IRIS, A SUITABLE SECURITY MEASURE IN MOBILE

Sr. Sagaya Mary James

Assistant Professor, Department of Computer Science
St. Joseph's College of Arts and Science for Women, Hosur, Tamilnadu, (India)

ABSTRACT

In today's fast moving world, mobile phones have become one of the basic needs and mobile security is of a major concern. Security risks and data breaches are growing while the form factors of computing devices shrink—because much enterprise data today is created and consumed on mobile devices. This clearly explains why mobile security persistently tops the list of most pressing enterprise security concerns. Mobile security also refers to the means by which a mobile device can authenticate users and protect or restrict access to data stored on the device through the use of passwords, personal identification numbers (PINs), pattern screen locks. These methods are highly vulnerable to spoof attacks. To avoid these attacks biometric based authentications are introduced. Among all biometric modalities, Iris is proven to be one of the best traits. In this paper, I propose the types of biometrics and how iris is chosen to be a suitable one in mobile security.

Keywords: Biometrics, Fingerprint, Iris Nodes, Ridges

I. INTRODUCTION

Biometrics consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. Currently biometrics is one of the biggest tendencies in human identification. Biometrics is claimed to be better than current and established authentication methods, Personal Identification Number(PIN), Password, Smart card. Key advantages of using a biometric feature are: availability (always), uniqueness (to each person), not transferable (to other parties), not forgettable, not subject to theft, not guessable.

II.BIOMETRICS IN MOBILE SECURITY

Since the smart phones have the higher feature called portability, the present scenario mostly depends on mobile than other devices called computer. We have so much more data on our phones than we had on our computers five years ago. Now a days smart phone are used for account transactions, mailing, storing secret data etc. Traditional way of security leads to various attacks. It is clear that the username-password system for logging in and out of things is ultimately doomed. It just doesn't work anymore. The only logical alternative is biometrics. The iPhone 5S and the Galaxy S5 already both have fingerprint readers. Eventually, this technology will become cheap enough to be on every phone.[2]

Figure 1: Statistics of smart phone users

Fig.1 shows the statistics of smart phone users all over the world. Based on this statistics smart phone users are increased in foreign countries and it is increasing in India. Security to smart phone is also essential.

III. BIOMETRICS SECURITY VERSUS OTHER SECURITY

Three factors can be used for security: something you know (password or PIN), something you have (smart token or access card), and something you are (biometric). Biometrics can be used alone or in conjunction with one of the other factors to strengthen the security check. Biometric technology has advantages over both of the other factors in that the user does not need to remember anything or possess a physical token in order to be identified. Tokens and cards can be lost, and passwords and PINs can be forgotten or compromised. A biometric is only susceptible to forgery, which can be extremely difficult, depending on the biometric.

