Volume 3, Issue 6, June 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Iris as a Biometric Feature: Application, Recognition, Advantages & Shortcomings

Samayita Bhattacharya, Kalyani Mali
Department of Computer Science & Engineering,
University of Kalyani, Kalyani, West Bengal, India

Abstract— Biometrics is one of the biggest tendencies in human identification. The iris is one of the recently developed biometrics, which is being used widely. This paper summarizes different aspect of iris, its application, recognition, advantages and shortcomings.

Keywords— Biometrics, Iris, Recognition, Advantage, Shortcomings.

I. INTRODUCTION

Identity or authentication conventions historically 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 [5][6]. 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 behaviour traits they exhibit, these are known as biometrics - measurements of behavioural 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. 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. Like a snowflake, the iris - the externally visible coloured 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^{78}.

Iris recognition is the best of breed authentication process available today. While many mistake it for retinal scanning, iris recognition simply involves taking a picture of the iris; this picture is used solely for authentication.

The features that makes iris recognition the authentication system of choice:

- Stable - the unique pattern in the human iris is formed by 10 months of age, and remains unchanged throughout one's lifetime.
- Unique - the probability of two rises producing the same code is nearly impossible.
- Flexible - iris recognition technology easily integrates into existing security systems or operates as a standalone.
- Reliable - a distinctive iris pattern is not susceptible to theft, loss or compromise
- Non-Invasive - unlike retinal screening, iris recognition is non-contact and quick, offering unmatched accuracy when compared to any other security alternative, from distances as far as 3" to 10".

II. BIOMETRICS

Biometrics consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioural traits. Currently Biometrics is one of the biggest tendencies in human identification [7].

Biometrics is claimed to be better than current and established authentication methods, such as:

- Personal identification numbers (PINs),
- Passwords,
- Smart cards.

Key advantages of using a biometric feature are:

- availability (always),
- uniqueness (to each person),
- not transferable (to other parties),
- not forgettable,

© 2013, IJARCSSE All Rights Reserved

- not subject to theft,
- not guessable.

