported devices, Use these APIs in conjunction with the Android key store system. Your app can authenticate users based on how recently they last unlocked their device. This feature frees users from having to remember additional app-specific passwords, and avoids the need for you to implement your own authentication user interface. Your app should use this feature in conjunction with a public or secret key implementation for user authentication. Biometric security implementations are believed to prevent intrusions and theft against mobile cellular devices.

Essentially, a biometric system is used for identification or verification based on physiological and biological factors.

Fingerprint recognition may seem to be a bit more secure because a fingerprint is extremely unique and difficult to mimic. One study used fingerprint authentication for digital signing based on the X.509 certificate infrastructure. A unique feature to this research was the fact that users were able to download third party algorithms to customize protocols.

2. Literature Review

All the reviewed literature describes the existing systems and the problems that we have to overcome, some of them are discussed here:

Kataria, Adhyaru, Sharma, Zaveri [1] have briefly explained biometric authentication process and different types of authentication techniques including its strength and limitations. Fingerprint authentication have high uniqueness, permanence, performance and medium universality, measurability, acceptability, circumvention which states that it is best among other biometric authentication like hand geometry, iris, retina, face, ear, voice, signature etc.

Ritu, Sonam, Vinita, Vishakha [2] have proposed an algorithm to generate pseudo random numbers.

The algorithm has large cycle and values are uniformly distributed. The algorithm takes a seed value (X0) as input further using formula given below it is used to generate a set of random numbers.

Donny, Liza, Lei [3] has proposed a system to discourage mobile theft and prevent theft of sensitive information. The mobile phone having biometric authentication will only charge when it gets connected to phone charger which consist biometric authentication that act as a dongle.

As Ashbourn (2013) explains, the main modes of internal representation of fingerprints include: those based on main attributes of the detected details, abstracted image of the fingerprint, or the various changes of digital image's coefficients.

The pre-processing of the fingerprints consists of:

Acquisition- The fingerprints images are taken with a resolution between 250 and 625 dpi (dots per inch). Most systems use a resolution of 500 dpi and the stored images are often represented using 8 bpp (bits per pixel) in 256 levels of gray.

Pre-processing- Higher image quality by emphasizing differences in intensity between ridge lines and intergrowths.

Detection of minutiae- The automatic fingerprint identification systems use only two types of characteristic known as basic details or minutiae: ridge ending and bifurcation.

3. Objective

This System is Simple but a smart application used to secure notes via Finger Print Authentication. This System can also be referred as Keyless Authentication unlike traditional way where it needed a password to enter.

This System doesn't have any Registration but only the owner of the phone can access these notes as it searches for the owners print. This System can be used as private notes or personal diary or important notes; can be given multiple names but plays a similar role of recording notes and keeping it away from everyone then the phones owner.

If there is no Biometric feature on the phone, this app can't be used. The user can add new notes, edit old notes as well as delete notes. The Front end used is Android Studio and the Back end used is SQLite. Biometric Authentication is the highest level of security any Phone can offer making it very accurate and very secure. We will be developing an application which can store personal notes in android mobile using fingerprint authentication.

Fingerprint Matching Techniques
The large number of approaches to fingerprint matching can be coarsely classified into three families.

Correlation-based matching: Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g. various displacements and rotations).

Minutiae-based matching: This is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. Minutiae are extracted from the two fingerprints and stored as sets of points in the two- dimensional plane. Minutiae based matching essentially consists of finding the alignment between the template and the input minutiae sets that results in the maximum number of minutiae pairings

Pattern-based (or image-based) matching: Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centres on that. In a pattern based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match. In Our project we have implemented a minutiae based matching technique. This approach has been intensively studied, also is the backbone of the current available fingerprint recognition products.

