

## Something You Are

Though many of us remember the eye-scanner identification device used in James Bond films in the 1980s, the technology remained a fiction until recently. Now, with the need for more secure systems and with the decrease in biometric technology costs, some colleges and universities are taking a close look at this same technology for security applications.

Biometric technologies use the concept of “something you are” to provide more secure identification. Of the available technologies, iris recognition may be the best choice to explain the basic principles and considerations in evaluating biometric identification. It is the most reliable for its price and ease of use, and some interesting real-world applications take advantage of iris recognition for secure biometric identification.

### Origins

In 1936, the ophthalmologist Frank Burch may have been the first to propose the idea of using the iris for identification. In 1989, the ophthalmologists Aran Safir and Leonard Flom enlisted the help of Harvard Professor John Daugman to develop iris-recognition algorithms, which Daugman subsequently patented. The algorithms are now owned by Iridian Technologies.<sup>1</sup>

Daugman is currently a professor at Cambridge University, where he has received numerous awards for his work on iris-recognition algorithms. Although other research exists in the iris-recognition field, the work done by Daugman is prominent in that it has produced commercial products and applications that

implement iris-recognition technology. Daugman developed a computerized process to generate a binary-encoded template, called an IrisCode, from a camera image taken of an iris. His algorithms then perform real-time identification of persons by searching through a database of enrolled IrisCodes for a match.

### Physiology

The iris is the colored part of the eye; it lies behind the cornea and in front of the lens and is protected by the eyelid. In the human body, the iris is the only internal organ that is normally externally visible. The iris is formed of a trabecular meshwork (elastic connective tissue), layers of pigment, muscle, and ligaments, and it controls the amount of light that enters the eye by allowing the pupil to dilate. Color is not used in iris-recognition technology. Instead, the other visible features—the connective tissue, cilia, contraction furrows, crypts, rings, and corona—distinguish one iris from another.<sup>2</sup>

By the time a person is about eight months old, the structures of the iris are complete, and they do not change in later life. The iris cannot be surgically altered without damage to a person's vision, and its physical response to light provides one test that prevents artificial duplication of the organ. No two irises are alike, even if they are from identical twins or from the left and right eyes of the same person. The physiological characteristics of the iris, combined with the fact that those characteristics are exhibited with so much variation over the population, make the iris a prime candidate for use in automatic identification.

### Biometric Technology Comparison

Three factors can be used for security: something you know (a password or a PIN), something you have (a smart token or an access card), and something you are (biometric). Biometrics can be used alone or in conjunction with one of the other factors to strengthen the security check. Biometric technology has advantages over both of the other factors in that the user does not need to remember anything or possess a physical token in order to be identified. Tokens and cards can be lost, and passwords and PINs can be forgotten or compromised. A biometric is susceptible only to forgery, which can be extremely difficult, depending on the biometric.

The National Center for State Courts (NCSC) has published information comparing physical biometric methods. The NCSC data is substantiated by a similar comparison table in an article published by the IEEE Computer Society. Both findings rank iris recognition as one of the most secure biometric technologies. Although facial recognition, voice recognition, and hand geometry are nonintrusive and have value for certain applications, all of these biometric methods are relatively unreliable compared with iris recognition, retinal scanning, and fingerprinting.<sup>3</sup>

Fingerprinting has been widely used, perhaps because the hardware is relatively inexpensive and available due to its use in the criminal justice system. A fingerprinting device is easy to use, but the technology is not as reliable as iris recognition or retinal scanning. External factors such as dryness, dirt, and scarring on the finger may account for the higher error rate in fingerprinting. Another ad-

vantage of iris recognition over fingerprinting is that forgery is not as much of a risk. Sophisticated fingerprinting technology is designed to detect false fingers, but a person's finger can be cut off or used for a mold much easier than an eyeball can be extracted and used for impersonation. In fact, the iris from an extracted eye would not be usable for more than a few seconds.<sup>4</sup> Iris-recognition devices can also detect the dilating pupil to ensure that the eye is live.

Retinal scanning is often confused with iris recognition, but they are very different biometric technologies. The retina is located at the back of the eye and contains distinctive vascular patterns that can be used for identification and verification. Retinal scanning is the only biometric that is more reliable than iris recognition. Retinal scanning requires that the subject stay very still, with the eye at a distance of no more than three inches from the scanner, whereas iris recognition can be accomplished with the subject at a distance of up to about two feet from the camera. Since retinal scans are more intrusive, they are probably most appropriate for applications that require the highest levels of security, in which the subject is very cooperative or is required by law to succumb to the scan.

