International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 04 - Issue 06 || June 2019 || PP. 132-137

Analysis of Biometric Systems in Mobile devices

Ms. Aakanksha Chopra
(Information Technology, Jagan Institute of Management Studies (JIMS), Rohini, Sec-5, New Delhi, India)

Abstract: Authentication techniques and biometric systems have occupied a major industrial area today. People have moved from big devices to small portable devices like mobile phones. Ample amount of systems requires relaibility as an important factor as they want that the access should be given only to the genuine users. Technology revolution has bought biometric systems to become more secure and highly user friendly. This paper is highlighting on various biometric technology available and their comparative analysis, strength, and related privacy issues with biometric system.

Keywords: Behavioral biometrics, Biometric systems, errors, identification, privacy, verification.

1. INTRODUCTION

Mid-19th century was an era that criminals were identified using their unique identity of face, fingerprinting, body marks, voice, color of eyes etc. this concept is termed as biological identification. These systems were used to identify for e.g. security clearance for employees for sensitive jobs, and positive identification of convicts and prisoners), later as medical field developed we moved towards DNA test forensics and other scanning mechanisms. If we look at the graph of human growth the standard of living and the basic utilities has changed tremendously. Currently, biometric systems are used for identification purposes. We are today living in 4th Industrial revolution world were technologies are changing their directions. Existing technologies are getting reinvented or rediscovered in this generation. We have heard about Windows, MAC, LINUX Operating systems and their upgraded versions. Software, Hardware, Memory, Storage Capacity everything had eventually evolved. 21st century is the century of Mobile devices. Like the operating system of desktops emerged; similarly it is emerging in Mobile devices.

Modern consumer of mobile devices are provided with large amount of multimedia applications and services over different utility networks hence this has led to monstrous hike in sale of mobile devices to extend that consumer are using two SIM cards or two mobile phones. Mobile devices which are best portable storage device with large amount of memory are not only used for communication but also for saving hypersensitive data and credential information like- username, password, personal details, bank details, and such information can be misused when mobile device gets stolen or lost [5]. Many researchers are testing amenabilities of mobiles by saving essential data in it. Therefore, any squandering of crucial information saved upon the mobile is a threat to its owner when the device is lost, spoiled by malware or invaded by social engineering [3].

The concern is that all the applications and or services provided by these applications are eminently galvanized by important user information, which is always progressively hypersensitive in nature. The major concern is this that people have humongous data available, which is both professional and private accessed from these mobile phones. Breach which used to take place from telephones, desktops, servers, are now happening from mobile phones also. Intrusion is the new trend in the market. Hacking someone's data today has become ethical today. We need a strong system where all these factors should be taken care of. Authentication is one crucial fundamental today. For any small access we need authentication; like withdrawing cash from ATM, transferring money online, unlocking mobile systems, accessing own email accounts etc. authentication is important. Authentication techniques have expanded so much because of increase in information.

Major hindrance of mobiles devices is the design of its authentication techniques. These devices confidently depend upon token based and alphanumeric password techniques like- PIN number, pattern lock, text passwords as a form of user authentication, and the loopholes of point- to- entry techniques is widely documented. Hefty number of devices currently requires explicit identification for an individual user to use various services because of booming security concerns. Biometric Authentication techniques are accessed for user identification to solve this issue [3].

1.1 Biometric Systems

A biometric system is a step by step process of *acquiring, extraction, pattern recognition, comparison, and authentication.* Biometric systems first acquire biometric form of data from the respective user, after acquiring the data a feature set is extracted from it. Next state is comparison; it compares extracted feature set of data entered at the time of *Login phase* with the data already pre-saved in the database at the time of

Registration phase. If after Comparison state the biometrics matches the Authentication is granted to the user, else it is not granted.