4. Methodology

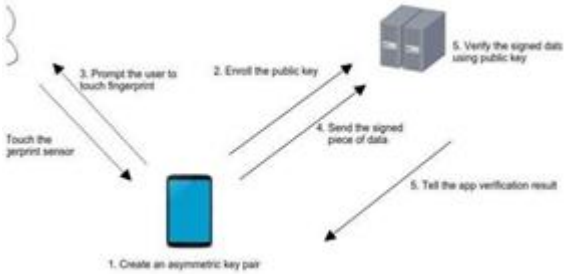
The block diagram of the Biometric Identification System (BIS) is clearly referred in a figure 2 given below. It consists of three components which are shown with the help of a flowchart to identify fingerprint image.

Each of the component mentioned in the flowchart are described as follows:

Image Generation with reference to problem domain, image sensor acquires digital images. First is a Physical device that is sensitive to the energy radiated by the object. The second, called a Digitizer, is a device for converting the output of the physical sensing device into digits' form. Specialized image processing hardware consists of the digitizer and hardware that performs other primitive operations. The Computer is an image processing system which ranges from PC to Supercomputer. Software for image processing consists of specialized modules that perform specific tasks. Mass storage capability is a must in image processing applications. An image of size 1024x1024 pixels, in which the intensity of each pixel is an 8- bit quantity, requires one megabyte (MB) of storage space, if the image is not compressed. Image displays in use are mainly colour TV monitors. Monitors are driven by the outputs of image and graphics display cards that are an integral part of the Computer System.

Image Enhancement Image enhancement approaches are basically categorized into two broad categories, which are discussed here. 1. Spatial Domain Methods Spatial domain refers to the aggregate of pixels composing an image. Spatial domain methods are procedures that operate directly on these pixels. It can be denoted by the expression: $g(x, y) = T [f (x, y)]$ Where f (x, y) is the input image, g(x, y) is the processed image and T is an operator of f, defined over some neighbourhood of (x, y). C.

Implementation



Step 1: Add the required permissions in the AndroidManifest.xml
AndroidManifest.xml

Step 2: Check if the device supports Biometric authentication

Specifically, we are going to check if the following conditions are met:

The device is running Android 6.0 or higher The device features a fingerprint sensor

The user has granted your app permission to access the fingerprint sensor.

The user has registered at least one fingerprint on their device.

We can create a separate until class to check if the above conditions are met:

Step 3: Display Biometric Prompt dialog

Once the above conditions are checked, we can check if the android version in the device is Android
P. The Biometric dialog is only supported in Android
P. Let's take a look at that first.

Below code is to display a biometric
Prompt dialog: Using the BiometricPrompt builder we can:
setTitle() — Set the title to display (Required)
setSubtitle() — Set the subtitle to display (Optional)
setDescription()— Set the description to display(Optional)
setNegativeButton() — Set the text for the negative button(Required). You must also provide an Executor instance and a click listener for the negative button.

Note: You can't customise the icon or error message that are used within the dialog.

A typical Biometric Prompt dialog.

Step 4: Handle authentication Callback

Next we use the Biometric Prompt. Authentication Callback to listen for authentication events from the users. It includes 4 methods: on Authentication Succeeded

When the fingerprint is has been successfully matched with one of the fingerprints registered on the device, then this callback will be triggered. An Authentication Result object will be passed the callback on Authentication Failed

When the fingerprint doesn't match with any of the fingerprints registered on the device, then this callback will be triggered on Authentication Error

When an unrecoverable error has been encountered and the authentication process has completed without success, then this callback will be triggered. The callback is provided with an error code to identify the cause of the error, along with the error message. The different types of error codes that can occur are:

BIOMETRIC_ERROR_LOCKOUT- The operation was cancelled because the API is locked out due to too many attempts.
BIOMETRIC_ERROR_LOCKOUT_PERMANENT- The operation was cancelled because
BIOMETRIC_ERROR_LOCKOUT occurred too many times.
BIOMETRIC_ERROR_NO_SPACE- The operation cannot be completed because there's not enough storage remaining to complete the operation.
BIOMETRIC_ERROR_TIMEOUT- Timeout occur as the current request has been running too long.
BIOMETRIC_ERROR_UNABLE_TO_PROCESS- The sensor was unable to process the current