IV. TYPES OF BIOMETRICS IN MOBILE SECURITY

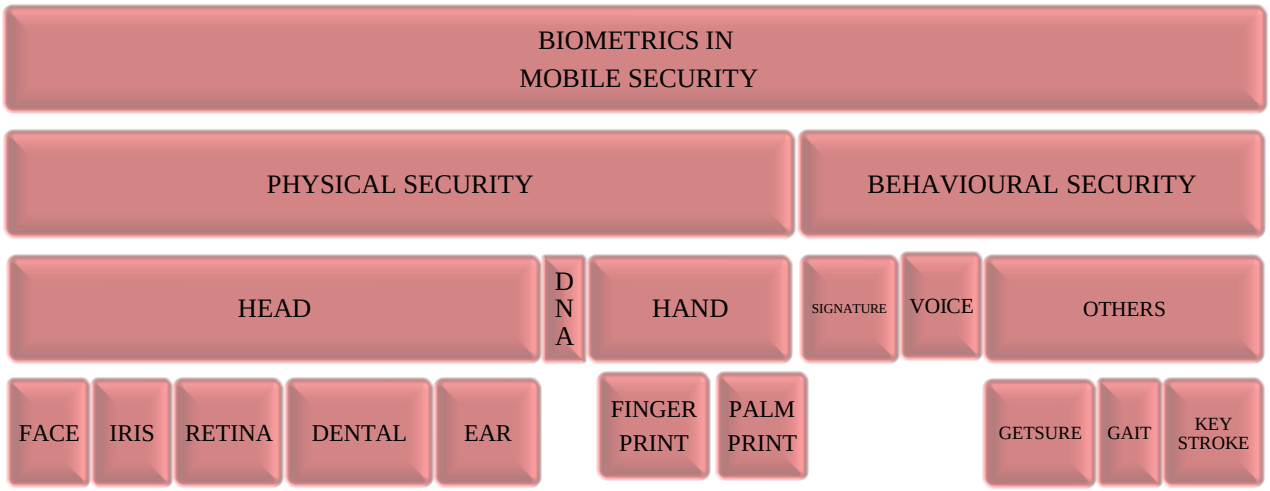

Figure 2: Types of biometrics

4.1 Physical Security

Biometrics based on physical traits of an individual is known as physical biometrics. Examples of physical biometrics include head, hand, DNA etc. The physiological biometrics is also called as static. Biometrics based on data derived from the measurement of a part of a person's anatomy is known as physical security.

4.2 Behavioral Security

Biometrics based on data derived from measurement of an action performed by a person and, distinctively, incorporating time as a metric, that is, the measured action is known as behavioral security.

4.3Comparison between Physical and Behavioral Biometrics

Biometrics Characteristic	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Face	H	L	M	H	L	H	H
Finger print	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	L
Digital Signatre	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Table 1: Characteristics of physical and behavioral biometrics

Note: [H=High,M=Medium,L=Low]

Universality: Each person should have the biometric characteristic.

Distinctiveness: Any two persons are not equal in terms of the characteristic.

Permanence: The characteristic remains the same over time or has not abrupt changes.

Collectability: The characteristic should be able to be measured quantitatively.

Performance: The achievable recognition accuracy and speed that the biometrics system can achieve.

Acceptability: The acceptance of the end-users in using the biometric system in their daily lives.

Circumvention: The degree of security of the system given fraudulent attacks.

Biometric Technology	Accuracy	Cost	Devices Required	Social Acceptability
DNA	High	High	Test Equipment	Low
Face	Medium-Low	Medium	Camera	High
Fingerprint	High	Medium	Scanner	Medium
Iris	High	High	Camera	Medium
Signature	Low	Medium	Optical pen, Touch panel	High
Voice	Medium	Medium	Microphone, Telephone	High

Table 2: Comparison of physical and behavioral biometrics

TABLE 1&2 explains that the physical biometrics is more suitable than behavioral.

PHYSICAL	BEHAVIORAL
Static	Dynamic

One more major difference between these two is Static like face, iris does not change in nature, but Dynamic like voice, signature may change. This major concern shows that physical biometrics give more security than behavioral.

V. PHYSICAL BIOMETRICS

5.1.1 DNA

Figure 3: Structure of DNA

Due to recent improvements in laboratory analysis and reduction in costs, many agencies are relying on deoxyribonucleic acid (DNA) as a form of identification.DNA is a chemical structure that forms chromosomes. A gene is piece of a chromosome that dictates a particular trait. That chemical structure can be identified through

laboratory analysis. DNA does not change over times, however, two people can have the same DNA (Identical twins) DNA identification processes require a lengthy time period. In addition, some consider DNA collection to be personally invasive.

5.1.2 Why DNA Is Not Applicable In Mobile Security

- DNA can be collected from any number of sources: blood, hair, finger nails, mouth swabs, blood stains, saliva, straws, and any number of other sources that has been attached to the body at some time. These sources are not used very often for giving security in mobile.
- Identification process takes lengthy of time.
- It can be identical for twins.
- It is extremely intrusive and expensive.

5.2 Face

A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. It is typically used in security systems. Face recognition can be considered to be same as photograph recognition. Most current facial recognition systems work with numeric codes called face prints. Such systems identify 80 nodal points on a human face. In this context, nodal points are end points used to measure variables of a person's face, such as the length or width of the nose, the depth of the eye sockets and the shape of the cheekbones. These systems work by capturing data for nodal points on a digital image of an individual's face and storing the resulting data as a face print. The face print can be used as a basis for comparison with data captured from faces in an image or video. [1]

