IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

Biometrics for Cell Phone Safety

Jyoti Tiwari[1], Santosh Kumar[2]

M.Tech Scholar, Department of Electronics and Communication, Invertis University, Bareilly, UP[1]

Assistant Professor, Department of Electronics and Communication, Invertis University, Bareilly, UP[2]

Abstract: In the recent times, a mode of communication has changed drastically. Since last decade technology has meticulously changed the use of cell phones. In the contemporary times cell phones have been transformed to a device that is not able to act as a mode of communication but it can also successfully perform all the work of a personal computer. This means executing half the official work by a pocket carrying device will be requiring high security and safety measures. Apart from the safety of confidential data, the safety of the device is becoming a concern for the common masses. As cell phones have turned into prime targets for theft. Cell phones are equipped with PIN security feature but people either do not use it or they simply do not trust. So it is the need of time to upgrade and update all the security features of a cell phone.

Keywords: Biometrics, security, fingerprint, face recognition, cell phones.

1. INTRODUCTION

All humans have questioned once in their entire life about their own identity who they are. Where have they come from or where are their roots implanted. These were some of near to impossible questions unanswered for people 2-3 decades ago. But the immense research and advances of modern science and technology introduced to a different experience that included all the population. Now with the help of different devices we can identify any person from any place and time. This technology came to be known as biometric. Biometrics is the measurement and statistical analysis of people's physical and behavioral characteristics. These charters tics are iris pattern, retina image, face or hand geometry, and behavioral characteristic such as voice, gait or signature. [1]Biometric security system identifies a person on the basis of what he is. This system has revolutionized the setup of security and safety in every phase of human life. The advantage of biometric system over conventional security methods that they cannot be breached or stolen anywhere. It provides convenient and low cost security. It reduces fraud as the chances of forging of ID cards or smart cards are diminished. It creates a vast database network that can be access from anywhere in the real time using internet. Biometric security systems are based upon two characteristics-physical and behavioral. In physical human characteristics, traits like finger print, iris, retina, DNA, hand geometry are included. On the other hand, under behavioral characteristics traits like speech, signature and keystroke timing are taken. If we look at the purpose for which biometrics system are use, we will see there are two main purposes. One is to validate the identity of user by comparing his biometric trait with the one stored for that user in the data base. The second purpose of using biometrics is to identify user by taking his biometric trait and comparing it with the group of same traits from various users. This purpose is to search for relationship of the user with the group of other users.

2. COMPONENTS OF BIOMETRIC SYSTEM

A biometric system usually consists of the following components:

Data collection: The first step for the use of a biometric system is the capture and acquisition of biometric data from biometric sensor hardware. Usually, it is affected by human factors, environmental conditions and quality of sensor used. The final result of enrollment process is an image or signal captured directly from individuals. The Failure to Enroll Rate measures the lack of success of enrollment process. In Signal Processing methods and algorithms are applied to the enrolled data in order to detect and extract their main features. Ideally, the extracted biometrical features must describe uniquely an individual. The final result of signal processing component is the template creation. A template is a structure for biometric features representation. The algorithms used for extraction are proprietary and are the core intellectual property of biometrics vendors. [2]

Transmission: In some biometric systems data collection and processing occurs at different places. In those cases, biometric data must be transmitted from data collection to the signal processing components. Generally, that transmission process involves a great amount of data and compression techniques are applied. The compression technique used depends of biometric type and some standards have been defined. Wavelet Scalar Quantization (WSQ) is the standard compression format for fingerprints images and JPEG200 standard format for facial images. For voice signal the Code Excited Linear Prediction (CELP) is defined as standard format.

Storage (Template Creation): Biometric data is never stored on database in its original format, i.e. digital image. The signal processing methods detect features on enrolled data and organize them as a so called characteristic vector.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

A characteristic vector is a description of the main features detected for Signal Processing component and must be small and easy to process. There exist proposals of standards format of templates for fingerprint based on minutiae point found in fingerprint images.
Nevertheless, usually the template format and type of information it stores is part of the proprietary core intellectual property. Some of the biometric technology contests as FVC (Fingerprint Vendor Competition) impose limits to the memory size of templates generated by algorithms.

