ISSN 2250-3153

Biometrics in IRIS Technology: A Survey

Prof. Chandrakant D. Patel, Prof. Sanket Trivedi, Prof. Sanjay Patel

Abstract- In olden days people were identified by physical characteristics such as birthmarks and scans, which was biometrics then. Today we have devices that do similar jobs and more accurately. Modern era is full of advantages and culprits who tamper with these advantages .In this we try to present a way to deal with these people at large. Biometric systems fall into two categories:

- Authentication
- Identification.

To be authenticated by a system, a subject presents a password or a token such as an ID card along with a live biometric sample such as fingerprint or iris. Airports, prisons, and companies that need secure access use these biometric systems [1].

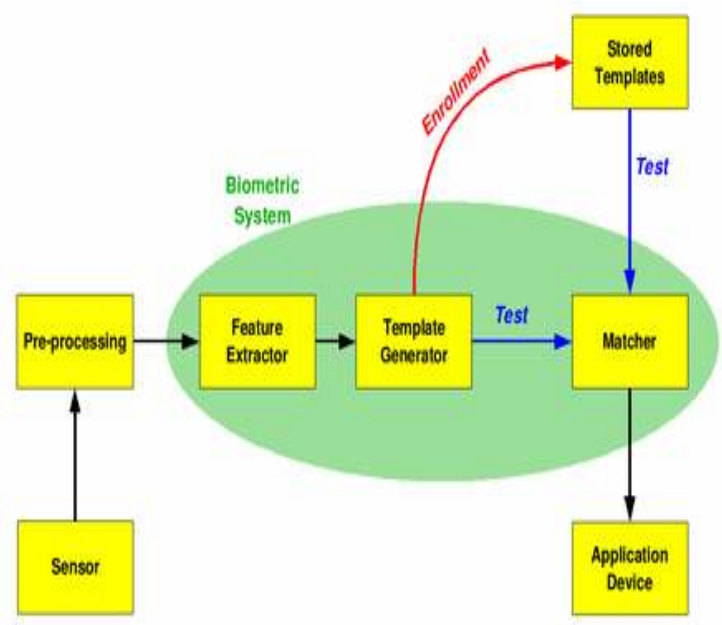

Figure 1: Biometric System

As time evolved various issues of the security, using recognition technologies has evolved. It comes in various forms like…

- Iris and retinal scans
- Facial recognition
- Finger print
- Voice recognition
- Hand geometry

Here we try to present one of the various above-mentioned ways that is iris Technology. We try to explain how and where it is employed.

Index Terms- Biometric Identification, Biometric Authentication, IRIS scans, Retinal scans, Remote Optical Unit

I. Introduction

In golden days people were identified by birth marks facial features and scans which were biometrics then. Biometrics is slowly but surely becoming standards of Authentication in everyday life. Banks worldwide are already experimenting with iris and Retinal scans for ATM machines; laptops are being produced with built in finger print scanners. There are more and more industries going biometric way. With the advent of Modern era, it has become important to go for technologies, which are more secure.

As time evolved various issues of the security, using recognition technologies has evolved. It comes in various forms like

1. Iris and retinal scans
2. Facial recognition
3. Finger print
4. Voice recognition
5. Hand geometry

II. Research Details About Other Authentication

A. Iris and Retinal scan

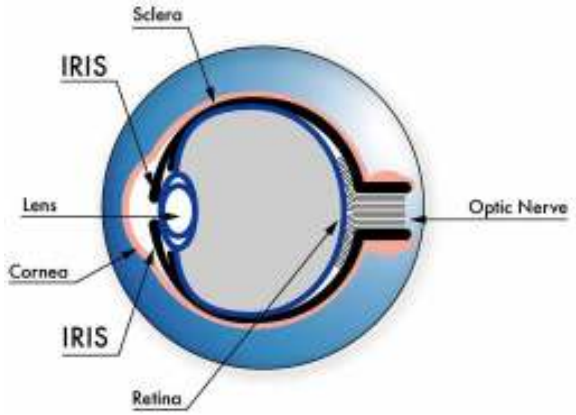

Figure 2: IRIS Scan

Iris and retinal scans are two completely different methods of identification.

1. The iris is photographed using a conventional COD camera, and the resultant image is compared to the template image that is stored in the database for iris characteristics such as filaments, crypts, striations and freckles.
2. In retinal scanning, the capillaries at the back of the eye are analyzed but it creates problem with those using spectacles.

