The Concept of Iris Identification in Biometric Security, the Present Scenario, Constraints and Future

Anupam Singh
3rd year Computer Science and Engineering
IEEE Student Member
Vellore Institute of Technology

Anupam Das
3rd year Computer Science and Engineering
IEEE Student Member
Vellore Institute of Technology

Abstract: **This paper deals with Iris recognition procedures and technology which associates the concepts of pattern identification and analysis, computer visioning, statistical dependency and elements of optics and photonics. It is a real time process. The algorithms help to confidently identify the identity of a person by mathematically analyzing the variance and randomness of the physical attributes of the iris surface. Presently employed in various walks of life for identification purpose, this process is open for further research. The authors try to dig deep into the underlying principles and make suggestions about improving overall efficiency of the process. The persistence of the iris as one of the identifying parameters, leads to some constraints and difficulties which have been underlined. The authors conclude by discussing the scope of further enhancements, suggestions on standardization and try to peer into the next generation of applications of iris recognition.**

.*Keywords*: Biometric, Iris, BioAPI, PKI, Forensics, Project IRIS.

Information Security- What is it?

The contemporary world is all about information. Vast repositories of information about virtually everything possible on earth consist of the data that is stored in the number of data banks all throughout the world. Information that is critical or of personal value is one such aspect that is vulnerable. Moreover in this ever changing world where a number of things are always on the line, some sort of security should be provided to protect the information. Hence it gives rise to the concept of information security which is the core issue of this paper. Hence we call information security as the techniques and methodologies that are applied for the protection and proliferation of data. The present information security measures that are being taken into account are password protection, smart cards, magnetic identifications, pattern recognizers, public key interface, voice identification, finger printing, hand geometry identification, face recognition, retina identification and iris recognition. The last six procedures are examples of the Biometric Security techniques.

What is Biometric Security?

Biometrics is that branch of science which employs biological components for measurement and identification. The use of biometrics in the field of security gives rise to the concept of biometric security. Biometric technology is gaining acceptance in today's world due to its high efficiency, cutting edge design, high reliability, fast processing and unparallel accuracy. Different applications require different biometrics.

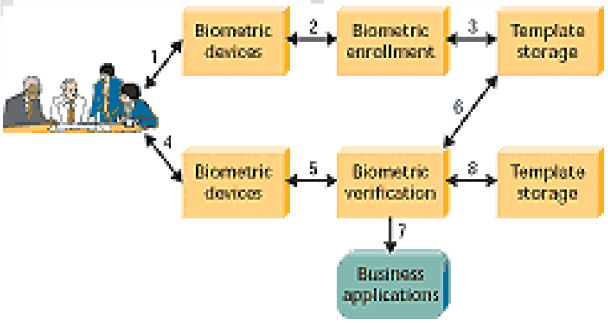
All the security devices available today use three different types of authentication:
something one knows—a password, PIN, or piece of personal information (such as your birthday); something one has—a card key, smart card, PKI (Public Key Infrastructure), or token (like a Ration Card); and/or something one is, which uniquely identifies himself- a biometric. The non biometric security devices have

a number of shortcomings. In case of password protection the password can be easily stolen or hacked. Even if it is not lost, it can be easily forgotten causing anxiety to the user. Smart cards usually have a magnetic band which looses much if it's effectively by getting scratches or accumulating dirt and grime. Moreover these card codes can be easily obtained by third party card reading tools and may cause unscrupulous breakage into system and loss of vital information. The main drawback of PKI is the management of the user's private key. To be secure, the private key must be protected from compromise; to be useful, the private key must be portable. The call for the adoption of biometrics is a reasonable one: it is far harder to fake a fingerprint or iris than it is to guess a password, fool a smart card system, or trick a filing clerk into issuing unauthorized documents.

One of the most dangerous security threats is the impersonation, in which somebody claims to be somebody else. The security services that counter this threat are identification and authentication. The verifier can be identified and authenticated by what he knows (password), by what he owns (passport) or by who he is (Biometrics). The current trend in the research world is headed towards Biometrics since the level of security is highly increased. The most popular biometric features are based on individuals' signatures, retinal, faces, iris, fingerprints, hand and voices.

