Iris Recognition Technology

Gerald O. Williams — *Iridian Technologies, Inc.*

Abstract

Iridian Technologies, Inc. (formerly IriScan, Inc.) has developed a biometric identification system capable of positively recognizing individuals without physical contact or human decision-making. Personal identification has historically been based on what a person possesses (a card); knows (a Personal Identification Number, or PIN); or is (an inherent physiological or behavioral characteristic). Facial features (both infrared signatures and geometry), fingerprints, hand geometry, vein patterns, retinal patterns, voice patterns, and signature dynamics have all been explored as biometric identifiers with varying levels of success. All but voice and facial identification require contact or have been characterized by some as invasive or intrusive in some other way. Many have suffered from high cost and unsatisfactory error rates. This new technology, using the unique patterns of the human iris, overcomes previous shortcomings and provides positive recognition of an individual without contact or invasion, at extremely high confidence levels.

The video-based system locates the eye and iris, evaluates the degree of occlusion by eyelid and specular reflection, determines the quality of image focus, and determines the center and boundary of the pupil and the limbus (outer edge of the iris) for processing. The features of the iris are then measured and encoded into a 512 byte IrisCode® record for enrollment or recognition. The resulting IrisCode record is compared to each and every IrisCode record enrolled in the database for recognition. Computations and decisions are accomplished at extremely high rates of speed, resulting in processing times of less than two seconds.

The process is based on the unique nature and the extreme richness of the human iris. The multiple contraction furrows, collagenous fibers, crypts, coronas, striations, serpentine vasculature, freckles, rifts, and pits produce a non-duplicable organ with complexity on the order of 240 degrees-of-freedom (DOF). This endemic and largely invariant complexity allows proprietary algorithms to create a code, which can be compared to an entire database in milliseconds, producing a positive recognition with "imposter odds" averaging 1 in 10^{48}. Six years of operational experience in sensitive and demanding environments has demonstrated the practicality of a recognition technology that is being even more widely accepted as imaging platforms become increasingly compact and inexpensive.

INTRODUCTION

Background

Personal identification has historically been based on what a person possesses (a letter of introduction, perhaps), knows (a secret password), or is (personal recognition). In today's security industry, possession has become an encoded card, knowledge equates to knowing one's Personal Identification Number (PIN), and personal recognition has given way to the measurement and comparison of physiological and behavioral characteristics — a process known as biometric identification. Various human features have been used as the basis for such measurement and comparison. These include fingerprints, palmprints, hand geometry, vein patterns, facial characteristics, and capillary patterns in the retina. Additionally, behavioral characteristics such as signature dynamics, voice patterns, and keystroke dynamics have been used for verification. Many of these require contact or are perceived as invasive or intrusive. Others require a person to make a final judgment or are costly, or suffer from unsatisfactory error rates.

Iridian Technologies, Inc. has developed an automated Iris Recognition Technology (IRT) capable of positively identifying persons without physical contact or real-time human decision-making. This technology, for which Iridian Technologies holds many U.S. and international patents, meets this challenge without the drawbacks exhibited by other technologies mentioned above. In addition to developing a commercially viable recognition system for industrial application, Iridian Technologies has developed systems for use by the U.S. government, correctional facilities, nuclear utilities, banks, and now, E-commerce and computer workstation security. This paper is intended for security practitioners who are knowledgeable, but not technically or scientifically oriented. Reference (1) is intended for the more technically or scientifically oriented readers.

Caveats

Iris recognition technology and the Iridian Technologies process are not associated with, or in any way similar to, retinal (capillary) pattern recognition. The iris is the externally visible, colorful, donut-shaped organ surrounding the pupil of the eye. The retina is the hemispherical organ behind the cornea, lens, iris, pupil, and vitreous humour and is not readily visible. The Iridian Technologies process captures a video image (takes a video picture, if you will) of the iris, externally visible behind the eye's cornea; whereas the retinal scan process scans the fovea, or innermost surface of the eye, the retina.