### Conclusions

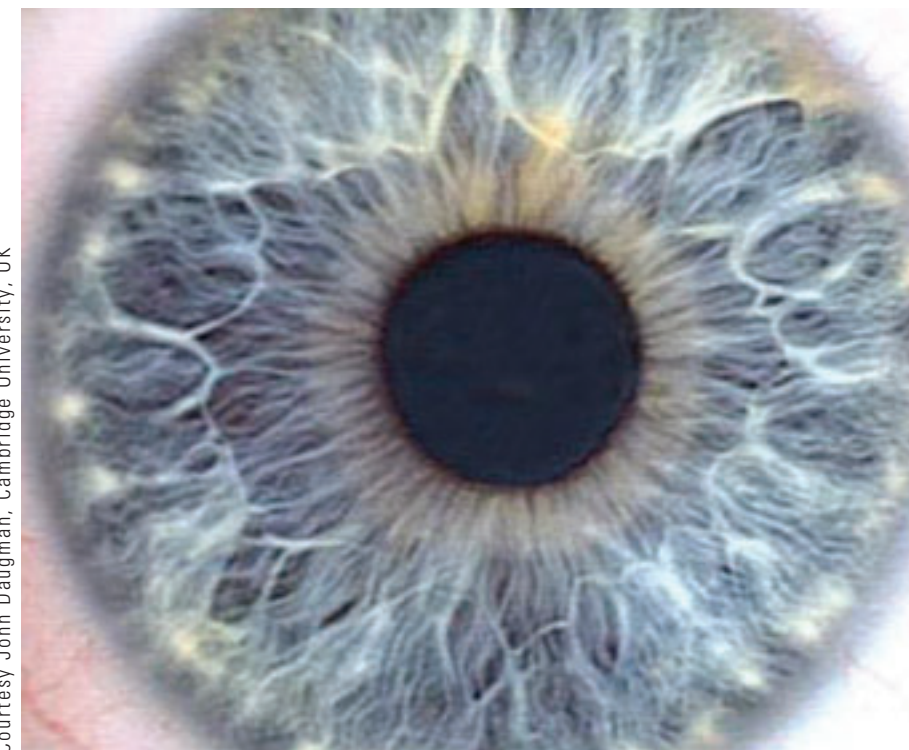
One of the most promising applications for iris recognition increases security for the transportation industry. The current requirements for securing airports could increase the use of biometric devices in this area. Since there were not many identification-verification systems in airports before September 11, 2001, the opportunity is ripe to install state-of-the-art biometric identification systems for travelers.

Another promising application is for bank ATMs. Someday ATM users may be identified by their irises rather than their PIN numbers. A person's IrisCode can be stored either in a database or on a smart card. The ability to store the IrisCode on a card or token is important because it eliminates privacy concerns associated with retaining identities in a centralized database. However, enrolling customers by using a biometric device takes longer than simply assigning and changing a

PIN. Since cards with PINs are already in use, it may be a while before any type of biometric device becomes prevalent in the banking industry.

Finally, a biometric technology such as iris recognition can easily eliminate or complement the standard log-in password for individual authentication to a

technology has made great strides in the last five years. It scores well, both in ease of use and reliability, when compared with the other biometric technologies. Perhaps someday, iris recognition will be implemented for many more applications, and the only thing a user will need to remember is, “Don't blink!”



Courtesy John Daugman, Cambridge University, UK

computer. Providing multifactor authentication is one of the great benefits of biometric technology. The ability to support single sign-on goes a step further to enable biometric authentication to be integrated into enterprise-class applications. Iridian Technologies supports an implementation of single sign-on with Computer Associates eTrust Single Sign-on. For computer log-in, however, cost and portability may be prohibitive factors. Even though the prices for an iris-recognition camera and software are not substantial, the costs add up when a device must be added to each workstation. The cameras are small and suitable for a desktop, but they would be cumbersome to carry around in order to facilitate logging in to a laptop.

Based on possible applications, reliability, ease of use, and available software and hardware, iris-recognition technology has potential for widespread use. The

### Notes

1. Background information is from John Daugman, “History and Development of Iris Recognition,” John Daugman Web page, <<http://www.cl.cam.ac.uk/users/jgd1000/>> (accessed May 10, 2004).
2. Physiology information is from John Daugman, “Anatomy, Physiology, and Development of the Iris,” *ibid.*
3. NCSC Court Technology Lab, “Biometrics Comparison Chart,” 2002, <<http://ctl.ncsc.dni.us/biomet%20web/BMCompare.html>> (accessed May 10, 2004); Simon Liu and Mark Silverman, “A Practical Guide to Biometric Security Technology,” *IT Professional* (January 2001), <[http://www.computer.org/itpro/homepage/jan\\_feb01/security3b.htm](http://www.computer.org/itpro/homepage/jan_feb01/security3b.htm)> (accessed May 10, 2004).
4. Carlos A. Soto, “Biometrics Gets Better but Still Needs Some Work,” *Government Computer News*, vol. 22, no. 10 (May 5, 2003), <[http://www.gcn.com/22\\_10/prod\\_reviews/21949-1.html](http://www.gcn.com/22_10/prod_reviews/21949-1.html)> (accessed May 20, 2004).



Mary Dunker is Director of Secure Enterprise Technology Initiatives at Virginia Tech.