# Iris Recognition Technology

**Gerald O. Williams**
*IriScan, Inc.*

## ABSTRACT

IriScan Inc. has, for the past three years, been developing an identification/verification system capable of positively identifying and verifying the identity of individuals without physical contact or human intervention. Facial features, fingerprints, hand geometry, vein patterns, retinal patterns, voice patterns, and signature dynamics have all been explored as biometric identifiers with varying levels of success. A new technology, using the unique patterns of the human iris, shows promise of overcoming previous shortcomings and providing positive identification 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 spectral 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 iris is zoned, and the features therein measured and encoded into a 256-byte (2048 bit) IrisCode for enrollment or identification. The presented biometric is compared to an extensive database for identification, or to a referenced IrisCode for verification. 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 extreme richness of the human iris. The multiple features produce a non-duplicable organ with more than 400 degrees of freedom, or measurable variables. The IriScan process typically uses about 200 of these to create a code which can be compared to an entire database in milliseconds, producing a positive identification with "imposter odds" as high as 1 in $10^{34}$.

## 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 physiological and behavioral characteristics known as biometrics. Various human features have been used as the basis for biometric measurement. These include fingerprints, palmprints, hand geometry, vein patterns, facial characteristics, and capillary pattern in the retina. Additionally, behavioral characteristics such as signature dynamics, voice pattern, and keystroke dynamics have been used for identification or verification. Many of these require contact or are perceived as invasive or intrusive. Others require a person to make a final judgement, or are costly, or suffer from unsatisfactory error rates.

IriScan Inc. has, for the past three years, been developing an automated identification/verification system capable of positively identifying and verifying without physical contact or human intervention. The iris identification technology, patented by IriScan, shows promise of meeting this challenge without suffering many of the inadequacies exhibited by the technologies mentioned above. In addition to developing a commercially viable identification system for industrial

Author's Current Address:
IriScan, Inc., 133-Q Gaither Drive, Mt. Laurel, NJ 08054.

Based on a presentation at the 1996 Carnahan Conference.
0885-8985/97/ $10.00 © 1997 IEEE

application, IriScan completed development of a brassboard model for use by the Department of Defense (DoD). This paper attempts to summarize the development of iris identification technology 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 identification technology and the IriScan process are not associated with, or in any way similar to retinal (capillary) pattern recognition. The iris is the colorful donut-shaped organ surrounding the pupil. The retina is an internal organ behind the cornea, lens, iris, and pupil. The IriScan process captures video images of the external iris, while the retinal scan process scans the innermost surface of the eye near the fovea.

Unlike most biometric systems today, the IriScan system operates primarily in the identification (recognition) mode where the code from the presented iris is compared with each file in the database to determine identity. (Colloquially described as "one-on-many.") The IriScan system can optionally operate in the verification mode (where card or PIN inputs are used to select and compare against a single enrolled file), because of its inherent speed of operation.

## 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 from another. The iris contains multiple collagenous fibers, contraction furrows, coronas, crypts, color, serpentine vasculature, striations, freckles, rifts, and pits. Further, measuring the spatial relationship and patterns of these features provides other quantifiable parameters useful to the identification process. In all, there are some 450 Degrees of Freedom (DoF) on which to base a statistical analysis and comparison. In practice, when all conjunct features are excluded, 200 or more DoF are useable in the IriScan comparison process. This is three to four times the number available to conventional fingerprint identification systems.

### Uniqueness of the Iris

The iris is unique because of the chaotic morphogenesis of that organ. To quote Dr. John Daugman, [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 identical by random chance is calculated at approximately 1 in $10^{52}$.

### 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 identification process). A normal iris is usually lubricated, not contaminated with foreign material, and instinctively, one of the most carefully protected organs in one's body. Additionally, the features of the iris, their placement, size, shape, and orientation remain stable and fixed from about one year of age throughout life.

### Natural Protection from Artifice

The iris has physiological characteristics which can be exploited to insure that reproductions of a human iris cannot be used to fool the system. One of these is known as pupillary unrest, the autonomic response of the eye to light variations that are so minute and rapid that they fall below our level of consciousness. An additional "live eye" test is the response of the pupil to light pulses detected by the eye either directly into the eye being presented (primary reflex) or the free eye (consensual reflex). Finally, there is a complex interaction of reflections and refractions which occurs in the human eye producing measurable "Purkinji images" which distinguish a live eye from a non-human representation of an eye.