Data flow diagram of Smart Glove image

BIOMETRIC_ERROR_USER_CANCELED- The user canceled the operation.
BIOMETRIC_ERROR_VENDOR- If there are conditions that do not fall under one of the above categories.
BIOMETRIC_ERROR_NO_BIOMETRICS- The user does not have any biometrics registered in the device.
BIOMETRIC_ERROR_CANCELED- The operation was cancelled because the biometric sensor is unavailable.
BIOMETRIC_ERROR_HW_NOT_PRESENT- The device does not have a biometric sensor.
BIOMETRIC_ERROR_HW_UNAVAILABLE- The device hardware i s unavailable.

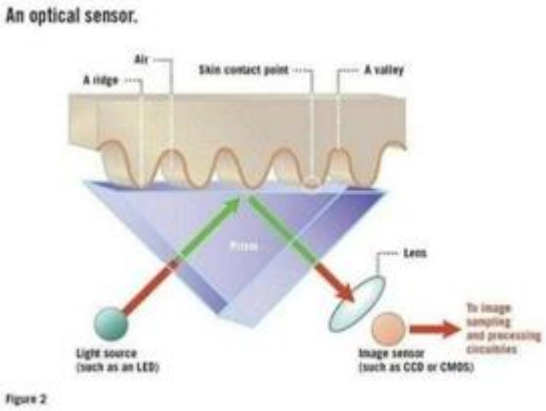
5. Comparative Study

Optical scanners
Optical fingerprint scanners are the oldest method of capturing and comparing fingerprints. As the name suggests, this technique relies on capturing an optical image, essentially a photograph, and using algorithms to detect unique patterns on the surface, such as ridges or unique marks, by analysing the lightest and darkest areas of the image.

Just like smartphone cameras, these sensors can have a finite resolution, and the higher the resolution, the finer details the sensor can discern about your finger, increasing the level of security. However, these sensors capture much higher contrast images than a regular camera. These scanners typically have a very high number of diodes per inch to capture these details up close. Of course, it's very dark when your finger is placed over the scanner, so optical scanners also incorporate arrays of LEDs as a flash to light up the picture come scan time.

Such a design is a bit bulky for a smartphone though, where slim form factors are important. The major drawback with optical scanners is that they aren't difficult to fool. As the technology is only capturing a 2D picture, prosthetics and even other pictures of good enough quality can be used to fool this particular design. This type of scanners really isn't secure enough to trust your most sensitive details too. It's also slowly being phased out these days.

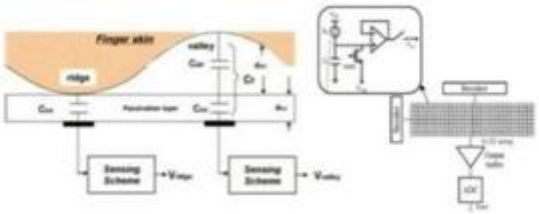
With increasing demand for tougher security, smartphones have unanimously adopted superior capacitive scanners, and the falling cost of technology has made capacitive alternatives viable for mid-range products too.



Advantages:
Works perfectly even with wet fingers.

Disadvantages:
Since it takes a 2D picture, it can be fooled easily Capacitive scanners.

The most commonly found type of fingerprint scanner used today is the capacitive scanner. Instead of creating a traditional image of a fingerprint, capacitive fingerprint scanners use arrays tiny capacitor circuits to collect data about a fingerprint. As capacitors can store electrical charge, connecting them up to conductive plates on the surface of the scanner allows them to be used to track the details of a fingerprint. The charge stored in the capacitor will be changed slightly when a finger's ridge is placed over the conductive plates, while an air gap will leave the charge at the capacitor relatively unchanged. An op- amp integrator circuit is used to track these changes, which can then be recorded by an analog-to-digital converter.



Advantages:
- More Secure than Optical Scanners.
- Can't be unlocked when a person is dead.

Disadvantages:
Even though it is secure, it only uses the 2D implementation i.e it can only scan the prints on the finger which are on the outer side.

Can't be unlocked when fingers are wet.

