Principles of Iris Recognition

Security, Personal Identification, & Privacy

Michael Negin, PhD (Vice President, Chief Technical Officer) & Machiel van der Harst (Sales Director , Europe/Middle East/Africa)
Sensar, Inc.; Moorestown, NJ USA

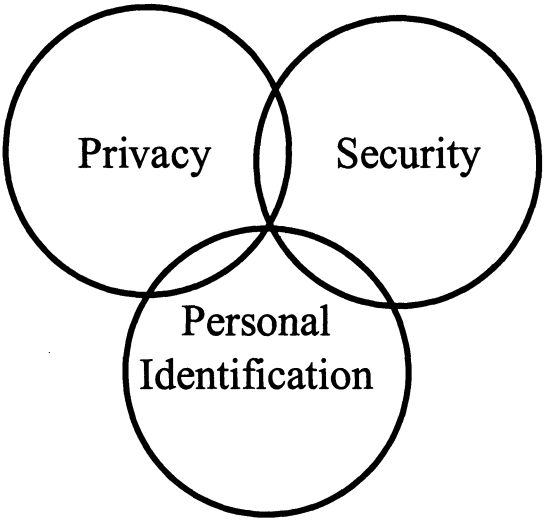
Key words: Iris Identification Biometrics, Unobtrusive Non Habituated Customer Use, Local & Central Identification

Abstract: Iris Identification can provide the linkage between three very important functions in modern transactions: Security of information, Virtually foolproof Personal Identification, and Protection of the Privacy of the individual. This paper will present an overview of the Iris as a means of individual identification with the capabilities of global uniqueness in performance. This physiological capability provides the basis for the three previously mentioned desired attributes that enable secure, private transactions, with the provision of non-repudiation as necessary for certain transactions. This presentation will provide some scenarios where these three functions may operate in concert, and lays the foundation for future development and growth as needs change.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35575-7_19

J. H. P. Eloff et al. (eds.), *Information Security Management & Small Systems Security*

Background:



1. THE IRIS AS A BIOMETRIC

The iris is an integral part of the eye and one of the most unique structures of the human body. Physiological states such as emotion, excitation or stimulation are gauged by the iris.

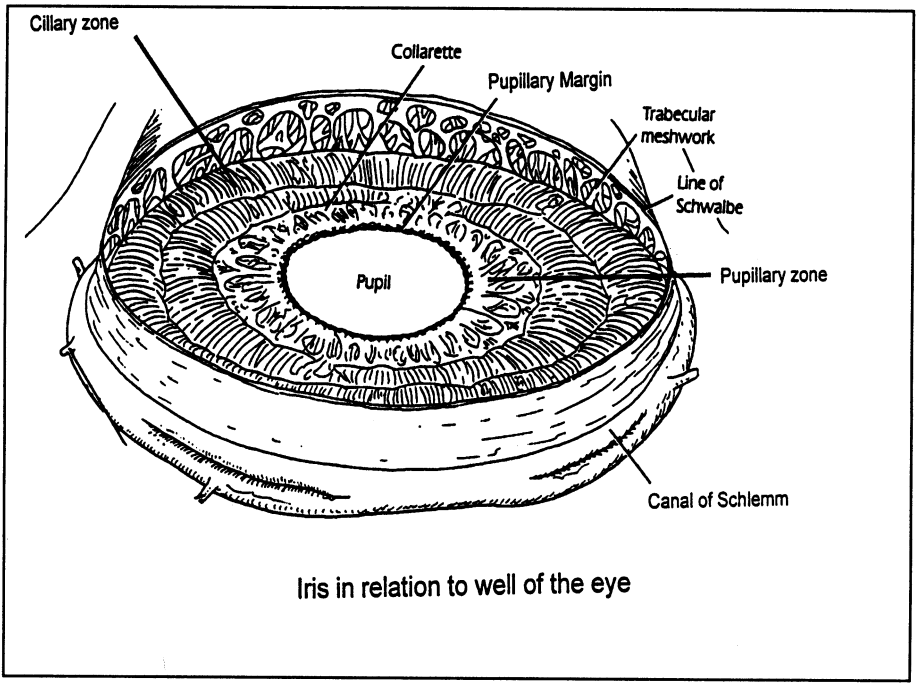
The iris is well suited as a biometric identifier. The eyes are used for tracking manual actions. Thus the iris presents instinctively to the field of attention and gaze that tend to attract a person such as lights and displays or monitors. This natural human response essentially aligns an individual for imaging of the iris through their natural gaze response.