Depending on the application context, a biometric system may operate either in *Verification* mode and *Identification* mode [2]-

• **Verification mode-** the system ratifies user's identity by comparing data entered with pre- saved data in database. The system in such mode performs one –to –one comparison to determine whether the request for access by the user is correct or not. In this user enter personal information like- PIN, username, or smart card. Identity verification is generally used for *positive recognition*, where the motive is to protect multiple users from using the identical identity.

• **Identification mode-** the system ratifies user's identity by searching the pre-saved templates of all the users in the database for a match. The system in this mode performs one-to-many comparison to determine a single identity (or fails if the user is not enrolled in the system database) without the subject having to claim an identity (e.g., "*this biometric data belong to whom?*"). This is a negative recognition in which personal information can only be established through biometrics. Identification is a crucial element in *negative recognition* applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities [2].

Biometric systems since long are already active in regions or areas that need some type of user verification. It is basically accepted that physical traits like iris, fingerprints and, hand shape and palm- prints can uniquely exemplifies each user of a large populace. Contrary to this on the other hand, in many small-populace applications, due of privacy or confined resources, we only need verification mode to verify the user (accept or reject users claimed identity). In these situations, one can also use behavioral traits which have less discriminating power such as voice, face, iris, retina, signature and human–computer interaction (HCI) derived patterns [1].

Other authentication schemes like knowledge based and token based approaches are also used on quite a good scale. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones, and ATMs. These systems are open to vulnerability in the absence of powerful personal recognition schemes. Biometric recognition is defined as an automatic recognition system of individual based on their physiological and/or behavioral characteristics [2]. Usage of biometrics specifically confirms and authorizes individual access into the system based on its unique integrity. It only covers factor of who user is rather than what user contains (PIN, Password, Card etc.)

Although biometrics developed from its extensive use in law enforcement to identify criminals but today, it is vastly used to establish person recognition in an extensive number of mobile applications. Any users physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the factors mentioned in TABLE 1.

Table 1: Characteristic features required for users in biometric systems

Universal	Every user should have characteristic, which is universally accessible.
Unique	No two users should have same characteristics
Invariant/Static	User identification cannot change over a period of time, example fingerprinting, palm print gets change with age.
Quantity	The characteristic should be measurable quantity wise.

In biometric systems with personal user identification or recognition there are other factors which should be kept into consideration. These factors are mentioned in TABLE 2

Table 2: Characteristic features required for users in biometric systems

Operational performance	Devices should be able to accurately in due timespan with due speed be able to operate properly.
Adaptability	Users should be able to adapt the system in their daily routine.
Bypass hoax	System should be powerful enough to avoid all hoax methods. All biometric system should practically meet the specified recognition methods, efficiency, speed, and resources required, be harmless to the users, be accepted by the users

This paper is a review paper about biometric authentication technology. Section II will be elaborating on various categories of biometric systems, describing how biometric system has bolstered widely from the past. It will be giving an insight about advantages and disadvantages of various biometric systems. Section III will be explaining about errors or privacy issues any user can face in biometric system. Section IV is describing various advantages and disadvantages of biometric systems.

2. CATEGORIES OF BIOMETRIC SYSTEMS

Biometric systems have actually provided a unique personal identification, validation, verification and authentication technique. This technique is highly reliable in terms of user's identity which wants to use it for identity. There are many biometric systems available today. They can be categorized as Contact biometric and Contact less Biometric systems. The contact biometric systems are those in which user need to contact directly with the system like- fingerprinting, palm or hand geometry, keystroke dynamics etc. on the other hand contact less biometric systems are those in which user do not directly interact with the system, in this only the body part of the user interacts with the system like- iris scan, retinal scan, voice recognition etc.

Sometimes the biometric systems are also differentiated by physiological type or behavior type biometrics. The techniques which fall under physiological system deals with statistical characteristics of person, rather than emotional factors like- Fingerprints, Face Recognition, DNA, Palmprint, Hand Geometry, Iris Recognition. Behavior Type of Biometrics system are methods of identification which pay attention towards the actions of a user, giving the user an opportunity to control his actions, it considers high level of inner variants- mood, health condition, etc., hence these methods are useful only in constant use like- voice, gait, typing rhythm. Because of the ability to change during the time period, such characteristics should be renewed constantly. Behaviour characteristics are influenced by controlled actions and less controlled psychological factors. As behaviour characteristics can be changed in time, registered biometric sample should be renewing every time of use [4].