B. Facial Recognition

Facial recognition tries to match various facial characteristics such as distance between eyes, width of nose, cheekbones, jaw line and chin characteristics to arrive at an identity match. This has found limited success in practical applications due to various factors such as facial features being covered by hats or hair, reflection from spectacles angle of capture.

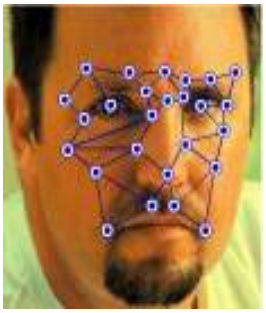

Figure 3: Face Pattern

C. Hand Geometry

Hands by themselves are not descriptive enough to result in positive Identification. It takes into consideration a combination of various factors such as shape, Size, finger length, thickness, and such. It is generally used where fingerprint is considered intrusive.

Figure 4: Hand Geometry Scan

D. Fingerprint Scans

Fingerprinting has played a very important role in forensics. Fingerprint scanning devices are one of the most common biometric devices available. However the device used are slightly more complex. They follow various methods from matching print patterns such as whorls, cusps, and ridge the matching of at least 15 different characteristics.

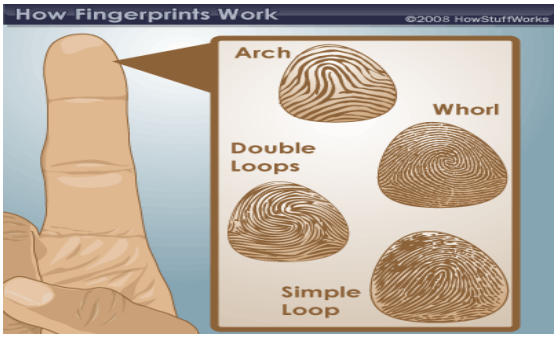

Figure 5: Finger Print

E. Voice Recognition

This is favorite of moviemakers. Some often access their cars, secret underground tunnels by just mentioning a few key phrases. Voice verification is not effective because acoustics and other external disturbances interfere with the process.

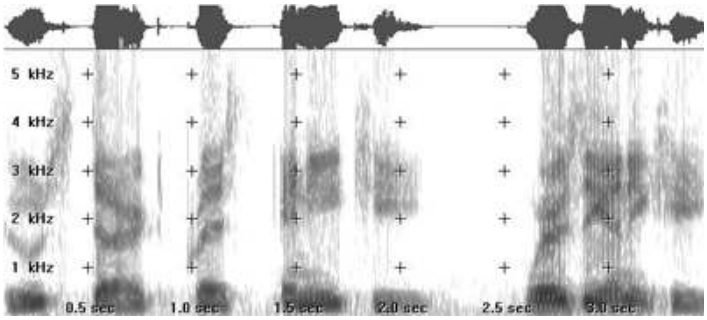

Figure 6: Voice print

III. IN DEPTH: IRIS TECHNOLOGY

Iris is a part inside our eye, which is unique in every individual, it remains unchanged till end of life this is the most prominent technique that can be implemented. The capture of iris is very simple one even need not stand before the camera. So here, we try to give the details of how iris scan is implemented.

Iris recognition is the best of breed authentication process available today. Iris recognition takes a picture of the iris; this picture is used solely for authentication it is different from retinal scanning.

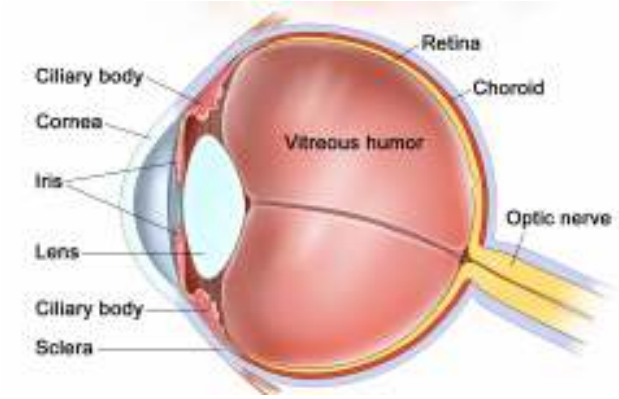

Figure 7: Retina Scan

Iris security system is smoother, smarter and more secure identification system Automated high speed iris capturing and precision identification make iris identification system the world's most advanced access and entry point security identification system. The automatic capturing of iris, identification is as simple as looking at the camera. High speed and precision make this system the world's most advanced access and entry point security identification system.