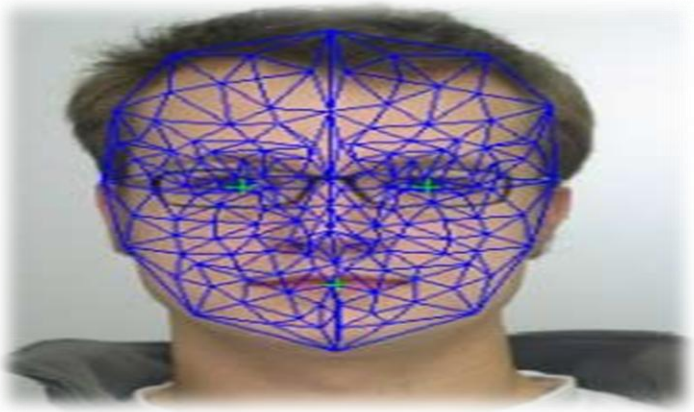

Figure 4: Nodes in Face

5.2.1 Face Recognition in Mobile Security

Figure 5: Face Recognition in mobile security

Facial recognition is a high-tech security feature available on smart phones . One example of such is the **Samsung GalaxyS®4**, which uses 2-D facial recognition technology. Essentially, these devices can be trained to recognize your face and unlock every time it sees it.Facial recognition software views the face as a map of sorts. It notes particular "landmarks" on the face, such as the distance between the eyes, nose width, eye socket depth, cheekbone shape and jawline length. The S 4 converts these measurements into a numerical code, much like fingerprint scanners do. This numerical code then represents the saved "map" of your face, which the phone uses for comparison when you try to unlock it.

5.2.2 Face Recognition Exists But With Serious Flaws in Mobile Security

- Face of the person changes over the time, unlike fingerprint which remains same throughout the life span of a person.
- It is less effective if facial expressions vary. Even a big smile can render the system less effective.
- The algorithm does not work well when the lighting changes.
- Isn't always accurate and can be hindered by glasses, masks, long hair etc.
- Must ask users to have a neutral face when pictures are being taken
- Considered an invasion of privacy to be watched

5.3 Fingerprint

Fingerprint identification, known as dactyloscopy ,or hand print identification, is the process of comparing two instances of friction ridge skin impressions, from human fingers or toes, to determine whether these impressions could have come from the same individual. The flexibility of friction ridge skin means that no two fingers are ever exactly alike in every detail; even two impressions recorded immediately after each other from the same hand may be slightly different. [4]

