Database Security in Retina Identification Biometrics System

Anil Dixit
Research Scholar
Jain University, Bangalore
Karnataka – 560027, India

Dr. Suchithra R
Jain Global Campus, Jain University
Jain University, Bangalore
Karnataka – 560027, India

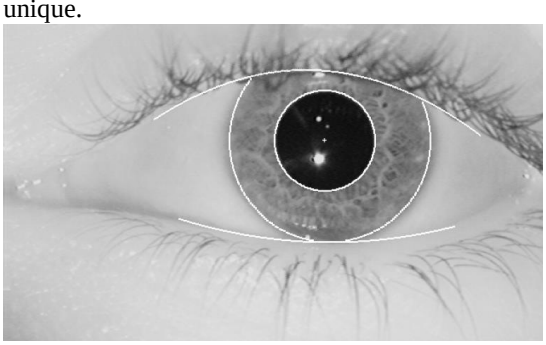
***Abstract*: Security is one of the key aspects and has become a part of every one's life. Threat to property, lives and the crucial data is ever growing. As humans have learnt to live with the above, there has been significant developments in securing them also. Biometrics is one of the key elements which has been invented and introduced in all key establishments to encounter and thwart security threats. Not only have the value of biometrics grown but also its use. Biometrics not only serve the authentication and security but it also increases efficiency among the working class by taking care of individual's punctuality and availability by the way of recording his / her authentication in the database which would be available later on for any kind of forensics. Some of the crucial sectors which has introduced the biometrics are Government Departments, Defense, Banking and Financial institutions. This paper focuses on efficiency of biometrics particularly IRIS and its accuracy when performance has been key to its functioning.**

Keywords: Security, Biometrics, Iris and Database.

I. INTRODUCTION

Electronic arena is witnessing rapid sophisticated jump, a large and important phase wherein recognition systems have a role to play a larger, effective and with accuracy as Information Technology has moved ahead by leaps and bounds [2]. Iris recognition is the best of breed authentication process available today. While it has been mistaken for Retinal Scanning, iris recognition simply involves taking a picture of the iris; this picture is used solely for authentication. Iris makes for a good choice because: -

(a) Of the unique pattern of One's Iris since its stabilizing from age of 10 months, it is stable and stands unique.



(b) Probability of two IRIS producing the same code is almost NIL.

(c) Provides flexibility as it is interoperable between different systems.

(d) Patterns are unlikely to be made a copy and hence reliable

(e) Retinal scanning is much complicated as it requires individual to get to the camera as close as much he / her she can whereas IRIS can match even from a distance of up to 15 feet.

II. LITERATURE SURVEY

Characteristics which could be used in biometric system must have two important things Uniqueness and repeatability properties. This means that the characteristics must be so that it could recognize all people from each other and also it must infinitely be measurable for all peoples [6].

III. THE EMERGENCE OF BIOMETRICS

To bind identity more closely to an individual and appropriate authorization, a new identity convention is becoming more prevalent. Based not on what a person has or knows, but instead on what physical characteristics or personal behavior traits they exhibit, these are known as biometrics – measurements of behavioral or physical attributes – how an individual smells, walks, signs their name, or even types on a keyboard, their voice, fingers, facial structure, vein patterns or patterns in the iris.

History

The Biology behind the Technology *[1-4, 15].*
Like a snowflake, the iris – the externally visible colored ring around the pupil – of every human eye is absolutely unique, exhibiting a distinctive pattern that forms randomly in utero in a process called chaotic morphogenesis. In fact, it's estimated the chance of two iris (irides) being identical is 1 in 10.

Who invented iris scans?

Here's a quick history of how iris scanning technology has developed: -

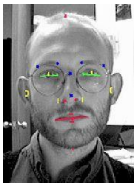
- 1936: US ophthalmologist Frank Burch suggests the idea of recognizing people from their iris patterns long before technology for doing so is feasible.

- 1981: American ophthalmologists Leonard Flom and Aran Safir discuss the idea of using iris recognition as a form of biometric security, though technology is still not yet advanced enough.
- 1987: Leonard Flom and Aran Safir gain US patent #4,641,349 for the basic concept of an iris recognition system.
- 1994: US-born mathematician John Daugman (currently a professor of computer science at Cambridge University, England) works with Flom and Safir to develop the algorithms (mathematical processes) that can turn photographs of irises into unique numeric codes. He is granted US patent #5,291,560 for a "biometric personal identification system based on iris analysis" the same year. Daugman is widely credited as the inventor of practical iris recognition since his algorithm is used in most iris-scanning systems.
- 1996: Lancaster County Prison, Pennsylvania begins testing iris recognition as a way of checking prisoner identities.
- 1999: Bank United Corporation of Houston, Texas converts supermarket ATMs to iris-recognition technology.
- 2000: Charlotte/Douglas International Airport in North Carolina and Flughafen Frankfurt Airport in Germany become two of the first airports to use iris scanning in routine passenger checks.
- 2006: Iris-scanning systems are installed at British airports, including Heathrow, Gatwick, Birmingham, and Stansted. Privacy concerns notwithstanding, hundreds of thousands of travelers voluntarily opt to use the machines to avoid lengthy passport-checking queues.