Following is the list of various biometric systems with their working-

2.1 Typing Rhythm: they are also known as "Biometric keystroke recognition" – typing rhythm is a technology of identifying users from the way they are typing. To understand more we should know that this technique does not depend on what is written and how is it written. It is directly related to the speed of typing of an individual.

2.2 Gait: it states that every person has a different way of walking. This method records way an individual user walks. Although gait is not affected by the speed of the user's walk.

2.3 Voice: Voice is a combination of physiological and behavioral biometrics. The uniqueness of the voice is accomplished because of different physical components of a human throat and mouth. To produce a sound, air leaves the body of a human being through resonators: larynx, the oral cavity (mouth), nasal cavity (nose) [4]. These physiological characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions (such as a common cold), and emotional state, etc. Voice is also not very specific and may not be appropriate for large-scale identification. [2]

2.4 Hand, finger geometry and palm geometry: Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers. The technique is very smooth, relatively easy to use, and economical [2]. Hand shape biometrics are easy to use, non-intrusive and have public acceptance hence widely used [1]. In the **palm geometry** it states that each person consists of some principle lines, wrinkles, secondary lines and ridges. The main feature for this method are calculating and recording the height, length of the fingers, distance between joints, shape of the knuckles, outer area of the hand [4]. Major drawback of this method is that the shape, size, principle lines of each hand changes with age. Although hand of one user differ from another but it is not unique.

2.5 Face recognition: is a nonintrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The face of a person has a numerous distinguishable characteristics, and is measure on distinctive factors like- distance between eyes, width of the nose, depth of the eye sockets, shape of the cheekbones, length of the jaw line, nose, eyebrows, lips size, chin [2,4].

2.6 Fingerprint: is the pattern of shape an length of fingertip and ridges. No two finger of a user is same; also fingerprints of identical twins are also different from each other. Fingerprint identification is also known as

dactyloskopy or also hand identification is the process of comparing two examples of friction ridge skin impression from human fingers, palm or toes [4]. This technique today is highly used in android and iOS mobiles.

2.7 Iris scan: The complicated iris texture carries very distinctive information useful for personal recognition. Every user has a unique shape and size of iris. The accuracy and speed of currently deployed iris-based recognition systems is promising and point to the feasibility of usage in large organizations [2].

2.8 Retinal scan: The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most sensitive and highly secure biometric since it is not easy to modify or replicate the retinal vasculature. This is most used technique today in which the image is captured and requires a user to peep into an eye-piece and concentrate on a specific spot in the visual field to capture retinal vasculature.

3. ERRORS IN BIOMETRIC SYSTEMS

We have discussed above that any biometric system can either operate on *verification mode, or validation mode.* Any biometric Verification mode system has two common types of errors-

a. **FALSE MATCHING-** considering biometric dimensions from two distinct users to be from the one user only.
b. **FALSE NONMATCHING-** considering biometric dimension of single user to be from two distinctive users.

False matching and False Nonmatching errors are often termed as *false accept* and *false reject* respectively [2].

Sometimes in fingerprinting systems two piece of sampling of same biometric feature from the same user (e.g., two impressions of a user's right index finger) are not exactly duplicate due to inexact imaging quality. This may happen due to extra dry or wet fingers or sensor noise, changes in the user's physiological or behavioral characteristics like- cuts and wounds on the finger and climatic conditions like- temperature and humidity, and user's interaction with the sensor device like- placement of finger.