Using the iris recognition technology has reduced errors to less than one in 1.2 million ensuring highly precise individual identification. Confusion or duplication with another individual

is virtually impossible. No physical contact makes it perfectly safe. As the users simply need to stand in front of the camera, physical contact is not required. A very weak amount of infrared illumination is used, making the system perfectly safe.

B. Camera Specification

Specifications of the camera used to capture the iris are-

1. It takes approximately 3 seconds for recognition that is to capture the eye and check the data.
2. It can recognize up to 4000 irises i.e. 2000 persons. This accepts an ID of maximum 17 digits and a password of 10 digits.
3. The iris can be captured within a distance of 20 meters from control unit. Backup for iris recognition is password access by 10 key inputs.
4. The camera can be installed on the table with camera stand indoor application only and only in vertical direction.
5. It requires a power of 32v DC from control unit max. 20m, from control unit and 24v DC with power supply of unit max. Of 100m from control unit.
6. The operating temperature is from +zero deg c - +40 deg c and operating humidity is 20% to 80%.

B. Why Iris recognition preferred

Iris recognition is preferred as it is

1. Stable: The iris in human has a unique pattern hitch is formed by 10 months of age, and remains unchanged throughout one's lifetime.
2. Unique: It is impossible for two irises to produce the same code.
3. Flexible: Iris recognition technology easily integrates into existing security systems.
4. Reliable: Iris pattern is distinctive and is not susceptible to theft, loss or compromise.
5. Non-Invasive: Iris recognition is non-contact and quick, and offers unmatched accuracy when compared to any other security alternative, from distances as far as 3" to 10" unlike retinal screening.

IV. HOW IT WORKS

Iris recognition technology provides accurate identity authentication without PIN numbers, passwords or cards and the enrollment takes less than 2 minutes. Authentication takes less than 2 seconds. Producing a template to enroll has been made easy with the use of Video-based technology.

The terminology "iris-scanning" is often used when referring to iris recognition technology, but there is no scanning involved at all. Iris technology is based on pattern recognition and the pattern-capturing methodology is based on video camera technology similar to that found in camcorders commonplace in consumer electronics.

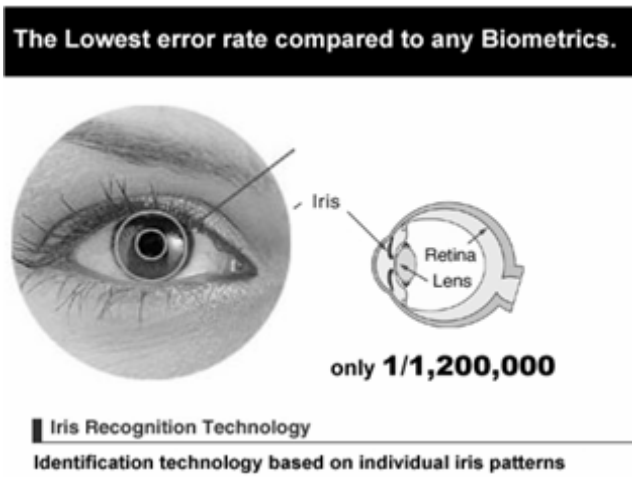

Figure 8 IRIS Ratio

B. Iris Scan

The camera has two apertures. The first contains a hologram that helps position the eye properly for registration or verification and performs the actual recognition. The second helps illuminate the eye to create an accurate image map of your eye as with the U. Are U system, enrollment is simple and straightforward. People wearing glasses need to take them off during enrollment, but they do not have to remove them later to be identified for login, according to the company.

We claim that we can replace any traditional authentication user ID and password schema with Iris recognition and iris authentication technology in any application, operating system or any web application. Retina is that reliable tool, that, any Organization, which is serious about protecting their network environment to help maintain network integrity.

B. Recognition

Recognition takes just 2 seconds. The proximity sensors activate the Remote Optical Unit (ROU) when the subject nears the operational range of the unit upon approaching a portal protected by iris access. The same mirror assisted, audio prompted interface that the subject became familiar with at enrollment helps ensure proper positioning and speedy recognition.