Iridian Technologies' iris recognition systems truly recognize individuals, doing an exhaustive, one-to-many search of an entire database without benefit of PIN, password, or token. Most other biometric technologies rely on verification, where card or PIN inputs are required to pre-select a single enrolled file for a one-on-one comparison.

BASIS OF THE TECHNOLOGY

Features of the Iris

The human iris is rich in features which can be used to quantitatively and positively distinguish one eye from another. The iris contains many collagenous fibers, contraction furrows, coronas, crypts, color, serpentine vasculature, striations, freckles, rifts, and pits. Measuring the patterns of these features and their spatial relationships to each other provides other quantifiable parameters useful to the identification process. In practical terms, statistical analyses indicate that the Iridian Technologies IRT process uses 240 degrees-of-freedom (DOF), or independent measures of variation to distinguish one iris from another. The availability of this many degrees of freedom allows iris recognition to identify persons with an accuracy that is orders of magnitude greater than other biometric systems.

Uniqueness of the Iris

The iris is unique because of the chaotic morphogenesis of that organ. To quote Dr. John Daugman (Reference 1), "An advantage the iris shares with fingerprints is the chaotic morphogenesis of its minutiae. The iris texture has chaotic dimension because its details depend on initial conditions in embryonic genetic expression; yet, the limitation of partial genetic penetrance (beyond expression of form, function, color and general textural quality), ensures that even identical twins have uncorrelated iris minutiae. Thus the uniqueness of every iris, including the pair possessed by one individual, parallels the uniqueness of every fingerprint regardless of whether there is a common genome." Given this, the statistical probability that two irises would be exactly the same is estimated at 1 in 10^{72}.

Stability of the Iris

Notwithstanding its delicate nature, the iris is protected behind eyelid, cornea, aqueous humor, and frequently eyeglasses or contact lenses (which have negligible effect on the recognition process). An iris is not normally contaminated with foreign material, and human instinct being what it is, the iris, or eye, is one of the most carefully protected organs in one's body. In this environment, and not subject to deleterious effects of aging, the features of the iris remain stable and fixed from about one year of age until death.

Natural Protection from Artifice

The human eye has physiological properties that can be exploited to impede use of images and artificial devices to spoof the system. As a matter of policy, Iridian Technologies, Inc. does not discuss the details of these properties or specific countermeasures in the open media.

PROCESSING

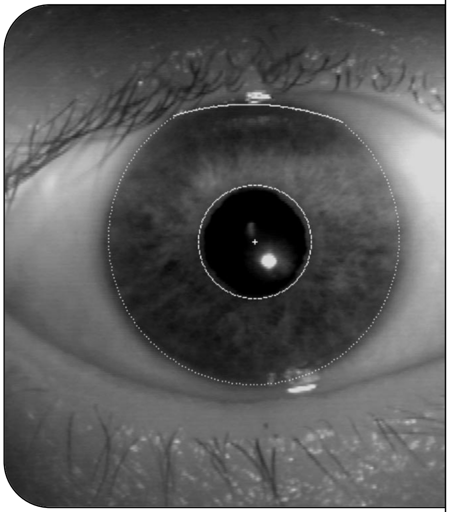

Figure 1 — Processing Zone

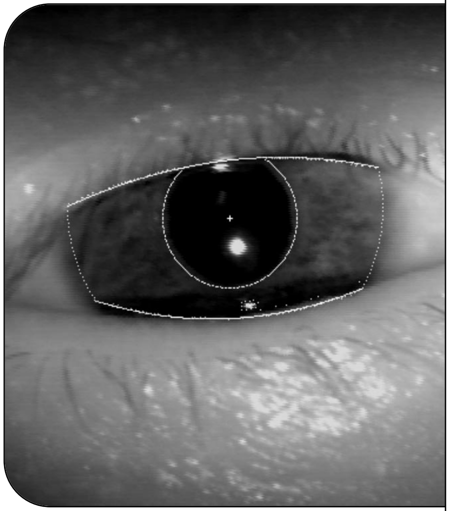

Figure 2 — Field Optimization

Image Acquisition

Optical platforms designed and optimized for specific iris recognition applications allow image acquisition at distances from 3.5" to nearly one meter. In its simplest functional configuration, an optical unit acquires multiple images of the presented iris through a simple lens, a monochrome CCD camera, and a frame grabbing board. Multiple low level LEDs operating in the 720 to 850 nanometer range provide illumination over the focal range of the camera. User alignment in the X, Y, and Z axes is aided by a combination of mirrors, audible verbal direction, and in some cases, zoom or auto-focus lenses. In some models, a range finder, initiates the process automatically when a subject approaches within 18" of the unit.