## PROCESSING

### Image Acquisition

The optical platform of the iris identification system acquires multiple images of the presented iris through a simple lens, a monochrome CCD camera, and a frame grabbing board. A low-level tungsten halogen illuminator (28 watts, operating at 7 watts, from .1 to 1.2 microns at 3200°k) provides illumination approximately 14" from the lens (9" from the front of the optical platform), and a liquid crystal display with beam splitter provides feedback through the lens to aid the user in alignment. There is a diamond shaped reflection in the pupil which shrinks to a dot as the user approaches the optimum focal point, which acts as a secondary aid to user alignment and image acquisition.

### Iris Definition

An iris image which meets the focus and detail clarity requirements of the system is then analyzed to locate the limbus (the outer boundary of the iris, where it meets the white sclera of the eye, see Figure 1, on next page), the nominal boundary where the circular pupil meets the iris, and the center of the pupil. The precise

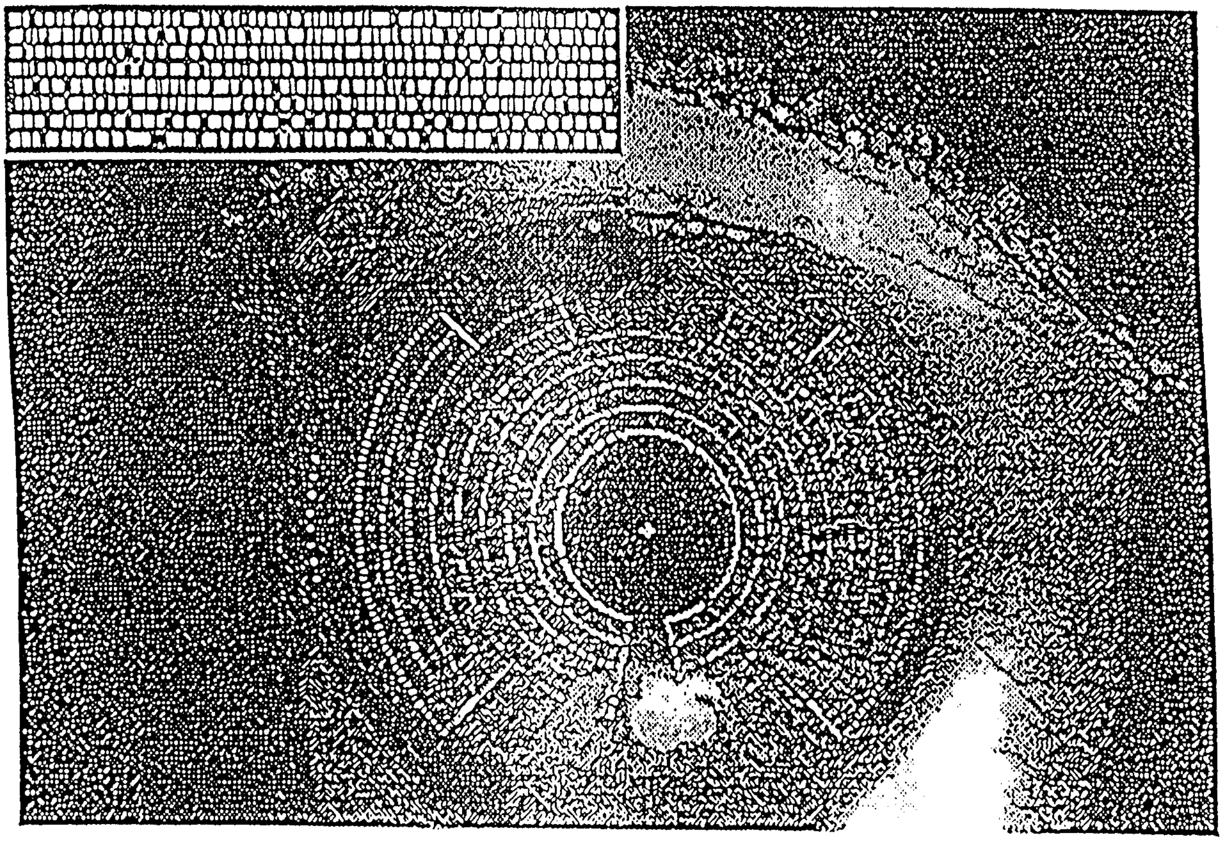


**Fig. 1. Processing Zones**

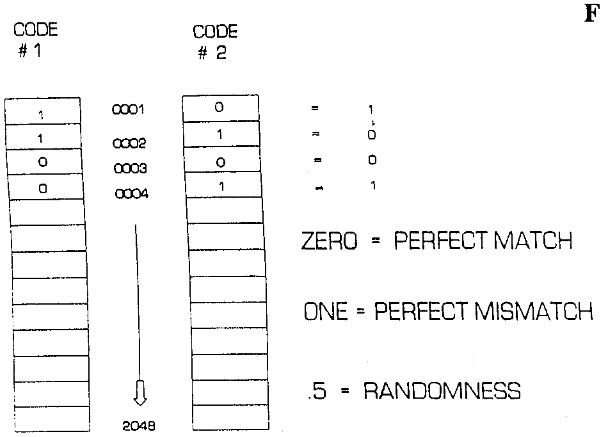


**Fig. 2. Hamming Distance**

location of the circular iris has now been defined and further processing can occur.

### Zones of Analysis

The system delineates eight zones of analysis on the iris (Figure 1) using a static/dynamic system. Through software, the static portion of the system truncates what would otherwise be circular zones. The zones are truncated at bottom and top to avoid analyzing spectral reflection from the six o'clock illuminator, and