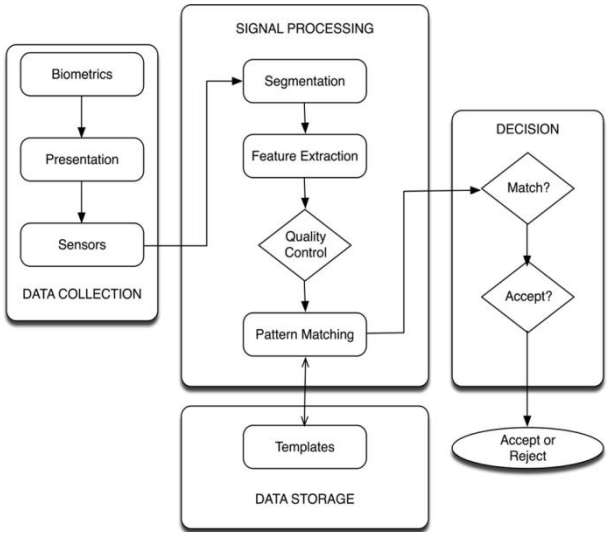

Figure 1: Biometric System

Decision Making: In Decision (Matching) the final component of a biometric system is the decision or matching component. Decision component compares a query biometric template with the stored template of claimed person and assign them a similarity score. That score is used for make decisions about the matching or not of the templates.

In Verification Systems if the similarity scores are greater than a fixed threshold the system decides that templates belong to the same person. In Identification System the database templates are compared query template and higher similarity score templates are selected to decide if some person was identified on database.

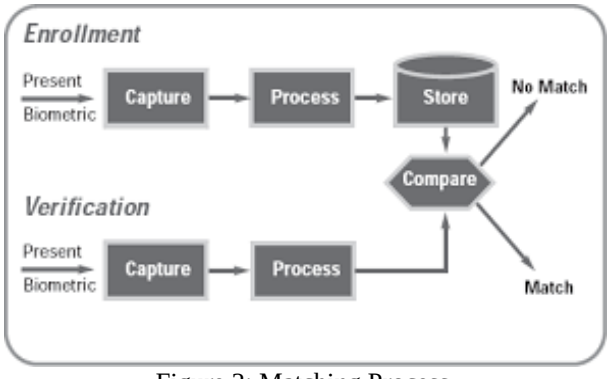

Figure 2: Matching Process

3. BIOMETRICS CHARACTERISTICS

Technology must be for every common person, similar is the cases with biometrics. It should reach each and every person. each biometric has its own negative and positive accept and the selection of the biometric should not relay on its matching performance but it should also see whether there is a need of biometrics system for the application or not. In this sequence we talk about accuracy, biometric technology itself is based on accurately validating a person's true identity. Without accuracy the idea of biometrics itself will be baseless.
Secondly biometric system must be reliable in every sense be it performance accuracy or speed. The work flow of biometric system should be continuous. It should not be interrupted in any case even when authorized persons access the system while blocking others.
Another factor is time consume while enrolling the user. [3] Today we see that biometric systems take very short time for enrolling which saves a lot of expense. A system requiring a -minute enrollment instead of 2 minutes' causes 50 hours of expensive nonprofit time if 1,000 users must be enrolled.

4. CELL PHONE AND BIOMETRICS

Improved technology has made a great change in the history of mobile phones, transforming the huge brick-like mobile phones of 1995 to sleek and stylish Smartphone we carry with us now. No one could have imagined that in a mere 20 years, mobile phones could have made the leap from just being the alternative to landlines to becoming a computer, GPS, radio and our lifeline to the Internet, and still be able to fit in your pocket. As we have discussed earlier that security is a major concern for us and our belongings biometrics has proved to be a boon for us. We just have to develop this particular technology to an extent so that it can be used in maximum places and by maximum gadgets. This paper should throw light on how phone security can be elevated to a new level that would not only save data but also the device.

The notion of fusion of biometrics to cell phone device is turning into a reality and the research phase is on. Researchers have successfully found out two ways by which biometrics can be used with mobile phone to them. The first way is to keep the phone connect through a network frequency so that all the data collected by the phone can be transferred online to the remote database and from there it can match the sent data with the previously stored templates. This proves useful for remote transactions when the identity of the caller has to be proven. [4] For example, when a user calls his bank to make a transaction he is requested to speak a sentence, the voice is then processed and compared to the sample that was collected when the user was enrolled in the system.If we look at the second way, then we will find that cell phones can secure themselves independently if loaded with biometric recognition features. It can totally diminish

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

the possibility of data breach and prevent unauthorized access to cell phone.
In the present time the applications of biometric systems on cell phones include fingerprint recognition, voice recognition, face recognition, signature recognition, gait recognition, gesture recognition and keystroke dynamics.
Now, let us look at some of the biometric traits that are being used successfully by cell phones.