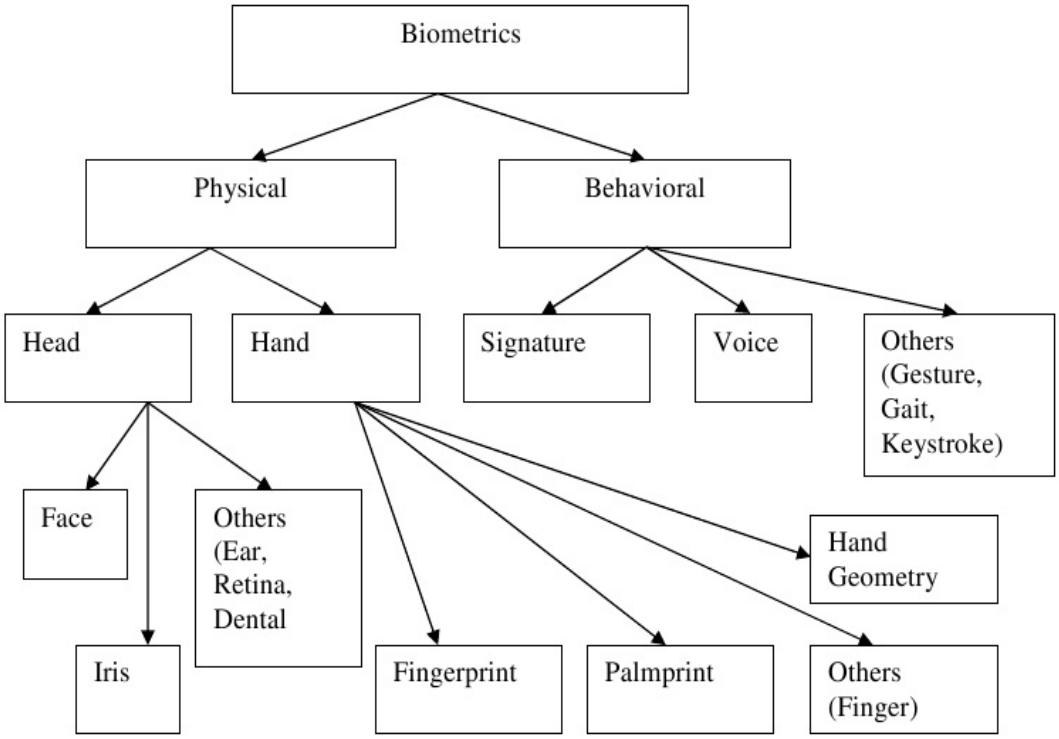

Figure 1: Various Biometrics

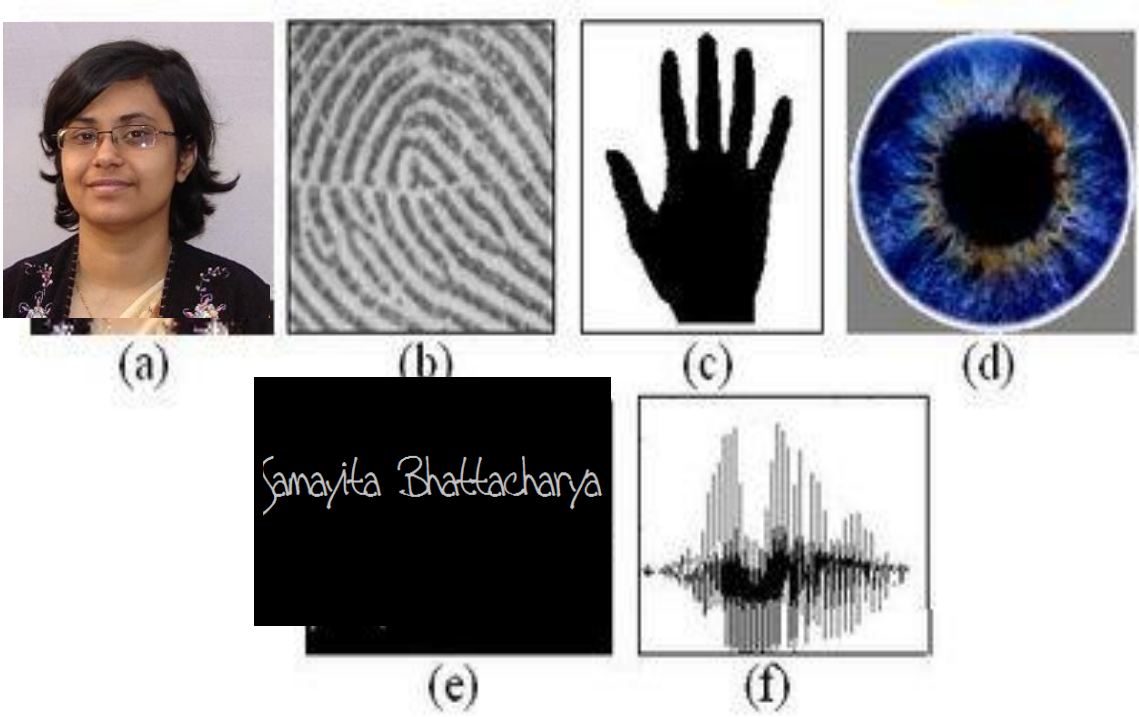

Figure 2: Few Biometric characteristics that are commonly used:
(a) face, (b) fingerprint, (c) hand geometry, (d) iris, (e) signature, (f) voice.

III. IRIS

The iris is a thin, circular structure in the eye, responsible for controlling the diameter and size of the pupil and thus the amount of light reaching the retina. The colour of the iris is often referred to as "eye colour."