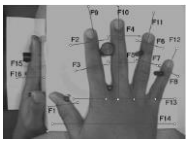
Traditional Notions of Establishing Identity

Historically, identity or authentication conventions were based on things one possessed (a key, a passport, or identity credential), or something one knew (a password, the answer to a question, or a PIN.) This possession or knowledge was generally all that was required to confirm identity or confer privileges. However, these conventions could be compromised – as possession of a token or the requisite knowledge by the wrong individual could, and still does, lead to security breaches

Types of Biometrics [1-15]



Facial Recognition: records the spatial geometry of distinguishing features of the face. Different vendors use different methods of facial recognition, however, all focus on measures of key features of the face. Face recognition has been used in projects to identify card counters or other undesirables in casinos, shoplifters in stores, criminals and terrorists in cities. This biometric system can easily spoofed by the criminals or malicious intruders to fool recognition system or program.



Palm Print: Palm print verification is a slightly modified form of fingerprint technology. Palm print scanning uses an optical reader very similar to that used for fingerprint scanning; however, its size is much bigger, which is a limiting factor for use in workstations or mobile devices.

Signature Verification: It is an automated method of examining an individual's signature. This technology is dynamic such as speed, direction and pressure of writing, the time that the stylus is in and out of contact with the board. Signature verification temples are typically 50 to 300 bytes. Disadvantages include problems with long-term reliability, lack of accuracy and cost.

Fingerprint: A fingerprint as shown in the figure is a recognition system which constitutes of fingerprint acquiring device, minutia extractor and minutia matcher. As it is more common biometric recognition used in banking, military etc., but it has maximum limitation that it can be spoofed easily. Other limitations are caused by particular usage factors such as wearing gloves, using cleaning fluids and general user difficulty in scanning.

Iris Scan: Iris as shown in figure is a biometric feature, found to be reliable and accurate for authentication process comparative ot other biometric feature available today.

Components of Biometric Systems [13]

- Sensor module which acquires the biometric data.
- Feature extraction module where the acquired data is processed to extract feature vectors.
- Matching module where attribute vectors are compared against those in the template.
- Decision making module in which the user's identity is established or a claimed identity is accepted or rejected.

Characteristics of Biometric Systems [13]

- Universality – Everyone should have it.
- Distinctiveness – No two should be the same
- Permanence – It should be invariant over a given era of time.

- Collectability – In real life application, three more factors need to be considered i.e. Performance (Accuracy, speed, resource requirements), Acceptability (should not harm users) and circumvention (anti-hack methods incorporated).

Image Processing Methods / Extraction of features [1-4 and 10-14]

Figure1: Structure of Eye (Iris system)

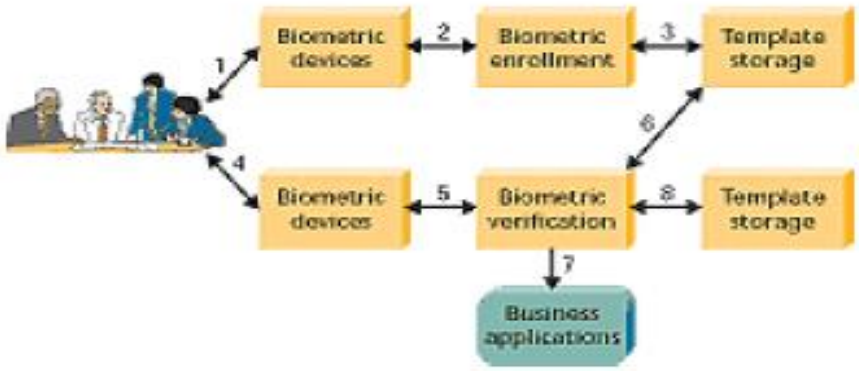


Figure2: Process of Enrollment and Verification

Iris Access system incorporates other system-designed elements. A low profile Identity Controller (ICU) offers easy greater integration convenience while ensuring that biometric templates are kept safe, protected and secure, off the imager.