Biometric is the most secure and convenient authentication tool. It can't be borrowed, stolen, or forgotten, and forging one is practically impossible. Biometrics measures individuals' unique physical or behavioral characteristics to recognize or authenticate their identity. Behavioral characters include signature, voice (which also has a physical component), keystroke pattern, and gait. Of this class of biometrics, technologies for signature and voice are the most developed.

The method of analysis of any biometric



system consists of the following sequence of events:

(1) Capture the chosen biometric;

(2) Process the biometric and extract and enroll the biometric template;

(3) Store the template in a local repository, a central repository, or a portable token such as a smart card;

(4) Live-scan the chosen biometric;

(5) Process the biometric and extract the biometric template;

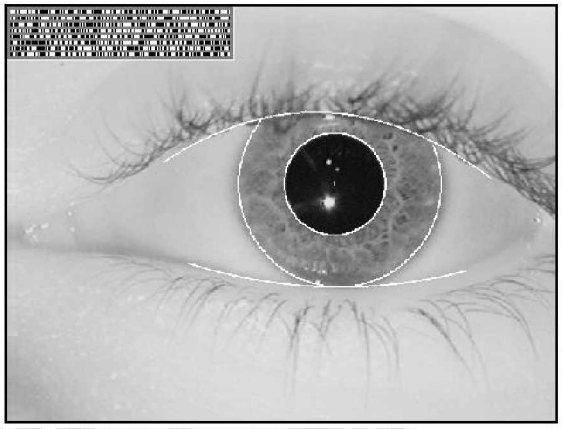
(6) Match the scanned biometric against stored templates;

(7) Provide a matching score to business applications;

(8) Record a secure audit trail with respect to system use.

What is iris recognition?

The human Iris is an internal organ of the eye, protected by the eyelid, cornea and the aqueous humor. It is part of the middle coat of the eye and lies in front of the lens. It is the only internal organ of the body that is normally visible externally. On of its distinctive characteristics is its stability. The iris features remain constant throughout the years. The iris is composed from several layers. Among the visible features of an iris throughout the layers are multiple collagenous fibers, contraction furrows, coronas, crypts color, serpentine vasculature, freckles rifts and pits.



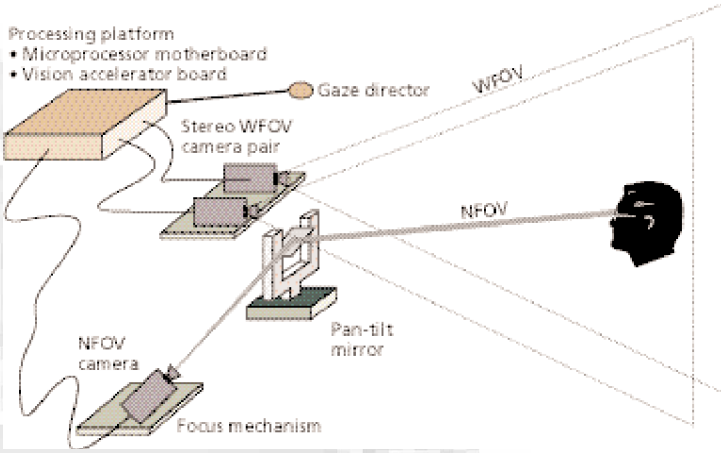
The Iris

In the iris alone, there are over 400 distinguishing characteristics, or Degrees of Freedom (DOF), that can be quantified and used to identify an individual). Approximately 260 of those are used or captured in a "live" Iris Identification application. These identifiable characteristics include: contraction furrows, striations, pits, collagenous fibers, filaments, crypts (darkened areas on the iris), serpentine

vasculature, rings, and freckles. Due to these unique characteristics, the iris has six times more distinct identifiable features than a fingerprint.

In identifying one's iris, there are two types of methods that are used by Iris Identification systems: passive and active.