to ignore the occlusion from the upper eyelid. The dynamic nature of the system is such that it automatically adjusts the width of the zones in real time to maximize the amount of iris analyzed given varying ratios of pupil to iris diameter. Truncation and reduction of the zones has little effect on the analysis process because of the richness of detail of the iris and the invariant spatial relationship of the features. In actual practice, excellent enrollments and subsequent identifications are obtained with only 40% or less of the iris available for analysis. Features are located based on a polar coordinate system.

### Image Analysis

The features of the iris are then analyzed and digitized into a 256-byte (2048 bit) IrisCode (Figure 1, upper left corner) which is then stored in the database for future comparison. When an iris is subsequently presented for identification, a similar process occurs, and the resultant IrisCode is compared to every file in the database in the identification or "recognition" mode, or to a selected file in the verification mode.

### Hamming Distance Calculation

Comparison of IrisCodes includes calculation of a Hamming Distance (HD) as a quantitative measure of variation between the IrisCode from the presented iris and each IrisCode enrolled in the database. Each of 2048 pairs of bits are compared (Figure 2). Bit #1 from the presented IrisCode is compared to bit #1 from the reference IrisCode; bit #2 from the presented IrisCode is compared to bit #2 from the reference IrisCode; and so on. If two bits are alike (two "1's" or two "0's") 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