A camera scans the person's eye and produces a digital image.

Image processing software attempts to isolate the iris by drawing two circles, one at its inner boundary (between the pupil and the iris) and the other at its outer boundary (known as the limbus, between the iris and the white, outer sclera). The inner boundary is relatively easy to detect, because it's generally a circle with a sudden change in brightness where the pupil gives way to the iris. A broadly similar process is used to find the outer boundary, though it has to allow for the likelihood of the eyelids blocking part of the iris.

Polar coordinates (concentric circles and radial lines from their origin) are then added to the image to define separate "zones of analysis," so that key features of the iris can be accurately located and compared in two-dimensional space. This system cleverly allows for the way the iris changes as the pupil grows (dilates) and shrinks (constricts) in different light conditions.

The pattern of light and dark areas in the iris is then converted into digital form using band pass filters (crudely speaking, if the brightness in a given area is more than a certain amount, the filters might register a 1, otherwise they would register a 0), and, with a bit of mathematical juggling, this generates the unique, digital Iris Code. A particular eye will generate roughly the same code whether its pupil is dilated or not.

The following tables show the probabilities of false accept and reject [15]:-

Sr.no.	Hamming Distance	False Accept Probability	False Reject Probability
1	.28	1 in 10^{12}	1 in 11.400
2	.29	1 in 10^{11}	1 in 22.700
3	.30	1 in 6.2 billion	1 in 46.000
4	.31	1 in 665 million	1 in 95.000
5	.32	1 in 81 million	1 in 201.000
6	.33	1 in 11 million	1 in 433.000
7	.34	1 in 1.7 million	I in 950.000
8	.342	1 in 1.2 million	1 in 1.2 million
9	.35	1 in 295.000	1 in 2.12 million
10	.36	I in 57.000	1 in 4.84 million
11	.37	1 in 12.300	1 in 11.3 million

Advantages of Iris Recognition [15]

Iris recognition is an attractive technology for identity authentication for several reasons.

a. The smallest outlier population of all biometrics. Few people can't use the technology as most individuals have at least one eye. In a few instances even blind persons have used iris recognition successfully, as the technology is iris pattern-dependent, not sight dependent.

b. Iris pattern and structure exhibit long-term stability. Structural formation in the human iris is fixed from about one year in age and remains constant (barring trauma, certain rare diseases, or possible change from special some ophthalmologic surgical procedures) over time. So, once an individual is enrolled, re-enrollment requirements are infrequent. With other biometric technologies, changes in voice timbre, weight, hairstyle, finger or hand size, cuts or even the effect of manual labor can trigger the need for re-enrollment.

c. Ideal for Handling Large Databases. Iris recognition is the only biometric authentication technology designed to work in the 1-n or exhaustive search mode. This makes it ideal for handling applications requiring management of large user groups, such as a National Documentation application might require. Large databases are accommodated without degradation in authentication accuracy. Iris Access platforms integrate well with large database back ends like Microsoft SQL and Oracle and other Relational Databases.

d. Unmatched Search Speed in the one to many search mode is unmatched by any other technology, and is limited not by database size, but by hardware selected for server management. In a UK Government-commissioned study, Iris ID's Iris Access platform searched records nearly 20 times faster than the next fastest technology. Iris ID has developed a high speed matching engine, Iris Accelerator, designed to deliver 10 million+ matches per second.

e. Versatile for the One to Many, One to One, Wiegand and Token Environments. While initially designed to work in one-to-many search mode, iris recognition works well in 1-1 matching, or verification mode, making the technology ideal for use in multifactor authentication environments where PINs, or tokens like prox or smartcards are used. In a token environment, many privacy issues related to biometric database management are moot, as the user retains control of biometric data – a small template of 512 bytes per iris.

f. Safety and Security Measures in Place. Iris recognition involves nothing more than taking a digital picture of the iris pattern (from video), and recreating an encrypted digital template of that pattern. 512-byte iris templates are encrypted and cannot be re-engineered or reconstituted to produce any sort of visual image. Iris recognition therefore affords high level defense against identity theft, a rapidly growing crime. The imaging process involves no lasers or bright lights and authentication is essentially non-contact.

g. Convenient, Intuitive User Interface. Using the technology is an almost intuitive experience, requiring relatively little cooperation from subjects. Proximity sensors activate the equipment, which incorporates mirror-assisted alignment functionality. Audio auto-positioning prompts, automated image capture, and visual and audio authentication decision-cueing completes the process.

Disadvantage of Iris Recognition Systems.