The active iris system requires the user to move back and forth so that the camera can adjust and focus in on the user's iris. The active iris system method requires that a user be anywhere from six to 14 inches away from the camera. The passive iris system is different in that it incorporates a series of cameras that locate and focus on the iris. The passive iris system allows the user to be anywhere from one to three feet away from the camera(s). This method provides for a much more user-friendly experience (International Biometric Group, 1999).Actual Iris Identification can be broken down into four fundamental steps. First, a person stands in front of the Iris Identification system, generally between one and three feet away, while a wide angle camera calculates the position of their eye. A second camera zooms in on the eye and takes a black and white image. After the iris system has one's iris in focus, it overlays a circular grid (zone's of analysis) on who he is (Biometrics).



Design of the Iris Recognition System

Ophthalmologists originally proposed that the iris of the eye might be used as a kind of optical fingerprint for personal identification. Their proposal was based on clinical results that every iris is unique and it remains unchanged in clinical photographs.

The highly randomized appearance of the iris makes its use as a biometric well recognized. Its suitability as an exceptionally accurate biometric derives from its extremely data-rich physical structure, genetic independence--no two eyes are the same, stability over time, and physical protection by a transparent

window (the cornea) that does not inhibit external view ability.

Conversion of an iris image into a numeric code that can be easily manipulated is essential to its use. This process, developed by John Daugman, permits efficient comparison of irises. Computing *iris codes* requires good-quality iris images that have the customer's iris in focus and properly positioned. Once the image has been obtained, an iris code is computed based on information from a set of Gabor wavelets. These wavelets are specialized filter banks that extract information from a signal at a variety of locations and scales. The filters are members of a family of functions, developed by Dennis Gabor in 1946, that optimizes the resolution in both the spatial and the frequency domain. The iris code is calculated using eight circular bands that have been adjusted to conform to the iris and pupil boundaries, as shown in Figure. Iris codes derived from this process are compared with previously generated iris codes. The difference between two iris codes is expressed as the fraction of mismatched bits, termed a Hamming distance. For two identical iris codes, the HD is zero; for two perfectly unmatched iris codes, the HD is 1. For different irises, the average HD is about 0.5, which indicates a 50 percent difference in the codes. For two different images from the same iris, the HD ranges from approximately 0.05 to 0.1, a variation that includes contributions from video noise as well as variations in the position of the user's eye with respect to imaging optics. Generally, an HD threshold of 0.32 can reliably differentiate authentic users from impostors.

Real World Implementations

Iris recognition is forecast to play a role in a wide range of other applications in which a person's identity must be established or confirmed. These include electronic commerce, information security, entitlements authorization, building entry, automobile ignition, forensic and police applications, network access and computer applications, or any other transaction in which personal identification currently relies just on special possessions or secrets (keys,

cards, documents, passwords, PINs). Unfortunately the implementations are not in widespread use in real world and instead of iris, retinal scanning systems are employed more.

Iris and retinal scanning systems have predominately been implemented in high security access control situations. The military as well as financial institutions make up most iris scanning employments. For instance, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and the National Aeronautical Space Agency (NASA) have all been implementers of iris as well as retinal scanning. Other more recent customers have included the Cook County Prison in Illinois and defense contractor, General Dynamics. Financial institutions have also explored the means of Iris Identification technology. In fact, the English bank, Nationwide, just completed a test pilot of the world's first automated teller machine (ATM) machine equipped with Iris Identification capabilities. Responses from customers were overwhelmingly favorable. Citibank is also in the test pilot stages with Iris Identification technology. Iris identification is gradually gaining popularity and favorable press. Experts predict that the "killer application" for iris identification technology will be e-commerce. Engineers around the world are betting that legal tender in the e-commerce age will be digital certificate combined with a coded image of a person's iris

Constraints

The basic constraint and primary hindrance in Iris Identification is that of user acceptance. Iris identification has several disadvantages including:

- One to one matching of the templates has to be done which is very time consuming especially when the number of identifiable people is more.
- viewed as intrusive and not very user friendly
- high amount of both user and operator skill required
- not enough funding from government and private sectors
- identification system difficult to design.

The biometrics industry includes more than 150 separate hardware and software vendors, each with their own proprietary interfaces, algorithms, and data structures. Standards are emerging to provide a common software interface, to allow sharing of biometric templates, and to permit effective comparison and evaluation of different biometric technologies.