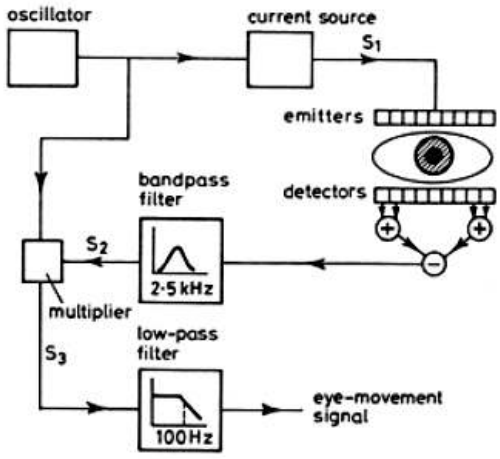

Figure 9 IRIS Scanning

To create, select and digitize an image to be compared against the stored value retained at enrollment the ROU uses the video and Frame grabbing method. The live presented value is compared against stored values at the Well-secured Identification Control Unit assigned to the portal. Once the iris is matched, Either a direct signal is sent to activate a door, or a Weygand signal sent to a central Access panel provides the drive to open the door to an individual authorized to enter.

C. *How Iris recognition compares to other Biometrics (Merits)*

Accurate: The iris recognition is the most accurate of the commonly used biometric technologies. There are a number of factors that weigh heavily in iris recognition's favor for applications requiring large databases and real-time authentication.

Every iris is absolutely unique. A subject's left and right iris is as different from each other as they are from any other individual's. The chance of finding two randomly formed identical irises has been calculated and is on an almost astronomical Order of one in 1078.

No human intervention is required to "set" thresholds for False Accept and False Reject performance is another differentiator affecting accuracy, while an unmatched EER (equal error rate) performance of 1 in 1.2 million is delivered.

The data-richness of the iris itself is at the root of iris recognition's accuracy. The Iris Access system captures over 240 degrees of unique characteristics in formulating it algorithmic template. Fingerprints, facial recognition and hand geometry have far less .Detailed input in template construction. Iris recognition can authenticate with confidence even when significantly less than the whole eye is visible.

Stability: Virtually every other biometric template changes significantly over time, detracting from overall system performance and requiring frequent reenrollment. Voices change. Hands and fingers grow. The type of labor one does, even weather temperature or one's medical condition can result in template changes in other technologies. Barring suffering and certain ophthalmologic surgery, the patterns in the iris are constant from age one to death.

Fast: No other biometric technology is designed to deliver 1-n searching of large databases in real time. A 2001 study conducted by the UK's National Physical Laboratory found iris technology was capable of nearly 20 times more matches per minute than its closest competitor was. By speed in conjunction with accuracy, there is no other technology that can deliver high accuracy authentication in anything close to the real-time performance of iris recognition.

Conversely, fingerprint searches are challenged by database size, adding time to searches or necessitating filtering as a search acceleration technique. Even so, fingerprint technology often returns multiple "possible matches," forcing introduction of human decision factors and increasing the potential for error in an authentication decision.

Scalable: As iris data templates require only 512-bytes of storage per iris, very large databases can be managed and speedily searched without degradation of performance accuracy.

Non-Invasive: In the imaging and iris authentication, bright lights or lasers are used. The user can stand as far as 10" away from the unit, and even wear glasses or contact lenses without compromising system accuracy. Unlike some other popular biometrics, iris authentication involves no physical contact. Not only does this mean "no touch" zero authentications, it also means the technology is ideally suited for use in environments where rubber gloves or other protective gear is used.

V. DISADVANTAGES

1. Fingerprint technology seems best suited for PC and network access.
2. Managing this convergence of physical and information security requirements now drives security system architecture design and implementation, and is an increasingly key factor in biometric technology selection.
3. Managing convergence will only become a more complex task because as the IT and communications becomes increasingly wireless, the need for robust identity management will become more acute.
4. Small target (1cm) to acquire from a distance (1m).
5. Moving target within another on yet another.
6. Illumination should not be bright or visible.
7. Obscured by eyelashes, lenses, reflection.

VI. APPLICATIONS

Iris technology is implemented in various places like offices, traffic control centers, airports, and at several public places

1. Offices: Data centers, material storage, safes, executive offices, secure meeting rooms
2. Laboratories and Factories: Drug or dangerous materials storage rooms, night or holiday entry control
3. Financial Institutions: Safes, safety deposit box room
4. Lifeline Facilities: Power generator rooms, dam management offices, gas company control rooms
5. Traffic Control Centers: Expressway administration centers, railroad dispatcher rooms
6. Airport and Harbor Facilities: Staff gates, immigration, workshops.

VII. CONCLUSION

The versatility of iris technology lends itself to virtually any application where identity authentication is required to enhance security, ensure service, eliminate fraud or maximize convenience.