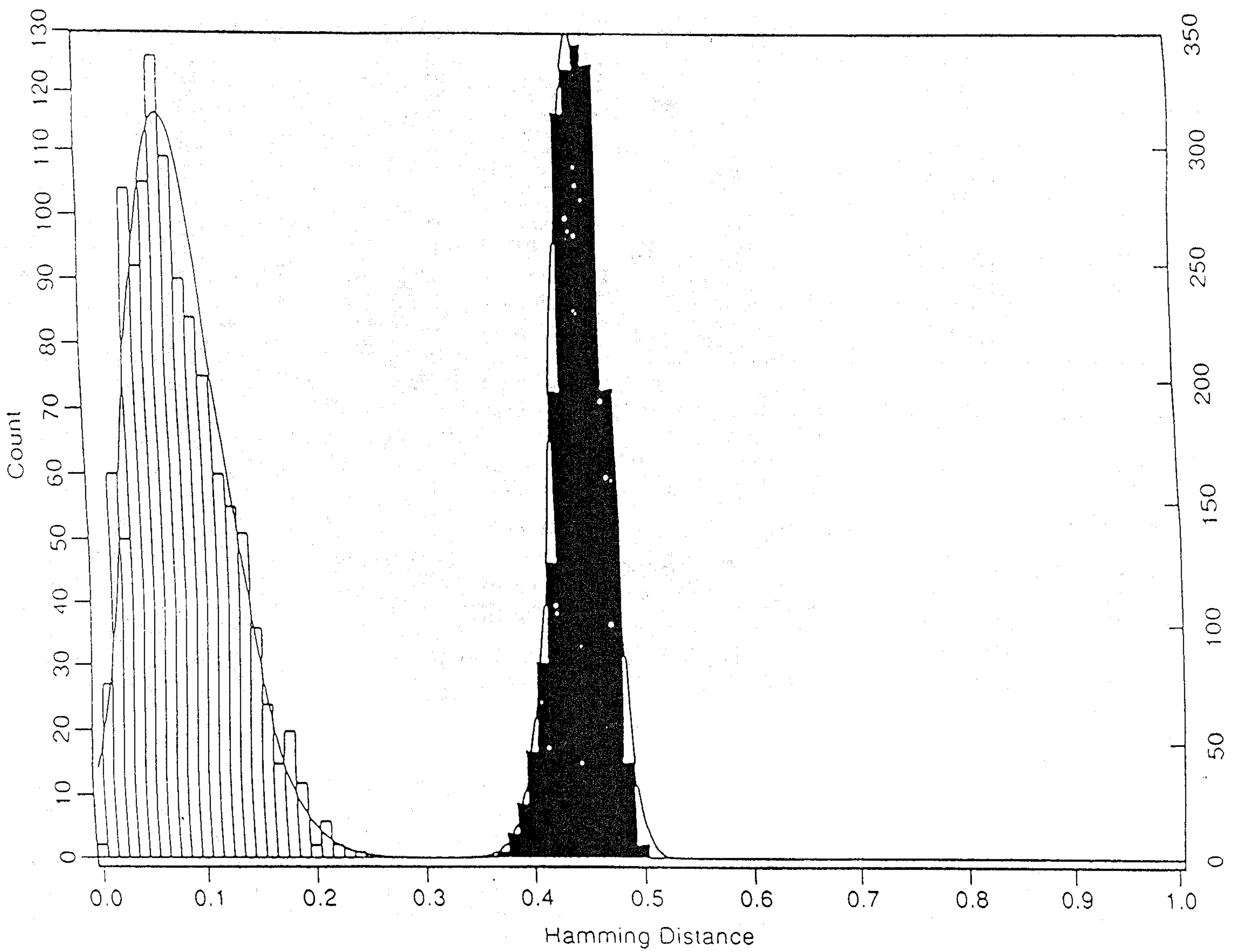


**Fig. 3. Hamming Distances for Authentics and Imposters**

comparison. After all pairs are compared, the assigned values are summed, and divided by the total number of pair comparisons resulting in a two-digit quantitative expression of how different the two IrisCodes are (sometimes the full 2048 pairs are not compared because the system detects and excludes spectral reflections that were not present during enrollment).

### Identification or Rejection

Many thousand IrisCode comparisons of both known impostors and known authentics have statistically defined the Frequency Distributions (Probability Densities) in Figure 3, next page. It is clear that the mean imposter Hamming Distance is near 0.5, which is what one would expect in a truly random relationship (flipping a coin several million times and noting the occurrence of heads versus tails). The mean value for authentics on the other hand is less than 0.10 (or 10%). Another feature of the Frequency Distributions is the very small Standard Deviation, resulting in very steep slopes and tightly clustered values for Hamming Distance in both. It appears, visually at least, to be two discrete distributions. The adjustable decision threshold can then be set at an HD of .32, the mathematical crossover point (the point where 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 that differs by more than 32% from the code(s) with which it is compared, is likely an Imposter because it displays the properties of a random relationship with the compared code. Another way of stating the relationship between the presented and the referenced IrisCode is that if they differ by 32% or more, they are considered to have emanated from different irises. Obviously, in the identification 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. (Roughly 7 seconds with a 1,500 IrisCode database). Identification occurs by selecting the best match of files who's Hamming

### Table 1. Hamming Distances and Associated Confidence Levels

| H.D. Criterion | Odds of False Accept (Imposter Odds) | Odds of False Reject |
|---|---|---|
| 0.25 | 1 in 13.5 billion | 1 in 1,490 |
| 0.26 | 1 in 2.04 billion | 1 in 2,660 |
| 0.27 | 1 in 339 million | 1 in 4,850 |
| 0.28 | 1 in 60 million | 1 in 9,000 |
| 0.29 | 1 in 12 million | 1 in 17,100 |
| 0.30 | 1 in 2.4 million | 1 in 32,800 |
| 0.31 | 1 in 603,000 | 1 in 64,200 |
| **0.32** | **1 in 151,000** | **1 in 128,000** |
| 0.33 | 1 in 39,800 | 1 in 260,000 |
| 0.34 | 1 in 11,500 | 1 in 536,000 |
| 0.35 | 1 in 3,630 | 1 in 1.12 million |

Distances are less than .32. As in any biometric, as one forces the selection threshold lower, the likelihood of a False Reject increases (although the probability of False Reject is markedly smaller than with most biometric systems available today).