The most distinctive property of the iris which makes it a truly unique biometric identifier is its integral and individual anatomy. The iris is a readily visible yet totally internal and extremely delicate structure of the human body. Its surface topography is highly detailed; composed of multiple crypts and furrows unique to each individual. By childhood, the iris has grown to its full size. The surface topography, except for rare

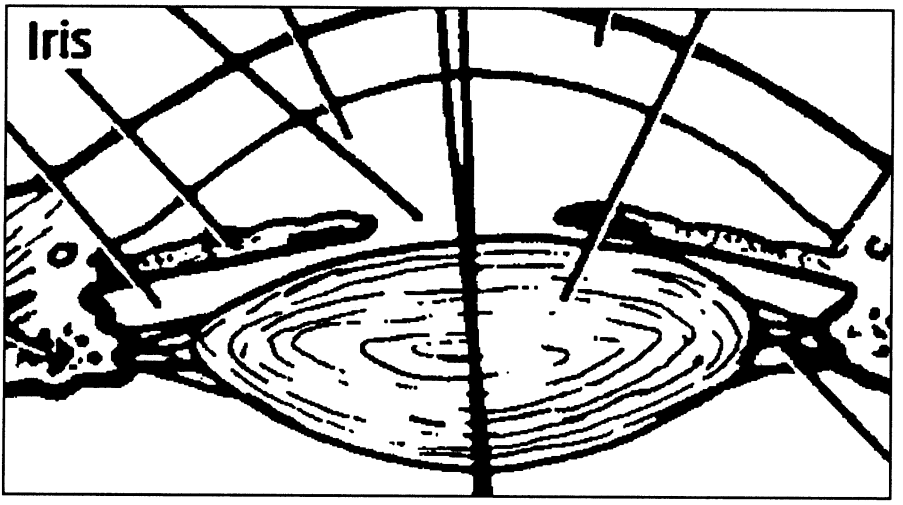
anomalous conditions and trauma, remains constant. The iris is the pupillary diaphragm positioned behind the cornea; that clear anterior 1/6 surface of the eye which allows visualisation of the internal structures. A distinctive light reflection is associated with the corneal surface. The peripheral border of the iris is readily seen in distinct contrast with its outlining white sclera. These definitive borders permit easy location for imaging analysis.

The iris surface and structure itself is composed of many contours, depressions and substructures which in effect allow it to be used as an excellent biometric or "optical fingerprint" for personal identification. The use of this anatomical structure was in fact suggested several years ago by ophthalmologists and even as early as over a hundred years ago by the forefathers of criminology. As noted in the enclosed sectional diagram of the human eye, the iris is an extremely delicate structure and located reasonably interior (see figure, Perspective Schematic of the Iris). Modification of the iris by any reasonable means would mean extremely intricate microsurgery. Fraudulent manipulation could result in drastic visual jeopardy to the individual and an obvious enough variation of topography and morphology to be easily detectable by visual means including image analysis. Furthermore, the individual's iris would not have a normal reactive or possibly symmetric reflex to light and because of possible alterations in the flow of the anterior chamber aqueous fluid there could also be risk to the eye from glaucoma.

The formation of the iris is a genetic expression that determines form, physiology, colour and general appearance. This detailed and intricate embryogenesis depends only on the initial conditions of the three present embryonic layers. Thus identical twins having the same genotype will express uncorrelated minutia in their irises with a uniqueness in each individual. This is not only seen in the fact the identical twins have un-identical irises, but also within the same individual where the right iris differs from the left iris, while both irises have totally identical genetic makeup. In this respect, the iris parallels that uniqueness and individuality that is inherent to every fingerprint, but incorporates a much greater amount of topographic knowledge.