How to increase the efficiency?

We would like to suggest a number of methods which can help in increasing the efficiency and acceptance of the iris recognition system.

The concept of indexing can be employed to increase the overall processing and data matching rate of the system. Efficient searches can be implemented if the iris scan template can be merged with another key such as the hand geometric pattern or finger printing techniques. It would lead to an indexed sorting method to be used and could reduce the search and sort time by magnitudes. Some additional bytes of data would be required to store the hand pattern or finger print template.

Instead of using light rays for taking the grid image of the eye, we suggest that employment of IR waves would produce more efficiency. Presently the light waves which reflect back from the eye use a grid to form the eye template. The IR waves (as used in retina scan) can be projected from the transreceiver which would sense back the change in the intensity of the rays reflected back from the eyes. This would lead to a much simpler design of the Iris Identification device. Even such devices can be formed which a very portable and can be carried around easily.

Further Research

There is a lot of research going on in this field. Scientists are continually trying hard to bring more efficiency and reliability in the present devices. New biometric components are also being sought after. The BioAPI standard released at the conference, defines a common method for interfacing with a given biometric application. BioAPI is

an open-systems standard developed by a consortium of more than 60 vendors and government agencies. Written in C, it consists of a set of function calls to perform basic actions common to all biometric technologies, such as enroll user, verify asserted identity (authentication), and discover identity. Another draft standard is the Common Biometric Exchange File Format, which defines a common means of exchanging and storing templates collected from a variety of biometric devices. The Biometric Consortium has also presented a proposal for the Common Fingerprint Minutia Exchange format, which attempts to provide a level of interoperability for fingerprint technology implementers and vendors.

Biometric assurance, confidence that a biometric device can achieve the intended level of security—is another active research area. Current metrics for comparing biometric technologies, such as the crossover error rate and the average enrollment time, are limited because they lack a standard test bed on which to base their values.

Conclusion

The usage of biometric security is clear in the present world. Among biometrics, the Iris Identification procedures have proved their importance in the field of security be it identification of a person for security checks or for restricting the access. Internetworking this identification technique with the network or the internet can work wonders for data security and passage of information. It is one such attribute which cannot be stolen, hacked, copied or forgotten. This technique is fast, efficient, highly dependable and cost effective. Biometric Security and especially Iris Identification are clearly the building factor of the next generation of information security and identification. They have immense promise and possibilities. We are just getting started and more is still to come.

References:

J.D. Daugman, “High-Confidence Visual Recognition
of Persons by a Test of Statistical Independence,” *IEEE*

Trans. Pattern Matching and Machine Intelligence, Nov.
1993, pp. 1,148-1,160.
L. Flom and A. Safir, "Iris Recognition System," US
Patent 4,641,349, 3 Feb. 1987
J. Daugman, "Biometric Personal Identification System
Based on Iris Analysis," US Patent 5,291,560, 1 Mar.
1994.
D. Gabor, "Theory of communication", *J. Institute of
Electrical Engineers*, Vol. 93, 1946, pp. 429-457.
T.A. Chmielewski, G.A. Vonhoff, and M. Negin, "Compact
Image Steering Device," US Patent 5,717,512, 10
Feb. 1998.
Biometrics, Personal Identification in Networked Society,
A. Jain, R. Bolle, and S. Pankanti, eds., Kluwer Academic
Publishers, Boston, July 1999.

Michael Negin *has a PhD in electrical engineering*

About the authors:

Anupam Singh is a Bachelor's degree student of Computer Science and Engineering at Vellore Institute of Technology, India. He is a student member of the IEEE, ISTE and IEI. His research interests include Human Computer Interfaces, Intelligent Systems, Reverse Engineering and Applied Software Engineering. He can be contacted regarding queries at contact@anupamsingh.cjb.net.

Anupam Das is a Bachelor's degree student of Computer Science and Engineering at Vellore Institute of Technology, India. He is a student member of the IEEE and ISTE. His areas of interest include Artificial Intelligence, Software Re-Engineering and Theory of Computation. He can be contacted at anu_einstein2003@yahoo.co.in.