Fingerprint: As a matter of fact, fingerprint recognition technique is the oldest approach among all the biometric techniques ever discovered. True Print® is used to capture the fingerprint image from the live layer of skin beneath the surface. [11] This has reduced the risk of not accepting a fingerprint because the skin surface has worn-out.

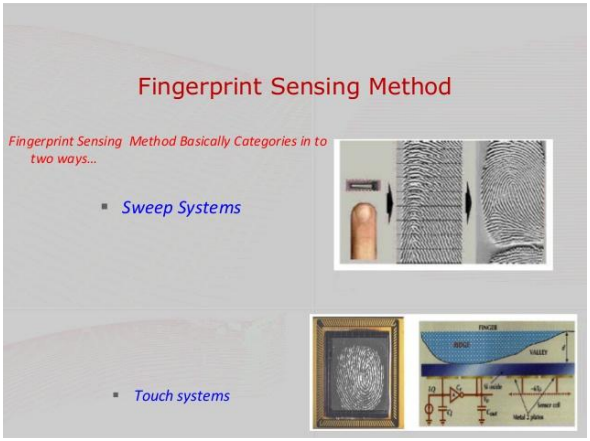

Figure 3: Fingerprint Sensing Method

The most commonly found type of fingerprint scanner used today is the capacitive scanner. Capacitive fingerprint scanners use arrays of tiny capacitor circuits to collect data from a fingerprint. We know that capacitors can store electrical charge, if we connect them to conductive plates on the surface. Then the scanner will allow them to be used to track the details of a fingerprint. When a finger's ridge is placed over the conductive plates the charge stored in the capacitor will be changed slightly 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 (ADC).

After captured, the digital data it can be analysed for distinctive and unique fingerprint attributes, that is saved for comparison. Using more capacitors results in a higher resolution scanner, increasing the level of security. In 2011, among Android phones, Atrix became the standard-bearer by getting this feature. iPhone 5s in 2013 and naming it as Touch ID. [12]

In April 2014, Samsung finally launched a phone that boasted fingerprint sensor and that was Galaxy S5. Galaxy S5 featured a fingerprint sensor that worked just like iPhone 5S Fingerprint scanner is studded on Samsung galaxy S7&S7 Edge in 2016.

Face recognition: At present majority of mobile devises use PIN security system to access the device, everyone who uses pass code is aware of how much effort it takes to remember a long and tricky password. Few of them have developed security module based on fingerprint recognizing devise, thanks to biometrics. But then also it requires having a fingerprint of which all the ridges are in proper condition, a problematic condition for old people and injured or burnt skin. [13] To solve both security and usability problem simultaneously, various types of biometrics have been proposed. Among many biometric solutions the idea of face recognition is developing too, as all the phones are equipped with camera. Now how it actually works, we have to first set our picture on the Smartphone to recognize ourself, the phone's owner, by facing the camera toward us and lining up our face inside the dotted lines on the screen. Then, anytime we want to use the phone then we have to simply point the camera toward our face and it unlocks. But it has a flaw been that this Android facial recognition feature can be tricked with a photograph of the owner.The Smartphone is doing its job correctly to analyzing the face to confirm it's the person who set up the phone but it can't distinguish between a live person and a still photo. It also creates trouble while detecting the in low lighting situation. So these problems need more research for smooth process.

Signature: Now we move to handwritten signature. It is one of the important biometrics in terms of establishing the identity of an individual, mainly because of the social and legal acceptance of handwritten signatures. The latest innovations using touch screen technologies have provided a working environment for signature verification in smart phones.

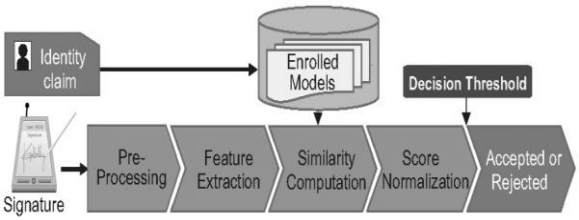

Figure 4: Decision Making

Various steps that are administered while verifying the signature of user are as follows:

A. Data Acquisition: For acquiring a signature data in general we use devices like digitizing tablets or through the touch screen technologies provided on Tablet PCs, PDA or Smart Phones. The dominant attributes captured are x and y pen positions, and the time taken. Other attributes such as pressure, pen-azimuth, pen-up positions, etc can also be captured.