Perspective Schematic of the Iris



Side View of the Iris

2. PERSONAL IDENTIFICATION

Because of the random appearance of the iris, its use as a biometric is well recognised. The conversion of an iris image into a code that can be easily manipulated mathematically is vital. This process has been reduced to practice by Professor John Daugman, a world renowned computer scientist at Cambridge University, UK. This encoding and comparison process is licensed from IriScan, Inc. (Marlton, NJ, USA), and permits the very efficient matching of irises among individuals.

Statistical analysis on the encoding and comparison of irises shows that the iris is a very discriminating biometric, with an equal error rate between False Reject Rate and False Accept Rate of approximately one in 1.2 million. The power of the iris as a personal identification technique is so great that it has the capability of being used in very large database recognition applications.

In summary, the key features of the iris for use in Personal Identification are:

- Iris
  1. Extremely data rich physical structure
  2. Very stable over time
  3. Externally viewable
  4. Not genetically dependent (no two eyes are the same)
- Rich feature set
  1. Wavelet coding of the iris yields 266 independent measurements
  2. 2,048 bit IrisCode (only ~1,000 bits need to match for practical use)
- Accuracy
  1. Extremely Low False Reject and False Accept Rates
  2. Low crossover equal error rate (1:1,200,000)
- Unobtrusive customer use
  1. Non Contact
  2. Requires very little habituation
- Verification (1:1) or Identification (1:many)

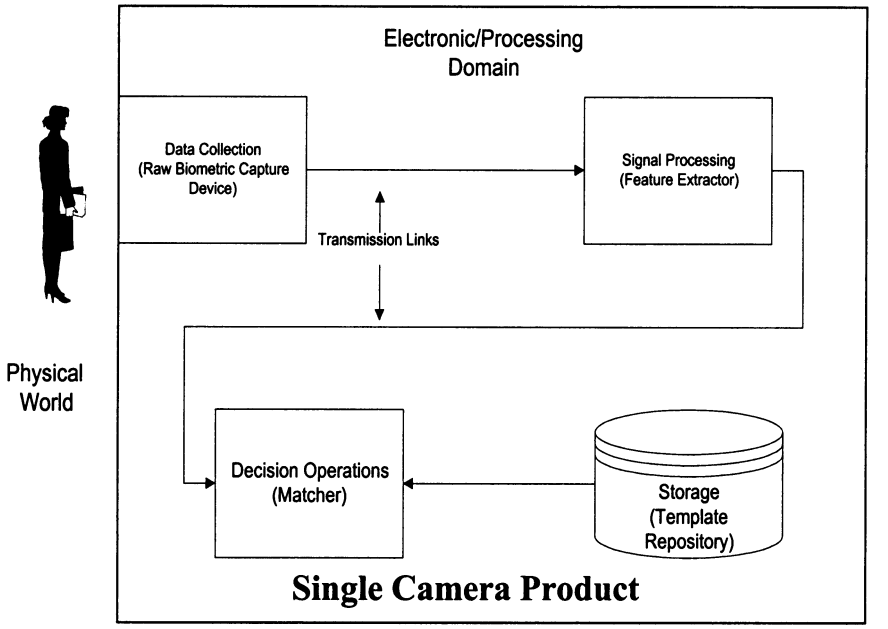
3. SECURITY

From a Security perspective, the iris fits naturally into most standard security contexts. The example given here is for an ANSI Standard that is under development. The iris code is essentially transparent to standard encryption techniques as used in networks so that the iris technology will naturally migrate with advances in encryption and security technology.

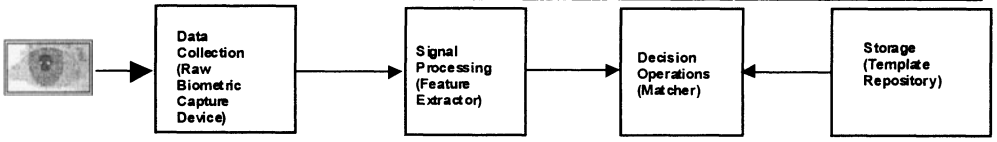
The two figures below show how the iris can be easily integrated into standard security architecture.