Iris Definition

The image that best meets the focus and detail clarity requirements of the system is then analyzed to locate the limbus (the outer boundary of the iris that meets the white sclera of the eye), the nominal pupillary boundary, and the center of the pupil (see Figure 1). The precise location of the circular iris has now been defined and processing can take place.

Field Optimization

The system quickly defines the suitable usable area of the iris for feature extraction and analysis. Using algorithms that exclude areas covered by eyelids, deep shadow, specular reflection, etc., it concentrates its feature-extraction power in those areas most visible (Figure 2). A dynamic feature of the system automatically adjusts the width of the pupillary boundary-to-limbus zone in real time to maximize the amount of iris analyzed, given varying ratios of pupil to iris sizes. Elimination of marginal areas has little negative impact on the analysis process. In actual practice, excellent enrollments and subsequent recognitions are obtained with 40% or less of the iris available for analysis. Feature locations and dimensions are defined using a polar coordinate (as opposed to a Cartesian, X, Y) system.

Image Analysis

The features of the iris are then analyzed and digitized into a 512 byte (4096 bit) IrisCode record, half of which describes the features, half of which controls the comparison process. During enrollment, this IrisCode record is stored in the database for future comparison. During a recognition attempt, when an iris is presented at a recognition point, the same process is repeated; however the resulting IrisCode record is not stored, but is compared to every file in the database.

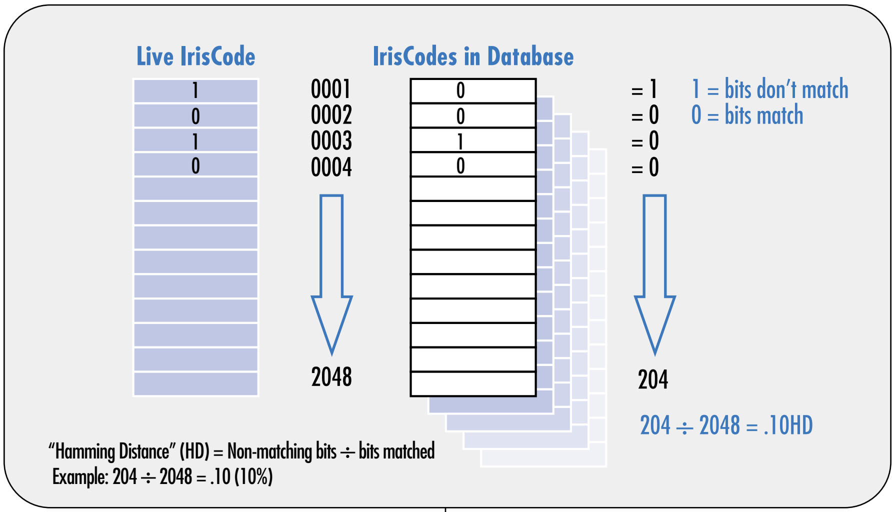

Figure 3 — HD Calculation

Hamming Distance Calculation

Comparison of IrisCode records includes calculation of a Hamming Distance (HD), as a measure of variation between the IrisCode record from the presented iris and each IrisCode record in the database. Each useable pair of the 2048 available pairs of bits is compared (Figure 3), and a value assigned using exclusive-OR logic. (The total 2048 pairs are seldom compared in their entirety, because of the field optimization process described above.) Bit #1 from the presented IrisCode record is compared to bit #1 from the reference IrisCode record, bit #2 from the presented IrisCode record is compared to bit #2 from the reference IrisCode record, and so on. If two bits are alike, the system assigns a value of zero to that pair comparison. If two bits are different, the system assigns a value of one to that pair comparison. After all pairs are compared, the number of disagreeing bit-pairs is divided by the total number of bit-pair comparisons resulting in a two digit quantitative expression of how different the two IrisCode records are. A Hamming Distance of .10 means that two IrisCode records differed by 10%.

