Contribution of Biometrics in Securing Mobile Phones

Bojamma A.M [1], Rohini Suzana J [2], Dr.M.P.Indra Gandhi[3]

Abstract— Many mobile phone users consider the PIN to be inconvenient as a password that is complicated enough and easily forgotten and very few users change their PIN regularly for higher security as can been seen. Mobile phones have become the most important resource an individual can possess and has a million chances of getting stolen. With the expansion of the functionalities of a mobile phone personal digital assistance, banking, e-commerce, remote work, internet access and entertainment, more and more confidential data is stored on these devices is highly at stake. How can the data that is present in the mobile phones be secure? Biometrics is the solution to it. This article describes the role of biometrics in cellphones to ensure security.

Index Terms— Biometrics, 7 keywords are mandatory, Keywords should closely reflect the topic and should optimally characterize the paper. Use about four key words or phrases in alphabetical order, separated by commas.

1 Introduction

Cell phones are turning out to be progressively refined and now fuse numerous various and intense sensors.

The most recent era of advanced cells is particularly loaded down with sensors, including GPS sensors, vision sensors (cameras), sound sensors (receivers), and light sensors, temperature sensors, heading sensors (compasses), and speeding up sensors. The most important aspect of any gadget is to ensure security of the data stored in it. This can be achieved by the use of Biometrics. Mobile biometrics deals with deploying biometric authentication methods on mobile devices such as smartphones and tablets. Functionalities of mobile biometrics include securing sensitive data on personal or corporate mobile devices, such as enterprise or financial information (bank details), providing authorization of users.

Biometric systems can be used with cell phones in two ways: As a biometric collecting device or as a stand-alone system to protect unauthorized use of the cell phone. In the first scenario cell phones are collecting the biometric information and then it is passed over via internet or via voice communication to a remote location where it is evaluated and matched. This serves for remote transactions when the identity of the caller has to be authenticated. Another way of biometric systems being integrated on cell phones is that the entire biometric system resides on the cell phone and it serves to prevent against unauthorized access to cell phone's functions and data. Biometric systems can be a substitute for the annoying PIN security and with a swipe of a finger the phone can be unlocked and accessed. As of now the most common implementations of biometric systems on cell phones include voice recognition, fingerprint recognition, face recognition, signature recognition and keystroke recognition.

2 Working of Biometrics

The biometric system follows four steps to perform identification and verification −

Record live sample from candidate. (using sensors)

Extract prominent features from sample. (using processing unit)

Comparison between the live sample with samples stored in database. (using algorithms)

Decision making. (Accept or reject the candidate.)

The biometric sample is recorded by the candidate user. The prominent features are obtained from the sample and it is then compared with all the samples stored in the database. When the input sample matches with one of the samples in the database, the biometric system allows the person to access the resources; otherwise prohibits.

3 Applications of Biometrics in Mobiles

3.1 Fingerprint identification on mobile phone

Fingerprint biometric has been used widely for having authorized access in devices requiring high level of security such as military bases and laboratories. By embedding a fingerprint scanner to the mobile phone assures high security.

Fingerprint Recognition is responsible for taking a fingerprint image of a person and recording its features like arches, whorls, and loops along with the outlines of edges, minutiae and furrows. An exact match of the Fingerprint can be attained in three ways, such as minutiae, correlation and ridge

•Minutiae based fingerprint matching: In this technique the image is stored as a plane which includes a set of points and the set of points are corresponding in the template and the input minutiae.

- *Bojamma A.M is currently an assistant professor of the Computer Science Department of St Jospehs College 36, Lal Bagh Main Road, Bengaluru, Karnataka 560027*
- *Rohini Suzana J is currently is currently pursuing masters degree program in Computer Science Department of St Jospehs College 36, Lal Bagh Main Road, Bengaluru, Karnataka 560027*

•Correlation based fingerprint matching: This technique uses the concept of overlaying two fingerprint images and associating the difference between equivalent pixels.
•Ridge feature based fingerprint matching: In this method the ridges are capture, as minutiae based fingerprint, but capturing of the fingerprint images is difficult in low quality.

3.2 Voice Recognition:

Voice recognition is used to produce speech patterns by combining physiological and behavioral factors that can be captured by processing the speech technology. The most important parameters used for speech authentication are fundamental frequency, nasal tone, inflection, and cadence. Voice recognition can be classified into different categories based on the kind of, such as a fixed text method, in the text dependent method, the text independent method and conversational technique.

3.3 Face Recognition

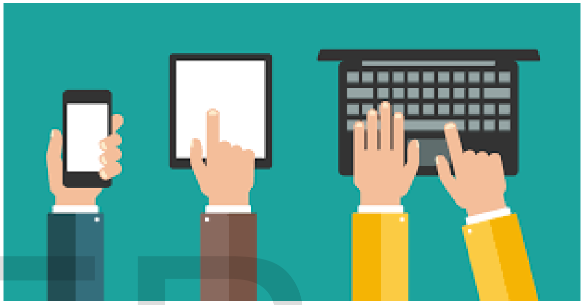
Face recognition system is a one type of biometric application which has the ability to identify or verify a person by using a digital image by comparing and analyzing patterns. As of now the facial recognition systems work with face prints and these systems can recognize 80 nodal points on a human face. Nodal points are defined as the end points that are used to measure variables on a person's face, which includes the length and width of the nose, cheekbone shape and the eye socket depth. Currently, these face recognition techniques focus on smartphone applications which include personal marketing, social networking and image tagging purposes and also authorizing the owner of the phone or laptops.

3.4 Signature Recognition

This method is used to analyze and measure the physical activity of signing with the help of few attributes such as pressure applied, stroke order and the speed. Some biometrics compare visual images of signatures. Signature recognition can be checked for using two different ways, such as static and dynamic.

In Static mode: consumers usually write their signature on paper, digitize it with the help of a camera or an optical scanner. This system identifies the signature examining its shape. In dynamic mode: consumers write their signature in a tablet which obtains the signature in real time and digitizes it.

3.5 Key stroke recognition:



Keystroke dynamics also known as typing dynamics is an automated method of confirming the identity of an individual based on the manner and the rhythm of typing on a keyboard. With keystroke individual can be identified based on the typing pattern, speed of typing and the rhythm on a keyboard. The parameters used for keystroke dynamics are dwell time and flight time.
•Dwell time is the time duration that a key is pressed
•Flight time is the time duration in between releasing a key and pressing the next key

4 Conclusion

The use of pin numbers to secure mobile devices have been replaced with hassle free biometrics techniques. There is no longer a necessity to remember a password to access mobile phones. The ideology of securing mobile phones with biometrics is highly appreciated over using pins. No more doubts about someone else being able to retrieve data from mobile devices by guessing passwords. The techniques discussed above if employed in mobile phones can definitely reassure the security of mobile phones.

References

[1] International Journal of Emerging Technology and Advanced Engineering Biometric Based Secured Authentication in Mobile Web Services Ms. K. M. Brindha Shree, Mrs. M. Rajalakshmi

[2] Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption Shari Trewin, Cal Swart1, Larry Koved, Jacquelyn Martino, Kapil Singh, Shay Ben-David

[3] Biometric Security for Cell Phones Adrian POCOVNICU Academy of Economic

Studies, Bucharest, Romania
[4] Biometrics on Mobile Phone Shuo Wang and Jing Liu Department of Biomedical Engineering, School of Medicine, Tsinghua University
[5] Cellular Phone: A Contemporary Tool for Biometric Implications Neeraj Kumar, Raees A. Khan, and Dhirendra Pandey, Senior Member, IACSIT