© 2013, IJARCSSE All Rights Reserved

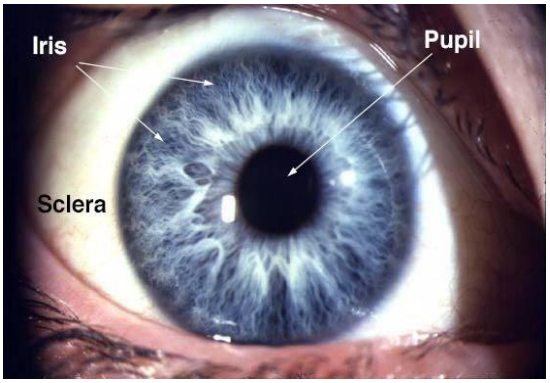

Figure 3: Iris Sample

IV. IRIS RECOGNITION

Iris recognition is a method of biometric authentication that uses pattern-recognition techniques based on high resolution images of the irises of an individual's eyes. Iris recognition uses camera technology, with subtle infrared illumination reducing specular reflection from the convex cornea, to create images of the detail-rich, intricate structures of the iris. Converted into digital templates, these images provide mathematical representations of the iris that yield unambiguous positive identification of an individual. Iris recognition efficacy is rarely impeded by glasses or contact lenses. Iris technology has the smallest outlier (those who cannot use/enroll) group of all biometric technologies. Because of its speed of comparison, iris recognition is the only biometric technology well-suited for one-to-many identification. A key advantage of iris recognition is its stability, or template longevity, a single enrollment can last a lifetime. There are few advantages of using iris as biometric identification: 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 labor. 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. Even genetically identical individuals have completely independent iris textures, whereas DNA (genetic "fingerprinting") is not unique for the about 0.2% of the human population who have a genetically identical twin. An iris scan is similar to taking a photograph and can be performed from about 10 cm to a few meters away. There is no need for the person to be identified to touch any equipment that has recently been touched by a stranger, thereby eliminating an objection that has been raised in some cultures against fingerprint scanners, where a finger has to touch a surface, or retinal scanning, where the eye can be brought very close to a lens (like looking into a microscope lens).While there are some medical and surgical procedures that can affect the colour and overall shape of the iris, the fine texture remains remarkably stable over many decades. Some iris identifications have succeeded over a period of about 30 years.

But Iris scanning is a relatively new technology and is incompatible with the very substantial investment that the law enforcement and immigration authorities of some countries have already made into fingerprint recognition. Iris recognition is very difficult to perform at a distance larger than a few meters and if the person to be identified is not cooperating by holding the head still and looking into the camera. However, several academic institutions and biometric vendors are developing products that claim to be able to identify subjects at distances of up to 10 meters. As with other photographic biometric technologies, iris recognition is susceptible to poor image quality, with associated failure to enroll rates [1]. As with other identification infrastructure (national residents databases, ID cards, etc.), civil rights activists have voiced concerns that iris-recognition technology might help governments to track individuals beyond their will.

Iris recognition is an attractive technology for identity authentication for several reasons, such as:

- Iris is 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.
- 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 a 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.
- 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. IrisAccess platforms integrate well with large database back ends like Microsoft SQL and Oracle 9i.
- 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

© 2013, IJARCSSE All Rights Reserved

ID's IrisAccess platform searched records nearly 20 times faster than the next fastest technology. Iris ID has developed a high speed matching engine, IrisAccelerator™, designed to deliver 10 million+ matches per second.

- 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.
- 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 defence against identity theft, a rapidly growing crime. The imaging process involves no lasers or bright lights and authentication is essentially non-contact.
- 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.