Recognition or Rejection

Millions of IrisCode record comparisons have defined the Frequency Distributions (Probability Densities) in Figure 4. Here, the mean imposter Hamming Distance is near 0.5, which is what one would expect in a truly random relationship (flipping a coin many times and noting the occurrence of heads versus tails). Conversely, the mean value for authentics is 0.08 (or 8%). Another key aspect of the Frequency Distributions is the very small Standard Deviation (amount that scores deviate from the mean), resulting in very tightly clustered HD scores for both impostors and authentics. These two "spikey" distributions appear, visually at least, to be discrete (totally separate). Mathematically, however, the adjacent slopes cross, and at that point, a nominal Accept/Reject decision threshold can be established. At Hamming Distance (.342), the probability of a False Reject is approximately the same as the probability of a False Accept. That setting reflects a conscious decision that an IrisCode differing by more than .342 (34.2%) from the codes with which it is compared, is likely to be part of the Imposter Frequency Distribution because it is approaching a random relationship with the compared code. Another way of stating the relationship between the presented and the referenced IrisCode record is that if they differ

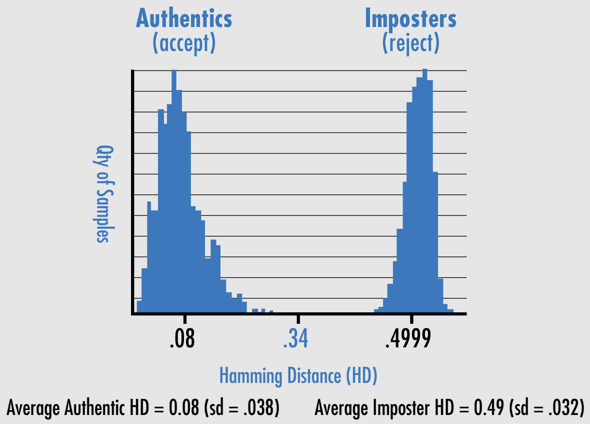

Figure 4 — Recog/Reject

HD	False Accept Probability	False Reject Probability
.28	1 in 10^{12}	1 in 11,400
.29	1 in 10^{11}	1 in 22,700
.30	1 in 6.2 billion	1 in 46,000
.31	1 in 665 million	1 in 95,000
.32	1 in 81 million	1in 201,000
.33	1 in 11 million	1in 433,000
.34	1 in 1.7 million	1in 950,000
.342	1 in 1.2 million	1 in 1.2 m
.35	1 in 295,000	1 in 2.12 m
.36	1 in 57,000	1 in 4.84 m
.37	1 in 12,300	1 in 11.3 m

— Table 1 —
Hamming Distances & Error Probabilities

by 34.2% or more, they are considered to have emanated from different irises. Sophisticated algorithms have been developed to adjust automatically that threshold based on number of bit-pairs available for comparison and the size of database.

Obviously, in the recognition mode (requiring an exhaustive database search), this decision process must be applied to each of the stored files before rejection of an individual. Rejection of an individual occurs only after rejection of all stored files (normally less than two seconds). In the extremely rare case that more than one IrisCode record in the database varies from the presented IrisCode record by less than .342, recognition occurs by selecting the best match (lowest Hamming Distance). As in any biometric, as one forces the threshold lower, the likelihood of a False Reject increases (although, as one can see from Table 1, even with dramatic reduction of the Hamming Distance threshold, the probability of False Reject is markedly smaller than with most biometric systems available today).