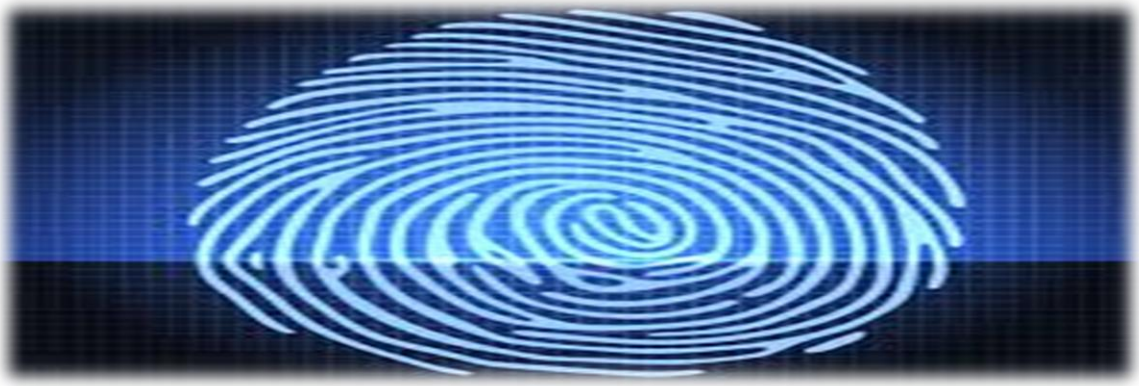

Figure 6: FingerPrint

5.3.1 Fingerprint in Mobile Security

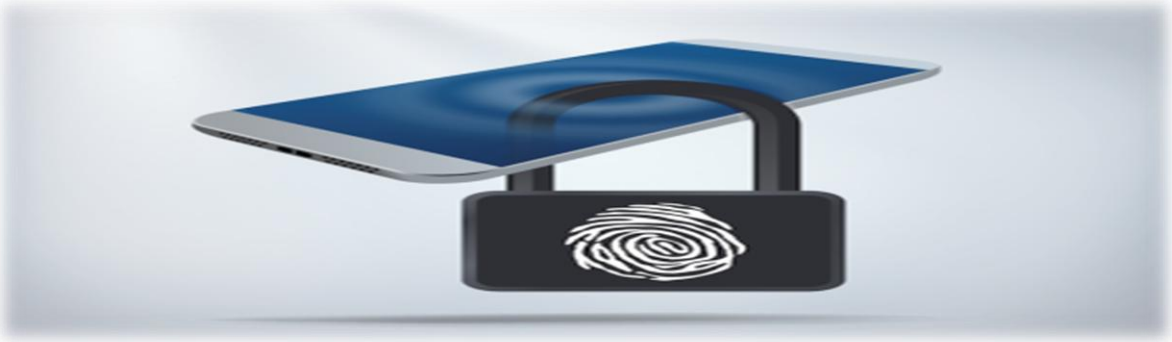

Figure 7: Fingerprint Recognition in Mobile Security

Fingerprint recognition technology for mobile devices is posed to become the preferred user authentication solution mobile device security. First, the fingerprint scanner captures an image of the ridges-and-valleys pattern on your fingertip. The scanner saves the fingerprint's unique characteristics as an encrypted biometric key, or mathematical representation in binary code. This code is then saved and used for future comparisons every time you unlock your phone. When you swipe your finger, the scanner must assess the ridges and valleys in the new image and create a binary code, and then match the new code with that of the stored code.[3]

After setting up your HTC One® (M8) to recognize your fingerprint, simply swiping the correct finger across the scanner unlocks your Smartphone and grants access to all of the great features it has to offer. Also, you can program your Smartphone to recognize up to three distinct fingerprints and assign each a specific function, like launching your camera or accessing select apps that you use more than others. [5]

5.3.2 Flaws of Fingerprint In Mobile Security

- Fingerprints may be distorted and unreadable or unidentifiable if the person's fingertip has dirt on it, or if the finger is twisted during the process of fingerprinting.

- Although fingerprints do not naturally change over the course of a person's lifetime, it is possible for fingerprints to become damaged to the point where they are not useful for identification. Injuries, trauma, burns or deliberate injury to the fingertips can all cause a person's fingerprints to become different, unreadable or even eliminated.
- Lower cost system may incorrectly identify unauthorized person.[3]

5.4 Iris

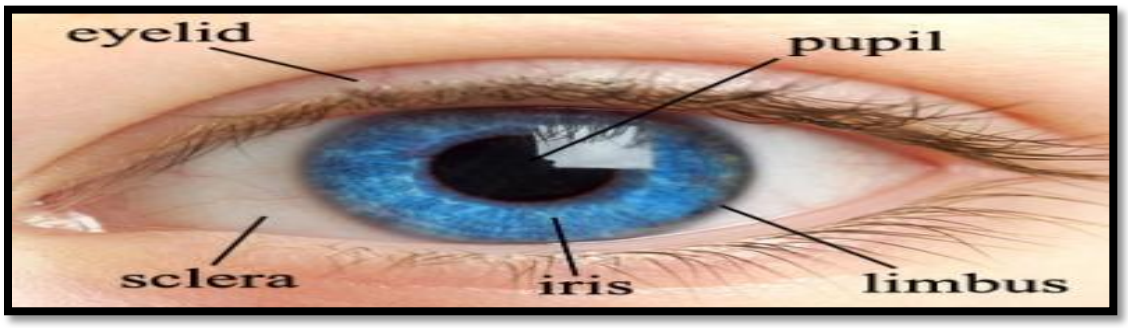

Figure 8: Structure of Iris

The iris is the colored part of the eye that lies behind the cornea, in front of the lens, and is protected by the eyelid. John Daughman points out that the iris is the only internal organ of the human body that is normally externally visible. Color is not used in iris recognition technology. Instead, the other visible features such as the connective tissue, cilia, contraction furrows, crypts, rings and corona distinguish one iris from another.By the time a human is about eight months old, the iris' structures are complete, and they do not change in later life. No two irises are alike, even if they are from identical twins or the left and right eye in the same person.

5.4.1 Comparison of Iris and Face

- During fetal development, the eye goes through a process called chaotic morphogenesis that gives each iris its unique appearance.
- Iris recognition systems are extremely accurate; they're 100,000 times less likely to produce a false match than facial recognition systems.
- The matching process is very fast when it is compared with face.
- The eye doesn't change much with age

5.4.2 Comparison of Iris and Fingerprint

- Both biometric technologies are reliable and very accurate, but iris recognition has a much lower error rate (1 in 131,000) than fingerprinting (1 in 500+).
- Forgery can be possible in fingerprints than iris.
- Since older people tend to have drier skin, fingerprints can be more difficult to verify as a person ages.