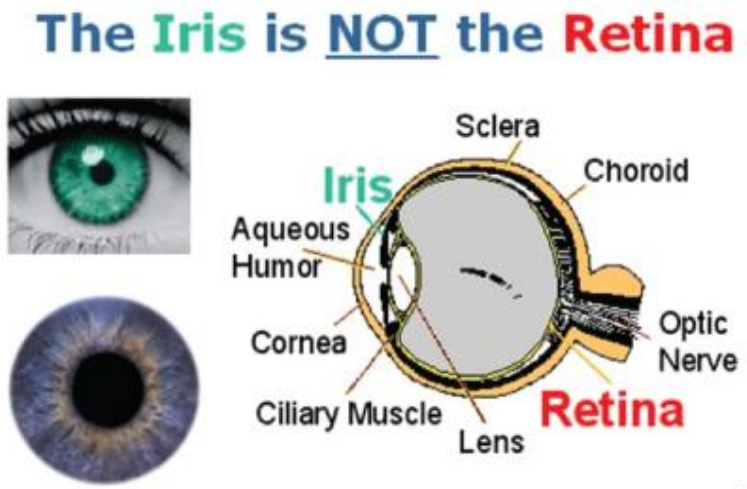

Figure 4: Difference of Iris & Retina

V. OPERATING PRINCIPLE

An iris-recognition algorithm first has to localize the inner and outer boundaries of the iris (pupil and limbus) in an image of an eye. Further subroutines detect and exclude eyelids, eyelashes, and specular reflections that often occlude parts of the iris. The set of pixels containing only the iris, normalized by a rubber-sheet model to compensate for pupil dilation or constriction, is then analyzed to extract a bit pattern encoding the information needed to compare two iris images. In the case of Daugman's algorithms, a Gabor wavelet transform is used. The result is a set of complex numbers that carry local amplitude and phase information about the iris pattern. In Daugman's algorithms, most amplitude information is discarded, and the 2048 bits representing an iris pattern consist of phase information (complex sign bits of the Gabor wavelet projections). Discarding the amplitude information ensures that the template remains largely unaffected by changes in illumination or camera gain (contrast), and contributes to the long-term usability of the biometric template. For identification (one-to-many template matching) or verification (one-to-one template matching), a template created by imaging an iris is compared to stored template(s) in a database. If the Hamming distance is below the decision threshold, a positive identification has effectively been made because of the statistical extreme improbability that two different persons could agree by chance ("collide") in so many bits, given the high entropy of iris templates.

VI. ADVANTAGES

The iris of the eye has been described as the ideal part of the human body for biometric identification for several reasons:

- 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. Like the fingerprint, it is very hard (if not impossible) to prove that the iris is unique. However, there are so many factors that go into the formation of these textures (the iris and fingerprint) that the chance of false matches for either is extremely low. Even genetically identical individuals have completely independent iris textures.

© 2013, IJARCSSE All Rights Reserved

- An iris scan is similar to taking a photograph and can be performed from about 10 cm to a few meters away. There is no need for the person being identified to touch any equipment that has recently been touched by a stranger, thereby eliminating an objection that has been raised in some cultures against fingerprint scanners, where a finger has to touch a surface, or retinal scanning, where the eye must be brought very close to an eyepiece (like looking into a microscope).
- The commercially deployed iris-recognition algorithm, John Daugman's IrisCode, has an unprecedented false match rate (better than 10−11 if a Hamming distance threshold of 0.26 is used, meaning that up to 26% of the bits in two IrisCodes are allowed to disagree due to imaging noise, reflections, etc., while still declaring them to be a match).
- While there are some medical and surgical procedures that can affect the colour and overall shape of the iris, the fine texture remains remarkably stable over many decades. Some iris identifications have succeeded over a period of about 30 years.

VII. SHORTCOMINGS

- Many commercial iris scanners can be easily fooled by a high quality image of an iris or face in place of the real thing.
- The scanners are often tough to adjust and can become bothersome for multiple people of different heights to use in succession.
- The accuracy of scanners can be affected by changes in lighting.
- Iris scanners are significantly more expensive than some other forms of biometrics, password or prox card security systems
- Iris scanning is a relatively new technology and is incompatible with the very substantial investment that the law enforcement and immigration authorities of some countries have already made into fingerprint recognition.
- Iris recognition is very difficult to perform at a distance larger than a few meters and if the person to be identified is not cooperating by holding the head still and looking into the camera. However, several academic institutions and biometric vendors are developing products that claim to be able to identify subjects at distances of up to 10 meters ("standoff iris" or "iris at a distance" as well as "iris on the move" for persons walking at speeds up to 1 meter/sec).
- As with other photographic biometric technologies, iris recognition is susceptible to poor image quality, with associated failure to enroll rates.
- As with other identification infrastructure (national residents databases, ID cards, etc.), civil rights activists have voiced concerns that iris-recognition technology might help governments to track individuals beyond their will.
- Researchers have tricked iris scanners using images generated from digital codes of stored irises. Criminals could exploit this flaw to steal the identities of others.
- Alcohol consumption causes recognition degradation as the pupil dilates/constricts causing deformation in the iris pattern.