### Calculation of Confidence Level

When connected to a monitor, information about the identified subject is printed on-screen and includes the Hamming Distance (HD) scored on the match between the presented image and the matched image in the database. The HD determines under which portion of the Imposter Frequency Distribution that identification fell (Figure 3, on previous page) and thus allows a direct calculation of the degree of confidence one can have in the identification. Table 1 provides an abbreviated list of HD's and associated imposter odds. For some sense of the accuracy of the iris identification technology, consider that the HD for the average authentic comparison in the authentic Frequency Distribution of Figure 3, equates to imposter odds of 1 in $10^{34}$. Another way of stating this is that following an identification decision based on a mean HD of .08, the probability that the identification was wrong is .00000000000000000000000000000000001.

## PERFORMANCE

### Crossover (Equal) Error Rate

The IriScan crossover error rate (that point where the probabilities of False Reject (Type I error) and False Accept (Type II error) are approximately equal) is .0000076, or .00076%. Table 2 represents this in a graphic form, similar to graphics provided in biometric tests by Sandia National Laboratories (SNLA). What is remarkably different, however, is the scale of error rates on the ordinate (the Y axis). Representation of error rates for most biometrics requires a range of 0 to 10%. In order to show a crossover point with iris identification technology, the range had to be reduced to 0 to 0.09%.

### Identification Speed

The speed of the identification/verification process is determined by many interacting variables. It varies naturally, with the inherent clock speed of the processor (standard production model speed averages about 1.6 seconds with its 486DX66 processor), the mode of operation (identification vs. verification), and the number of images presented improperly.

### Table 2. Database Distribution by Color

| Color | Orig. D/B | New | Total | Dups | Adj. Total | % of Total |
|---|---|---|---|---|---|---|
| Blue | 133 | 38 | 171 | (7) | 164 | 30% |
| Blue/grey | 20 | 6 | 26 | (1) | 25 | 5% |
| Grey | 24 | 2 | 26 | (1) | 25 | 5% |
| Blue/green | 05 | 2 | 7 | (0) | 7 | 1% |
| Grey/green | 06 | 0 | 6 | (0) | 6 | 1% |
| Grey/brown | 0 | 0 | 0 | (0) | 0 | 0 |
| Green | 0 | 0 | 0 | (0) | 0 | 0 |
| Hazel | 33 | 30 | 63 | (13) | 50 | 9% |
| Brown | 184 | 82 | 266 | (5) | 261 | 49% |
| TOTAL | 405 | 160 | 565 | (27) | 538 | 100% |

### Enrollment

Most enrollments, including administrative data entry and verification, can be accomplished in less than two minutes. Some have occurred in less than six seconds and some have exceeded two minutes where the user had some difficulty acquiring the proper focus or where the system operator was not satisfied with the average Hamming Distance. Nearly all users were proficient enough after enrollment to perform subsequent identifications without additional instruction or assistance.

### Proximity

Currently, the system displays optimum operation with the user standing approximately 9" from the aperture in the optical platform, although the capability to make identifications at a distance of 24" - 36" has been demonstrated. As one might expect, the distance is primarily a function of lens design and adequate illumination. Because initial models are designed to be used in an entry/access control application, we do not anticipate extending the identification distance beyond the current 9".

### Confidence

The vast promise of the iris identification technology described herein is based on over a billion file comparisons using five separate databases totalling approximately 3,000 irises. With 99% confidence we can state that the values established for means and Standard Deviations of our distributions are within 9% of the whole (infinite) population. To date, we have never experienced a False Accept, and to the best of our knowledge, False Rejects have occurred only when lighting and focus have been degraded beyond specified parameters. Although we have not recorded and statistically analyzed imposter odds for all of the identifications performed to date, a "typical" identification yields imposter odds of 1 in $10^{17}$, or .00000000000000001.

## Testing

Extensive testing in-house, under Defense Nuclear Agency monitoring, and in multiple Beta test facilities has confirmed and verified the following:

Formal quantitative testing:

- The system effectively and accurately performs identification and verification with a False Accept rate of 0;
- The system effectively and accurately rejects impostors and persons not enrolled;
- Virtually all subjects were capable of being enrolled. Average time is approximately 25 seconds, plus typing time;
- 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 others;
- The system has made over 1,000,000,000 file comparisons without error; and
- The Defense Nuclear Agency Brassboard System met or exceeded all test standards and requirements.