The first figure shows this integration into a developing ANSI X9.84 protocol. The second figure shows how Sensar's single camera product can be made congruent with this architecture.

Biometric System Security Context
(per ANSI X9.84 Standard in development)



Domain	Physical	Data Collection (Sensor)	Data Collection to Feature Extractor Link	Feature Extractor	Feature Extractor to Match Link	Matcher	Matcher-Store Link	Store
Techniques (Prototype)	Live Eye Detect	None	Secure Sockets Layer (SSL V3) 128 Bit U.S. Non U.S. via Permit Process	Runs in Centralized Server with Physical and Logical Access Controls	None Needed - Connected Modules Reside in Same Physical Device	Runs in Centralized Server with Physical and Logical Access Controls	Runs in Processor in Same Physical Facility as Matcher over Private Network	Stored Encrypted using Entrust Toolkit Symmetric Key - 128 Bit Triple DES (U.S.) Selectable Key Length Password authentication of matcher modules to Database Store
Techniques (Final Product)	Live Eye Detect	Sensor Hardware-based Video Signing and Replay Prevention	Secure Sockets Layer (SSL V3) TBD Bit Key Length (U.S.) Non U.S. via Permit Process	Runs in Centralized Server with Physical and Logical Access Controls Digitally Signed Executables (optional)	None Needed - Connected modules reside in same physical device	Runs in Centralized Server with Physical and Logical Access Controls Digitally Signed Executables (optional)	Runs in Same Physical Facility as Matcher over Private Network	Stored Encrypted using Entrust Toolkit Symmetric Key Selectable Key Length Mutual Authentication of Matcher/Store Modules



4. PRIVACY

The question of privacy and the impact that biometrics have on privacy is one open to vigorous debate. Many parties believe that the use of biometrics bring the "big brother" scenario closer to reality. The other side of the equations suggests that theft of identifies and the concomitant personal property loss is of equal concern. There is no question that the use of a well performing biometric can greatly alleviate the concerns and risk associated with identity theft. Of course, since a high performance biometric can be used for high reliability identification, the question of covert tracking or interference with one's private affairs must be raised. Of course, other public identification means such as credit cards, drivers licenses, identity cards, can also be used to track purchases and activities, but in general society seems to tolerate those as a fact of life. The use of a biometric can be used to **enhance privacy**, since identification on-line (e.g., the use of the Internet) can be highly encrypted at the source and decrypted at the destination so that

interception of the encrypted transaction would be very difficult to decipher to the extent that it probably wouldn't be worthwhile for the vast majority of transactions. This engenders the concept of a "transient alias" that could be assigned to a specific transaction for a short time (e.g., a few seconds), and then that "transient alias" would evaporate. In this fashion, the biometric would not only ensure the **identification** of the correct individual, and provide a **secure** transaction, but would actually improve the **privacy** of the individual.

In the final analysis, the customer must demand and the vendor must provide the mechanism so that concepts such as "transient alias" are provided. The biometric provider must provide the framework for these protections (as Sensar is doing) but the onus rests on those who manage the **USE** of the biometric (the customer and vendor) to require the safeguards. Biometrics fundamentally do not violate those safeguards. There will always be challenges to privacy, and it is the responsibility of the providers and users to jointly agree on the management of the technology so potential abuses are designed out of the system.

5. REFERENCES

1. "Biometric Personal Identification System Based on Iris Analysis." U.S. Patent No. 5,291,560 issued March 1, 1994 (J. Daugman).

2. J. Daugman (1998) "Recognizing persons by their iris patterns." In: Biometrics: Personal Identification in Networked Society. Amsterdam: Kluwer, pp 103-121.

3. M. Negin, M. Salganicoff "Consumer Friendly Iris Recognition using 3-D Vision Technologies", 11th Biometric Consortium Meeting, September 22, 1998

4. http://www.sensar.com/

5. http://www.iriscan.com/

6. http://www.nationwide.co.uk/whatsnew/Iris.htm