In biometric systems taking iris or retinal scan if a user is wearing lens or undergoes cataract surgery or if a user hurts his/her eye the user will not get access to the system. Hence, the feedback from a biometric matching system is the identical score S(Y, Z) (typically a single number) that assess the correlation between the input (Y) and the pre-saved database (Z) representations. The higher the score, the more certain is the system that the two biometric dimensions come from the same user.

4. ADVANTAGES OF BIOMETRIC SYSTEM

4.1 In Conventional authentication methods like: token based and knowledge based set their passwords which are easy to remember and are generally repeated, such as- same passwords as usernames, birthdate, music stars, and dictionary words. Though it has already been advised and proven to better be safe by keeping different and difficult passwords or PIN number, but users never change it [6]. If a single password is exposed, it may result in a breach in security in many other applications also. Hence, an intruder needs to breach only one password among all the employees to steal access to a company's Intranet and hence, a single weak password impacts negatively on overall company [8]. Biometrics introduces incredible convenience for the users (as users are no longer required to remember multiple, long and complex frequently changing passwords) while maintaining a sufficiently high degree of security [2].

4.2 Longer passwords are highly secure but difficult to recall which results in some users to write them down in accessible locations e.g.- on mobile phone notes, on mails, in phone directories or and hide it under the keyboard. Strong passwords are difficult to remember resulting in forgotten or expired passwords. Cryptographic techniques such as encryption as defeats badly in password key as they keep passwords, which are further stored with simple text (again risky), hence, chances of attacks are high in these systems. Whereas, in biometric system tendency of brute force attack is very low.

4.3 The fundamental drawback of the PIN-based approach is that as a point-of-entry technique, it does not validate the user's unique identity on accessing it again. Rather in biometric systems no matter how many number of times user try to enter into system it is always validated [3].

4.4 Copying, sharing and circulating biometrics with as much ease as passwords and tokens is not possible, it is almost impossible.

4.5 Biometric systems cannot be lost or forgotten and online biometrics- based recognition systems require the person to be recognized to be present at the point of recognition.

4.6 It is difficult to forge biometrics and extremely unlikely for a user to repudiate, for example, having accessed a computer network.

4.7 Further, all the users of the system have relatively equal security level and one account is no easier to break than any other (e.g., through social engineering methods).

Situations like- Noise in sensed data, Intra-class variations, Distinctiveness, Non- universality, Spoof attacks are supposed to be taken care of. A standalone biometric security is unreliable because of device vulnerabilities [5].

5. CONCLUSION

The traditional knowledge-based and token-based methods do not prove any personal identity of user. Hence, it is mandatory that any system which requires unique identity of user they should involve Biometric system. Threat security and cost-benefit are two important factors which are required for higher level of security systems. It is thus concluded that implementing biometric systems sincerely are effective hindrance to intruders. Biometrics provides tools to enforce responsible chunk of system transactions and to prevent an individual's right to confidentiality. As biometric technology expands and grows, there will be a rising interaction among the market, technology, and the applications. But, still there are a number of privacy concerns issues about the use of biometrics like- Noise in sensed data, Intra-class variations, Distinctiveness, Non- universality, Spoof attacks that are supposed to be taken care of. Therefore, it is certain that biometric-based recognition will have a profound influence on the way we conduct our daily business.

REFERENCES

[1]. N. Duta, A survey of biometric technology based on hand shape, *Pattern Recognition, Elsevier, 2009*, Pattern Recognition *42 (2009) 2797 – 2806, available at: www.elsevier.com/locate/pr, doi:10.1016/j.patcog.2009.02.007, 2797- 2806.*

[2]. A. K. Jain, A. Ross, and S. Prabhakar, An Introduction to Biometric Recognition, *Transactions On Circuits And Systems For Video Technology, IEEE, vol. 14, no. 1, Jan 2004.*

[3]. F. Li, N. Clarke, M. Papadaki and P. Dowland, Active authentication for mobile devices utilising behaviour profiling, *International Journal of Information Security***,** *Springer, June 2014, published online Sept 2013, ISSN 1615-5262, vol. 13, Number 3, Int. J. Inf. Secur. (2014) 13:229-244, doi: 10.1007/s10207-013-0209-6, 229-244.*

[4]. A. Babich, *Biometric Authentication. Types of biometric identifiers, Hagga- Helia, Univeristy of Applied Sciences, Finland,* 2012.