Beta testing: non-quantified Beta testing validated the form, fit, and function of the system as follows:

- User reaction to the system was overwhelmingly positive.
  Average rating on ease-of-use was 9 on a scale of 1 to 10.
  Average rating on user-friendliness was 9 on a scale of 1 to 10.
  Average rating on system speed was 8 on a scale of 1 = Very slow to 10 = Very fast.
  Willingness to use the system to identify personnel and/or protect assets averaged 7 on a scale of 1 to 10.
- There were no incidents of vandalism.
- 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 test.

## Conclusions and Lessons Learned (All Testing To Date)

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

User acceptance was excellent. The 28-watt quartz-halogen light, operated at approximately 7 watts and filtered with a magenta acrylic filter provided a comfortable amount of light without harshness or irritation. Most users were able to see clearly and simply the image they should expect to see when they approached the unit. The additional focusing aid (the triangular reflection of light low in the iris image) provided an immediate feedback mechanism to even presbyopic individuals. Most initial orientations required less than 30 seconds to train subjects on how to acquire a proper image.

## IriScan Systems Have Enrolled 99.99% of the Irises Presented to Them

The IriScan iris identification system has been absolutely accurate in the area of False Accepts, allowing no errors in over three million file comparisons during the two referenced testing programs. When the laboratory developmental testing is included, there have been no False Accepts in approximately one billion file comparisons. Under the formal, controlled testing scenario, the system has been 99.95% accurate in the area of False Rejects, with only 1 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 in either enrollment or identification / verification. Enrollment without contacts can be followed by identification / verification 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 identification / verification 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 I/V process.

An ancillary lesson from the foregoing is that rejections can be induced in many ways and that a " False Reject Rate" may well be a failure of the user to present a proper image. The degree to which subjects *want* to make the system operate can well 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 has a high probability of being rejected.

Absence of training and initial user orientation may lead to high and 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 binocular vision (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 his iris image without assistance.

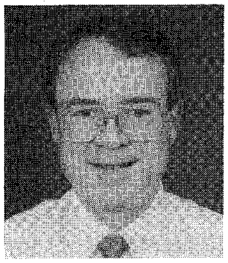
## CONCLUSIONS

Highly accurate, positive personal identification is feasible today using the iris of the human eye. This unique organ, which has more discriminators 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 256-byte code which is then compared against an entire database in less than two seconds. Identifications can then be used to control access and entry, or to provide identification information to an existing entry control system. Testing, under US Government controlled conditions and in numerous real-world environments, have proven the practicality and feasibility of extremely accurate iris recognition for any function requiring positive identification.

## REFERENCES

[1] J.G. Daugman, Ph.D., November 1993,
"High Confidence Visual Recognition of Persons by a Test of Statistical Independence,"
IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 15, No. 11.

[2] J.E. Siedlarz, et al., 1995,
"Biometric Identification / Verification Brassboard Proof-of-Concept System Phase II,"
Defense Nuclear Agency Technical Report No. DNA-TR-95-18, Alexandria, VA.



**Gerald O. Williams** has over 25 years of security management experience, including assignment as manager of a government agency's research and development program. He managed twenty security R&D projects which included development, testing, and evaluation of facilities, sensors, and security system interfaces. He managed technical contracts, ranging from interactive computer graphics development to behavioral studies of nuclear weapons security forces. He was instrumental in the definition, design, and testing of security systems and served as anti-terrorism liaison officer to DoD operations in Europe, NATO, and the military services, and to civilian law enforcement agencies. Mr. Williams has managed classified programs, and he has presented many educational sessions to concerned organizations. He has had a leading role in many security systems upgrade programs, such as the Department of State Embassy Security Upgrade Program and the General Accounting Office's electronic security system renovation project. He has been Program Manager for security programs development and operation at the US Army's Center for Software Engineering. Mr. Williams has a BA in Psychology and an MS in Industrial Management, and is currently Director of Product Development for IriScan.

# 1997 IEEE International Carnahan Conference on Security Technology

### 15-17 October 1997 — Canberra, ACT, Australia

## PURPOSE

This international conference is directed toward the research and development aspects of electronic security technology. It establishes a forum for the exchange of ideas and dissemination of information on both new and existing technology. Conference participants will be stimulated to consider the impact of their work on society. The Carnahan Conference also provides a basis for long range support and assistance to authorities and agencies responsible for security, safety and law enforcement in the use of available and future technology. A conscientious effort will be made to communicate the significance of developments to other interested groups. Liaison is maintained with professional societies and information media not especially related to engineering.

**Chairman:** Tom Andrews
P.O. Box 2149
Canberra, ACT, Australia
V (61) 6-2412049
F (61) 6-2412874

For E-Mail and www addresses, see rear cover.