PERFORMANCE

Crossover (Equal) Error Rate (CER)

At present, a crossover error rate is estimated based on the point at which the Impostor and Authentic distributions cross. The Iridian Technologies' (theoretical) crossover error rate is .0000008, or 1 in 1,200,000 (Note Table 1). This would equate to a Hamming Distance of just under .342. This is an extremely conservative statement about an error rate, because in many comparisons over time, recognition HDs average 0.08, where the probability of a False Accept is 1 in 10^{48}.

Recognition Speed

The speed of the recognition process is determined by many interacting variables, the speed of the processor and size of the database being the two most obvious. Databases containing millions of IrisCode records have been searched in seconds. Faster processors have kept recognition speeds in the 2–3 second range, even with large databases.

Enrollment

Most enrollments, including administrative data entry, verification of the recognition capability, and training the subject, can be accomplished in about two minutes. Some have occurred in less than a minute, and some have exceeded two minutes where focus difficulties or other enrollment parameters dictated a second iris image acquisition. Nearly all users were proficient enough after enrollment to perform subsequent recognitions without additional instruction or assistance. Enrollees who are not required to accomplish recognition without a system operator present, such as inmates in correctional institutions, need no special orientation.

Proximity

Currently, subjects in an access control or corrections applications typically stand between 8 and 12 inches from the Optical Unit. ATMs operate at nearly one meter, and computer workstation systems operate with the subject 17 to 19 inches from the Optical Unit. The distance is primarily a function of lens design and illumination.

Other

As a practice, subjects are asked to remove eyeglasses during enrollment to acquire the clearest enrollment image possible. However, contact lenses need not be removed. Thereafter, subjects can generally be recognized through eyeglasses or contact lenses. Colored contact lenses do not affect the enrollment/recognition process. Most sunglasses pose no impediment to recognition.

Confidence

The promise of the iris recognition technology described herein has been established based on millions of file comparisons with extraordinary accuracy. System problems almost exclusively reflect lighting, focus or image degradation issues. Having analyzed formally 12 separate databases totaling more than a million scores in accordance with recognized principles of statistical decision theory, one can say with 99% confidence that the values established for the Hamming Distances of authentics and impostors in Figure 4 are within 9% of the whole (infinite) population.

Although published Crossover Error Rates are "worst case" (that is, the worst possible score achievable that still qualifies as a match), the Hamming Distance for the average authentic comparison in the authentic Frequency Distribution of Figure 4, equates to imposter odds of 1 in 10^{48}. Another way of stating this is that following a recognition decision based on a Hamming Distance of .08, the probability that the recognition was wrong is an extraordinarily low .000000000000000000000000000000000000000000000001.

Testing

Extensive testing, under Defense Special Weapons Agency (DSWA), [Formerly Defense Nuclear Agency (DNA)], in multiple Beta test facilities and at Iridian Technologies' own facilities has confirmed the following:

- The system effectively and accurately performs recognition and verification with a False Accept rate of 0,
- The system effectively and accurately rejects impostors and persons not enrolled,
- Virtually all subjects with at least one functioning iris are capable of being enrolled,
- The user alignment, accept/reject light and audible signal systems worked effectively and reliably, without negative comment by users,
- Dark eyes were handled with virtually identical speed and accuracy as lighter colored eyes.

Detailed test results are contained in the two test-related references at the end of this paper. Non-quantified Beta testing validated form, fit, and function of iris recognition technology as follows:

- User reaction to the system was overwhelmingly positive. On a scale of 1-10:
  - – Average ease-of-use rating was 9,
  - – Average user-friendliness rating was 9,
  - – Average system speed rating was 8,
  - – Average rating on willingness to use the technology was 7.
- Learning curves did not affect the performance of the system. Once enrolled, there was no statistically significant performance difference between those enrollees who used the system 10 times or more and those who used the system less than 10 times.

- Subjective comments included:
  - – "We could do away with ID cards."
  - – "This is a quicker process."
  - – "Allows for stricter access control."
  - – "You can't lock yourself out."
  - – "Stolen ID cards can't be used"
  - – "It's better than a badge."

- System reliability was 100%. There were no failures with all systems running 24 hours per day for the duration of the Beta test.