[5]. P. P. Kuriakose, Ambili K, Secured Android Application Using Biometric Authentication, *International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization), available at:: www.ijircce.com, Vol. 5, Issue 4, April 2017, ISSN(Online): 2320-9801 ISSN (Print): 2320-9798, 7716- 7719.*

[6]. D. Impedovo and G. Pirlo, Automatic Signature Verification: The State of the Art, *IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, VOL. 38, NO. 5, SEPTEMBER 2008 609,* doi: 10.1109/TSMCC.2008.923866, 609-635.

[7]. N.L. Clarke, S.M. Furnell and P.L. Reynolds, Biometric Authentication for Mobile Devices, *3rd Australian Information Warfare and Security Conf. 2002, 61-69.*

[8]. A. Morales, M. A. Ferrer, F. Díaz, J. B. Alonso, and C. M. Travieso, Contact-Free Hand Biometric System For Real Environments, *16th European Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland, August 25-29, 2008.*

[9]. S. Sayeed, R. Besar, N. S. Kamel, Dynamic Signature Verification Using Sensor Based Data Glove, *ICSP2006 Proceedings,0-7803-9737-1/06/$20.00, 2006 IEEE.*

[10]. R. A. Patil and A. L. Renke, Keystroke Dynamics for User Authentication and Identification by using Typing Rhythm, *International Journal of Computer Applications (0975 – 8887) Volume 144 – No.9, June 2016* 27, *available at: www.ijcaonline.org, 27-33.*

[11]. A. Sierra, C. S. vila, G. B. Pozo and J. Casanova, Unconstrained and Contactless Hand Geometry Biometrics, *Sensors 2011, 11, ISSN 1424-8220, available at: www.mdpi.com/journal/sensors, doi:10.3390/s111110143, 10143-10164.*

[12]. A. N. Kataria, D. Adhyaru, A. K. Sharma and T.H. Zaveri, A survey of automated biometric authentication techniques, *International Conference on Engineering (NUiCONE) IEEE Proc., Nirma University, 2013, 1-6.*

[13]. W. Meng, D. S. Wong, S. Furnell, J. Zhou, Surveying the Development of Biometric User Authentication on Mobile Phones, *Communications Surveys & Tutorials, IEEE 2014,1268 – 1293*.

[14]. Ankur, Divyanjali, Bhardwaj, A dissection of pseudorandom number generators, *IEEE Proc. Of 2nd International Conference on Signal Processing and Integrated Networks (SPIN), 2015, 318 –323.*

[15]. Z. Tu, Y. Yuan, Understanding User's Behaviors in Coping with Security Threat of Mobile Devices Loss and Theft, *IEEE Proc. of 45th Hawaii International Conference on System Sciences (HICSS), 2012, 1393 – 1402.*

[16]. R. Schwamm, N. C. Rowe, Effects of the factory reset on mobile devices, *The Journal of Digital Forensics, Security and Law (JDFSL), VOL 9, NO 2, 2014, 205-220.*

[17]. S. Nseir, N. Hirzallah, M. Aqel, Issues with Various Security Threats on Mobile Phones, *IEEE Proc. of Information and Communication Technology (PICICT), 2013, 37 – 42*.

[18]. Khan, Qureshi, Qadeer, Anti-theft application for android based devices, *IEEE Proc. of Advance Computing Conference (IACC), 2014, 365 – 369.*

[19]. Yamazaki, D. Li, Isshiki, Kunieda, SIFT-based algorithm for fingerprint authentication on smartphone, *IEEE Proc. of Information and Communication Technology for Embedded Systems (ICICTES), 2015, 1 – 5.*