The main disadvantage of Iris system is "data mismatch" error which needs to be taken care of at an early stage of enrollment. This if catered for during the enrollment will negate the error where-in user can be detected without any false-positives.

Securing and Developing IRIS

Securing Revocable IRIS and Retinal Templates using combined user and soft biometric based password hardened multimodal fuzzy vault speaks about the cryptographic construct to be used for improving the authentication system [3].

Combining face and iris biometrics for having a double check on authentication is also a viable option [10].

IWTHRS model is one of options to secure the system [12].

Storing Iris in different image formats and authentication is an option for high security areas [11].

Open source Iris recognition speaks of acquiring almost 40 images for a secure authentication and fool proof method [14].

CONCLUSION

Of all the biometric technologies used for human authentication today, it is generally conceded that iris recognition is the most accurate. Coupling this high confidence authentication with factors like outlier group size, speed, usage/human factors, platform versatility and flexibility for use in identification or verification modes – as well as addressing issues like database size/management and privacy concerns – iris recognition has also shown itself to be exceedingly versatile and suited for large population applications. Also, in the ever emerging security challenges IRIS system would almost be a deterrence to the enemies which cannot be compromised at lower levels.

REFERENCES:

[1] Efficient Iris Biometrics Technique for Secure Distributed Systems by Ammer A. Mohammed Baqer and Suhas H. Patil – International Journal of Computer Science and Network Security, Vol. 12, No. 3, March 2012.

[2] Biometric Iris Recognition Based on Hybrid Technique by Khattab M. Ali Alheeti – International Journal on Soft Computing (IJSC) Vol. 2, No.4/ November 2011.

[3] Securing Revocable Iris and Retinal Templates using Combined User and Soft Biometric based Password Hardened Multimodal Fuzzy Vault by VS Meenakshi and Dr. G. Padmavathi International Journal of Computer Science Issues, Vol. 7, Issue 5, September 2010. ISSN (Online): 1694-0814.

[4] A Comparative Study of Facial, Retinal, Iris and Sclera Recognition Techniques by Sugandha Agarwal, Rashmi Dubey, Sugandh Srivastava and Prateek Agarwal – IOSR Journal of Computer

Engineering (IOSR-JCE). e-ISSN: 2278-0661. P-ISSN: 2278-8727 Volume 16, Issue 1, Ver. VI (Feb 2014), PP 47-52.

[5] Improved Network Security through Retinal Biometric Based Authentication by Mohammed Basheer KP and Dr. T. Abdul Razak – Mohammed Basheer K P et al, Int.J.Computer Technology & Applications, Vol 4 (6), 1015-1019.

[6] Retina Identification based on the pattern of blood vessels using fuzzy logic by Wafa Barkhoda, Fardin Akhlaqian, Mehran Deljavan Amin and Mohammad Sadeq Nouraazzadeh –Barkhoda et al. EURASIP Journal on Advances in Signal Processing 2011, 2011:113.

[7] Retina based Personal Identification System using Skeletonization and Similarity Transformation by Geethu Sasidharan – International Journal of Computer Trends and Technology (IJCTT) – Volume 17 Number 3 – Nov 2014.

[8] Retinal Biometrics based Authentication and Key Exchange System by K Saraswathi, B Jayaram and Dr. R Balasubramanian – International Journal of Computer Applications (1975 – 8887) Volume 19 – No. 1, April 2011.

[9] Doubts about the Usefulness of Retina Codes in Biometric Recognition by Thomas Fuhrmann and Andreas Uhl.

[10] Combining Face and Iris Biometrics for Identity Verification by Yunong Wangm Tieniu Tana dn Anil K. Jain.

[11] Development of New Algorithm for Iris Biometric Recognition by Raida Hentati, Manel Hentati and Mohamed Abid – International Journal of Computer and Communication Engineering, Vol. 1, No. 3, September 2012.

[12] High Security Human Recognition System using Iris Images by CR Prashanth, Shashikumar DR, KB Raja, KR Venugopal and LM Patnaik – International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[13] Iris Biometric Recognition for Person Identification in Security Systems by Vanaja Roselin E. Chirchi, Dr. LM Waghmare and ER Chirchi – International Journal of Computer Applications (0975 – 8887) Volume 24 – No. 9, June 2011.

[14] Iris Recognition System using Biometric Template Matching Technology by Sudha Gupta, Abhinav Jain and Sreeram Iyer - International Journal of Computer Applications (0975 – 8887) Volume 1 – No 2, 2010.

[15] Penny Khaw SANS Security Essentials (GSEC) Practical Assignment - Version 1.3