As they are placed outside of the phone, there is a chance of dust and any stains on them. So they should be cleaned at least once in a while.

Ultrasonic scanners
The latest fingerprint scanning technology to enter the smartphone space is an ultrasonic sensor, which was first announced to be inside the Le Max Pro smartphone. Qualcomm and its Sense ID technology are also a major part of the design in this particular phone.

Advantages:
More secure than all other scanners as this uses a 3D reproduction. Can be unlocked with wet fingers.

6. Conclusion and Future Work

The simulation results showed that the proposed biometric authentication system performs better with the total memory and CPU usage. Most cell phones use a password, PIN, or visual pattern to secure the phone. With these types of security methods being used, there is much vulnerability. Another alternative is biometric authentication.

Biometric security systems have been researched for many years. Some mobile manufacturers have implemented fingerprint scanners into their phones. Since theft of cell phones is becoming more common every day, there is a real need for a security system that not only protects the data, but the phone itself. It is proposed through this research that a biometric security system be the alternative to knowledge-based and password based authentication. So we can utilize the systems biometric authentication feature towards our

application for better security and confidential data processing. This will not be a burden to integrate and not easy to stolen like traditional authentication factors like user id and password and also it will not consume much memory. So it would be a nice feature, the application with biometric authentication.

References

[1] Kataria, Adhyaru, Sharma, Zaveri, "A survey of automated biometric authentication techniques" In Proceedings of the IEEE Nirma University International Conference on Engineering (NUiCONE), pp. 1-6, 2013.
[2] Ritu, Sonam, Vinita, Vishakha, "VRS algorithm A Novel Approach to Generate Pseudo Random Numbers" In Proceedings of the IEEE International Advance Computing Conference (IACC), pp. 7-10, 2014.
[3] Donny, Liza, Lei, "Preventing Cell Phone Intrusion and Theft using Biometrics" In Proceedings of the IEEE Security and Privacy Workshops (SPW), pp. 173- 180, 2013.
[4] Charles Severance. "Anil Jain: 25 Years of Biometric Recognition" IEEE Journal Computer, pp. 8-10, 2015.
[5] Weizhi Meng, Wong, Furnell, Jianying, "Surveying the Development of Biometric User Authentication on Mobile Phones" Communications Surveys & Tutorials, IEEE, pp. 1268- 1293, 2014.
[6] Zhiling, Yufei, "Understanding User's Behaviors in Coping with Security Threat of Mobile Devices Loss and Theft" In Proceedings of the IEEE 45th Hawaii International Conference on System Sciences (HICSS), pp. 1393 – 1402, 2012.
[7] R. Schwamm, N. C. Rowe, "Effects of the factory reset on mobile devices," in The Journal of Digital Forensics, Security and Law (JDFSL), VOL 9, NO 2, pp. 205-220, 2014.
[8] L. Simon, R. Anderson, "Security analysis of android factory resets" n 3rd Mobile Security Technologies Workshop (MoST) IEEE Computer Society Security and Privacy Workshops, 2015.
[9] Laurent, Ross, "Security Analysis of Consumer-Grade Anti-Theft Solutions Provided by Android Mobile AntiVirus Apps" Mobile Security Technologies (MoST) IEEE Computer Society Security and Privacy Workshops, 2015.
[10] Nseir, Hirzallah, Aqel, "Issues with Various Security Threats on Mobile Phones" In Proceedings of the IEEE Information and Communication Technology (PICICT), pp. 37 – 42, 2013.
[11] Yamazaki, Dongju Li, Isshiki, Kunieda, "SIFT based algorithm for fingerprint authentication on smartphone" In Proceedings of the IEEE Information and Communication Technology for Embedded Systems (ICICTES), pp. 1 – 5, 2015.
[12] Khan, Qureshi, Qadeer, "Anti-theft application for android based devices", In Proceedings of the IEEE Advance Computing Conference (IACC), pp.365 – 369, 2014. al Conference Ankur, Divyanjali, Bhardwaj, "A dissection of pseudorandom number