- Fingerprinting hardware is generally less expensive than that for iris recognition, but recent technology is lowering costs of iris recognition devices.
- Both technologies are reasonably well accepted by the user population, but fingerprinting was rated more intrusive than iris scanning.
- There are some health related advantages of iris recognition over fingerprinting. It requires physically touching a device each time the finger is presented for verification. In contrast, the iris template is created without any physical contact with the person whose iris is encoded. The iris recognition process is, therefore, more appealing to those concerned with hygiene than is fingerprinting.
- Forgery is not as much of a risk with iris recognition as with fingerprinting. Although
  Sophisticated fingerprinting technology is designed to detect false fingers, a person's finger can be cut off or used for a mold much easier than an eyeball could be extracted and used for impersonation. In fact, the iris from a person's extracted eye would not be usable for more than a few seconds. Iris recognition devices can also detect the dilating pupil to ensure that the eye is live.
- Cuts, scars or bruises alter the fingerprints which negatively affects performance of fingerprint.[7]

5.4.3 Iris Is Best For Mobile Phone Security

Figure 9: Iris in mobile Security

Iris recognition systems encode the entire eye structure, following an open standard. And because the process doesn't focus on detailed feature points, a gray-scale 640-x-480-pixel image is sufficient. That's one reason why the recognition algorithms can speedily process data and respond quickly. One more major advantage of iris is that the blind's iris is also recognized as like normal people. Iris recognition is less intrusive. It's also less prone to changes due to disease, because a person's iris generally stays the same for their entire life, except in cases of extreme injury to the eye. The iris, as a protected, unchanging, yet completely unique feature of the human body, is often seen as the best chance we have of ever perfectly identifying people.[8] It is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane (the cornea). This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labour. The iris is mostly flat, and its geometric configuration is only controlled by two complementary muscles (the sphincter pupillae and dilator pupillae) that control the diameter of the pupil. This makes the iris shape far more predictable than, for instance, that of the face. The iris has a fine texture that—like fingerprints—is determined randomly during embryonic gestation.[6]

VI. CONCLUSION

Iris recognition gets more and more attention for its high accuracy rate. However, the iris images are often occluded by eyelids and eyelashes partly and if theses noises can't be removed the performance of iris recognition system will be regarded badly. With the increasing need of guaranteeing the security in case of using bank transaction service by using cellular phone, it is required to apply biometrics for the security of cellular phone. Especially, iris recognition is good for security because of its reliability and accuracy compared to other biometrics such as fingerprint and voice recognition.

VII. ACKNOWLEDGEMENT

With sincerely gratitude and indebtedness I thank GOD the almighty for all the graces and blessings showered upon me throughout my life and this work in particular. I sincerely thank our Mother Mary for her powerful intercession. I am so much delighted to acknowledge our Mother General, Provincial and Superior for their encouragement and all the sisters of presentation congregation for their support. I am so grateful and appreciative of all those who have helped and supported me in this endeavor.

REFERENCES

[1] http://whatis.techtarget.com/definition/facial-recognition
[2] http://www.sans.org/reading-room/whitepapers/physical/physical-security-biometric-approach-1325
[3] http://www.verizonwireless.com/mobile-living/tech-smarts/how-does-fingerprint-scanning-facial- recognition-work-technology
[4] http://en.wikipedia.org/wiki/Fingerprint
[5] http://searchmobilecomputing.techtarget.com/Fingerprint-recognition-and-mobile-security
[6]http://www.computerworld.com/article/2484968/security0/forget-fingerprints--your-iris-is-your-new-identity.html?page=3
[7] http://www.sans.org/reading room/whitepapers/authentication/dont-blink-iris-recognition-biometric-identification-1341
[8] Article "Forget fingerprints: Your iris is your new identity" by Robert L.mitchell Sep 30, 2013

AUTHORS BIOGRAPHY

Sr.Sagaya Mary James was born in Sathyamangalam, TamilNadu, India, in 1979.She received her Master in Science (M.Sc)in Information science and management at Bharathiar University,Coimbatore,TN,India and Master of Business Administration at Alagappa University and M.Phil at Bharathiar University and also She has completed B.Ed in Tamilnadu Education University, Chennai. At Present she is working in St.Joseph's College,Hosur as Asst., Professor.