Iris recognition applications are generally opt-in – there is none of the surveillance stigma sometimes affiliated with facial recognition, which scans crowds looking for individuals. Nor is there any tie –in to the large fingerprint databases maintained by law enforcement agencies, which often gives a negative stigma to fingerprint-based systems.

Today…

While the most common use of iris recognition to date is

physical access control in private enterprise and government, the versatility of the technology will lead to its growing use in large sectors of the economy such as transportation, healthcare, and national identification programs. Although security is clearly a prime concern, iris recognition is also being adopted for productivity-enhancing applications like time and attendance.

Tomorrow…

Enterprise and government both acknowledge the convergence of physical and information security environments, but there are new security challenges on the horizon – just-in-time inventory control, sophisticated supply chain management, and even a phenomenon called "coo petition"-in which companies that compete in some areas, cooperate in others.

REFERENCES

[1] P. J. Phillips, A. Martin, C.L. Wilson and M. Przybocky, "An Introduction to Evaluating Biometric Systems", IEEE Computer Magazine, February 2000, pp 56-63.
[2] UK BWG, "Best Practices in Testing and Reporting Performance of Biometric Devices", January 2000, web site: http://www.cesg. Gov.uk /technology/biometrics.
[3] A. Mansfield, G. Kelly, D. Chandler, and J. Kane, "Biometric Product Testing Final Report", issue 1.0, U.K. National Physical Lab, March 19, 2001 http://www.cesg.gov.uk/ technology /biometrics/.
[4] LibraryThinkQuest.org "Introduction to Biometrics". Retrieved March 29,2010 from http://library.thinkquest.org/28062/intro.html
[5] Tom Harris "How Fingerprint Scanners Work". Retrieved March 29,2010 from http://computer.howstuffworks.com/fingerprint-scanner4.htm
[6] WikTionary.org "biometrics". Retrieved March 29,2010 from http://en.wiktionary.org/ wiki/ biometrics
[7] It.Jhu.edu "biometrics". Retrieved March 29,2010 from http://www.it.jhu.edu/ glossary/ abc.html
[8] IdTeck.com "What is Fingerprint Recognition?" Retrieved March 29,2010 from http://www.idteck.com/support/w_fingerprint.asp
[9] BiometricNewsPortal.com "Fingerprint advantages". Retrieved March 29,2010 from http://www.biometricnewsportal.com/fingerprint_biometrics.asp
[10] IdTeck.com "What is Fingerprint Recognition?" Retrieved March 29,2010 from http://www.idteck.com/support/w_fingerprint.asp#1
[11] Britannica.com "Iris". Retrieved March 29,2010 from http://www.britannica.com/ Ebchecked /topic/294031/iris Vision.about.com "Iris". Retrieved March 29,2010 from http://vision.about.com/od/eyeanatomy/g/Iris.htm
[12] Daniel "Iris recognition at airports uses eye-catching technology". Retrieved March 29,2010 from http://www.howstuffworks.com/ framed.htm?parent=biometrics.htm&url=http://archives.cnn.com/2000/TECH/computing/07/24/iris.explainer/index.html
[13] Tracy V. Wilson "How Biometrics Works". Retrieved March 29,2010 from http://www.howstuffworks.com/biometrics4.htm
[14] DiscoveriesInMedicine.com "Retinography". Retrieved March 29,2010 from http://www.discoveriesinmedicine.com/Ra-Thy/Retinography.html
[15] WiseGeek.com "How does a Retinal Scan Work?". Retrieved March 29,2010 from http://www.wisegeek.com/how-does-a-retinal-scan-work.htm
[16] Ostaff, Courtney. (April, 2008) "Retinal Scans Do More Than Let You In The Door."
[17] Searchsecurity.Techtarget.com "Voiceprint". Retrieved March 29,2010 from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci946211,00.html
[18] Tracy V. Wilson "How Biometrics Works". Retrieved March 29,2010 from http://science.howstuffworks.com/biometrics3.htm

First Author – Prof. Chandrakant D. Patel, AMPICS MCA Department, Ganpat University, India, Email: cdp021@ganpatuniversity.ac.in

Second Author – Prof. Sanket Trivedi, Kalol Institute of Mgmt, Kalol, India, Email: sanket.trivedi@gmail.com.

Third Author – Prof. Sanjay Patel, AMPICS MCA Department, Ganpat University, India, Email: sbp053@ganpatuniversity.ac.in