B. Feature Extraction: In this level we can extract various types of discriminate features from the given sample. For signature data, the methods are traditionally classified into two: Feature-based and Function-based.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

C. Enrollment: When the user enrolls for the first time there are two ways they can be enrolled they can be classified into reference-based where features extracted from the signature are stored as templates and model-based where a statistical model representing the signatures is generated.

It is aptly said that future of smartphones will be totally fused with biometric system. The growth in number of units in 2017 is expected due to the integration of touch fingerprint sensors in the entry-level smartphone segment, which according to Strategy Analytics is estimated to reach somewhat more than 500 million devices, representing approximately 30 percent of the total smartphone market.

Fingerprint Cards (FPC) has introduced FPC1028, a touch fingerprint sensor developed for integration of touch fingerprint sensors in the entry-level segment of the smartphone market.

FPC1028 is FPC's most cost-efficient solution for smartphone manufacturers and will enable smartphone manufacturers to integrate a touch fingerprint sensor in the entry-level segment for secure and convenient user authentication. The lower manufacturing cost is due to a smaller sensor surface area as well as the total system solution, which has helped to reduce costs for integrating the touch fingerprint sensor in a fingerprint sensor module.

A revolutionary invention has just come into practice when smartphones are being added with smart card reader. Precise Biometrics announced that its smart card reader T active has been approved for usage with Swedish national healthcare system Pascal, a mobile prescription solution for dose packaged medicals used by nurses, doctors and midwives.

5. CONCLUSION

With the help of biometric systems are private information stored on mobile phone are getting secured in a more convenient manner. They are also adding security to remote transactions those are started using a phone. Face recognition, voice recognition signature recognition or keystroke recognition are biometric security systems that can be added implemented on most of the mobile phones because they don't require any additional hardware.

Biometric security systems for cell phone are not only making cell phones more secure but they are also being making cell phones use easier and even more entertaining. It stops people from getting into the data when they physically have possession of the phone. But there is a concern about hacking of device for data. This will need more research to figure out how to deal with hackers when the device is with the owner physically. Biometrics simply makes the physical phone more secure.

REFERENCES

[1] Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. on Circuits and Systems for Video Technology 14 (2004)
[2] Lawrence O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," in Proc. IEEE, vol. 91, No. 12, December, 2003
[3] http://www.biometricupdate.com/tag/ mobile-phones(online)
[4] A. K. Jain, P. Flynn, A. ROSS, Handbookof Biometrics, Springer, USA, 2008.
[5] A. K. Jain, A. Ross, S. Prabhakar, "An introductionto biometric recognition",IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No.1, pp. 4-20, January 2004.
[6] K. Revett, PhD, Behavioral Biometric A Remote Access Approach, Wiley, UK, 2008.
[7] S. Holtmanns, V. Niemi, P. Ginzboorg, P.Laitinen, N. Asokan, Cellular Authenticationfor Mobile and Internet Services,Wiley, UK, 2008.
[8] Motorola DynaTAC 8000X – World's First Mobile Phone [Online]. Available: http://www.tech-fresh.net/motoroladynatac-8000x-worlds-first-mobile-phone
[9] Nokia USA – Nokia 2135 [Online]. Available: http://www.nokiausa.com/link?cid=PLAIN_TEXT_842095
[10] Nokia USA – Nokia 9300 Smartphone – Phones [Online]. Available: http://nokia usa.com/find-products/phones/nokia- 9300-smartphone
[11] HTC – Products –HTC Touch Diamond2[Online]. Available:http://www.htc.com/www/product/touchdiamond2/overview.html
[12] Apple–iPhone – Gallery [Online]. Available:http://www.apple.com/iphone/ gallery/#image3
[13] M. Sauter, Beyond 3G – Bringing Networks,Terminals and the Web Together,Wiley, UK, 2009.
[14] www.ccure.org(online)
[15] yoursecurity.com(online)
[16] Technology News – PCWorld's Technologynews and Reviews [Online].Available: http://pcworld.about.com/ news/Mar0120 05id119850.htm
[17] Emerging Biometric Technologies – Crime, Law Enforcements and Corrections [Online]. Available: http://www.all business.com/crime-law/law-biometricsfingerprinting/1054 6671-1.html