Lessons Learned from All Testing to Date

Although control of ambient lighting is still a matter of some importance in operational applications, the units experienced no difficulty in operating in any of the lighting environments encountered during any phase of testing or demonstration.

User acceptance was excellent. Under a variety of lighting conditions, users were able to clearly and simply see the image they should expect to see when they approached the unit. Most initial orientations required less than 30 seconds to train subjects on how to acquire a proper image. Enhancements to earlier models consisting of voice instruction and zoom or auto-focus lenses provided an immediate feedback mechanism to even presbyopic individuals.

Iridian Technologies systems have enrolled 99.99% of the irises presented to them.

The Iridian Technologies iris recognition system has allowed no False Accept errors in over three million file comparisons during the two testing programs referenced in this paper, and in millions of file comparisons elsewhere. Under the formal, controlled DOD testing scenario, the system was 99.95% accurate in the area of False Rejects, with only one False Reject out of 1,995 trials. The reason for that error was identified, corrected and never repeated.

Conventional contact lenses (clear or tinted) pose no problem to either enrollment or recognition. Enrollment without contacts can be followed by recognition with the lenses, and vice versa, without impacting accuracy or speed. Similarly, the system handles imprecisely positioned lenses (not in same exact position on the eye every time) and colored contacts without difficulty.

Dirty and scratched glasses cause blooming that can interfere with recognition if not consciously and effectively avoided by subjects. We identified techniques, which can be applied by virtually anyone to easily move blooming to an area that will not affect the recognition process.

An ancillary lesson from the foregoing is that False Rejects can be made to happen in many ways and that an operational False Reject Rate may well be a function of factors beyond the control of any biometric system or manufacturer. The degree to which subjects want to make the system operate can influence Type I errors. The attentiveness of subjects, their concentration, and their preoccupation with other things in the environment and/or their lives, may well induce higher Type I error rates than the system is technically capable of. In short, a poorly presented biometric feature, which exceeds the system design parameters, increases the probability of being rejected.

Absence of training and initial user orientation may lead to unnecessary rejections. The vast majority of enrollees require only moderate direction to see their iris image in the unit's aperture. A small percentage of enrollees, however, experience some initial difficulty. This is particularly true of older persons, or persons with no dominant eye. Once the image is acquired, they are enrolled as easily as any other person. In these special cases, some practice (five or ten image acquisitions) under the tutelage of a qualified system operator is required to enable the enrollee to easily acquire an iris image without assistance.

CONCLUSIONS

Highly accurate, positive personal recognition is feasible today using the iris of the human eye. This unique and complex organ, which has more dimensions (measures) of variation than any other biometric feature currently in use, remains stable throughout a lifetime and is readily available for sampling in a non-intrusive way. The process uses simple and non-threatening video technology to take images of the iris, digitize the features, and create a 512-byte code, which is then compared against an entire database in less than two seconds. Recognitions can then be used to control access and entry, to provide recognition information to an existing entry control system, or for any other purpose where positive identification is needed. Recent testing, under U.S. Government controlled conditions, in three real-world environments, and in a variety of operational applications have proven the practicality and feasibility of the extremely accurate iris recognition for any function requiring positive recognition.

References:

[1] *J. G. Daugman, Ph.D., "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, vol. 15, No. 11, November 1993.*

[2] *DNA Report, DNA-TR-95-18, Biometric Recognition/Verification Brassboard Proof-of-Concept-System, Phase II, December 1995, Contract No. DNA 001-93-0137, available through the National Technical Information Service (NTIS), Springfield, VA, (703) 487-4650.*

[3] *Sandia Report, SAND 96-1033, April 1996, Laboratory Evaluation of the IriScan Prototype Biometric Identifier, available through Entry Control/Systems Engineering Department, Sandia National Laboratories, Albuquerque, NM 87185.*

1/2/01 12:26 PM

iridian™
technologies

Authentication solutions for a new economy™

Iridian Technologies, Inc.
Moorestown, NJ, USA

1-866-IRIDIAN
www.iridiantech.com