VIII. SECURITY CONSIDERATIONS

As with most other biometric identification technology, a still not satisfactorily solved problem with iris recognition is the problem of live-tissue verification.

The reliability of any biometric identification depends on ensuring that the signal acquired and compared has actually been recorded from a live body part of the person to be identified and is not a manufactured template.

Many commercially available iris-recognition systems are easily fooled by presenting a high-quality photograph of a face instead of a real face, which makes such devices unsuitable for unsupervised applications, such as door access-control systems. The problem of live-tissue verification is less of a concern in supervised applications (e.g., immigration control), where a human operator supervises the process of taking the picture.

Methods that have been suggested to provide some defence against the use of fake eyes and irises include:

- Changing ambient lighting during the identification (switching on a bright lamp), such that the pupillary reflex can be verified and the iris image be recorded at several different pupil diameters.
- Analysing the 2D spatial frequency spectrum of the iris image for the peaks caused by the printer dither patterns found on commercially available fake-iris contact lenses.
- Analysing the temporal frequency spectrum of the image for the peaks caused by computer displays.
- Using spectral analysis instead of merely monochromatic cameras to distinguish iris tissue from other material.
- Observing the characteristic natural movement of an eyeball (measuring nystagmus, tracking eye while text is read, etc.).
- Testing for retinal retroreflection (red-eye effect).
- Testing for reflections from the eye's four optical surfaces (front and back of both cornea and lens) to verify their presence, position and shape.
- Using 3D imaging (e.g., stereo cameras) to verify the position and shape of the iris relative to other eye features.

IX. CONCLUSIONS

In the ever-changing world of global data communications, and fast-paced software development, security is becoming more and more of an issue [5].

© 2013, IJARCSSE All Rights Reserved

No system can ever be completely secure. All one can do is make it increasingly difficult for someone to compromise your system. The more secure the system is, the more intrusive the security becomes. One needs to decide where in this balancing act the system will still be usable, and yet secure for the purposes. Each one of the Technologies used in our days bring us a manner to restrict the access to a system, allowing the entrance only to those persons who know a specific code, own a card or have determined physic marks. The more complex is the system, the most difficult is to be attacked, although it will be more expensive and will require more software and hardware resources. When a new authentication system is implanted, it is essential a judgment between simplicity, price and efficiency, as well as social acceptability.

Here in this paper we have discussed various aspects of iris as a biometric feature, and how it can further be made more suitable identifier.

REFERENCES

[1] Zhaofeng He, Tieniu Tan, Zhenan Sun and Xianchao Qiu, "Towards Accurate and Fast Iris Segmentation for Iris Biometrics", In: IEEETransactions on Pattern Analysis and Machine Intelligence, 15 July 2008.

[2] Retina and Iris Scans. Encyclopedia of Espionage, Intelligence, and Security. Copyright © 2004 by The Gale Group, Inc.

[3] Hill, Robert. "Retina Identification". Msu.Edu.

[4] Roberts, Chris. "Biometrics" Retrieved on 2009-06-11

[5] Samayita Bhattacharya and Kalyani Mali, "Security, Forgery and Fingerprints: Advantages, Drawbacks and Limitation of Biometrics", International Journal of Computer Information Systems, May Issue, ISSN 2229 5208, Vol. 4, No. 5, 2012, pp 6-10.

[6] Samayita Bhattacharya, Kuntal Barua and Kalyani Mali, "Inimitability of Fingerprint for Establishment of Identity," International Journal of Electronics and Computer Science Engineering (IJECSE), ISSN - 2277-1956, Volume 1, Number 2.

[7] Samayita Bhattacharya, Kalyani Mali, "Importance of Fingerprints; Fingerprint as Biometric: Feature, Application & Recognition", LAP-Lambert Academic publication, ISBN: 978-3-659-39430-0, 2013.

© 2013, IJARCSSE All Rights Reserved