Private Eyes

Biometric identification is set to replace passwords and PINs

By CORINNA WU

In the 1983 James Bond movie *Never Say Never Again*, a villain gains access to the United States' nuclear arsenal by foiling a presumably fail-safe passkey system—a scan of the president's right eye. This, of course, left the dapper British secret agent to set things right and save the world.

Now, eye-scanning technology has moved beyond Hollywood. By next year, some automated teller machines (ATMs) may use scans of the human iris—the ring of colored tissue surrounding the pupil—as a way to verify bank customers' identities. One application of iris scanning debuted this year, when the security-conscious officials of the 1998 Winter Olympic Games in Nagano, Japan, required biathletes to go through such a system to check out their rifles.

The iris can serve as a human bar code, its unique features captured and translated into a biological personal identification number (PIN). Iris scanning is just one technology in the burgeoning field known as biometrics. The word "biometrics" originally meant the statistical study of biological variation. However the term now also refers to technologies that analyze human traits for security purposes.

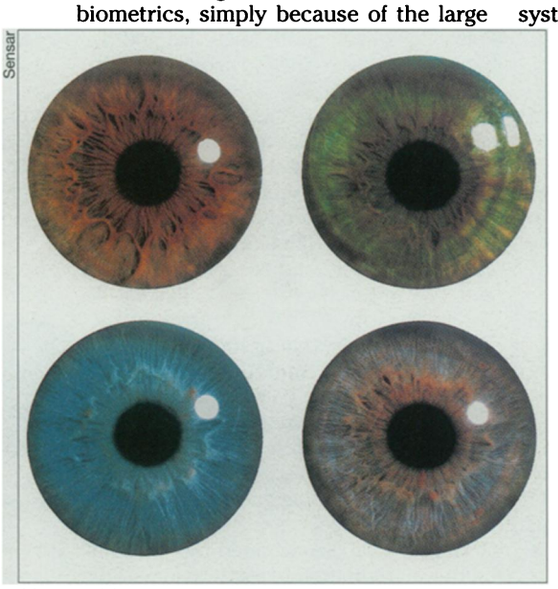
Many groups are developing biometrics to replace or supplement PINs, passwords, and access cards. In this way, banks and other businesses hope to reduce theft, improve security, and make consumer transactions more convenient.

"In a couple of years, biometrics will be everywhere," predicts Raj Nanavati of the International Biometric Group, a consulting firm in New York City. Although researchers have explored these technologies for years, devices have only recently become cheap enough to be integrated into common products.

Fingerprinting is the most widely known biometric, but other approaches, such as face recognition, hand geometry, voice printing, and signature verification, also have potential. Calculating the degree of security actually provided by these various biometrics is a difficult task, however, and researchers are still exploring this problem, even as actual devices are being rolled out into the marketplace.

When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warnings, many people continue to choose easily guessed PINs and passwords: birthdays, phone numbers, and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he or she claims to be. Biometrics may solve this problem, since a fingerprint or an iris is undeniably connected to its owner. The system can then compare scans to records stored in a central or local database or even on a smart card (SN: 2/1/97, p. 78).

Iris scanning is one of the most secure biometrics, simply because of the large number of independent features that can be coded. Consisting of fibrous and vascular tissue and pigment granules, the iris possesses about 266 measurable features. "No other part of the body has this many [useful attributes]," says Leonard Flom, an ophthalmologist in Westport, Conn. Fingerprints run a distant second, with about 40 characteristics.



Human irises possess unique patterns that can serve as identifiers, much as fingerprints do.

In 1981, after reading many scientific reports describing the iris' great variation, Flom and San Francisco ophthalmologist Aran Safir proposed using the iris as the basis for a biometric. In 1987, they began collaborating with computer scientist John Daugman of Cambridge University in England to develop iris identification software. Their system separates a black-and-white image of the iris into a pattern and converts it into a mathematical code. The system then compares the code to a stored one and decides whether they match.

The researchers eventually formed a company called IriScan in Mt. Laurel, N.J., which has licensed the technology to about 10 other groups, including the Japanese company that made the Olympic biathlon security system. Other companies want to develop iris scanning for automobile or Internet security, and even as a mass transit fare system.

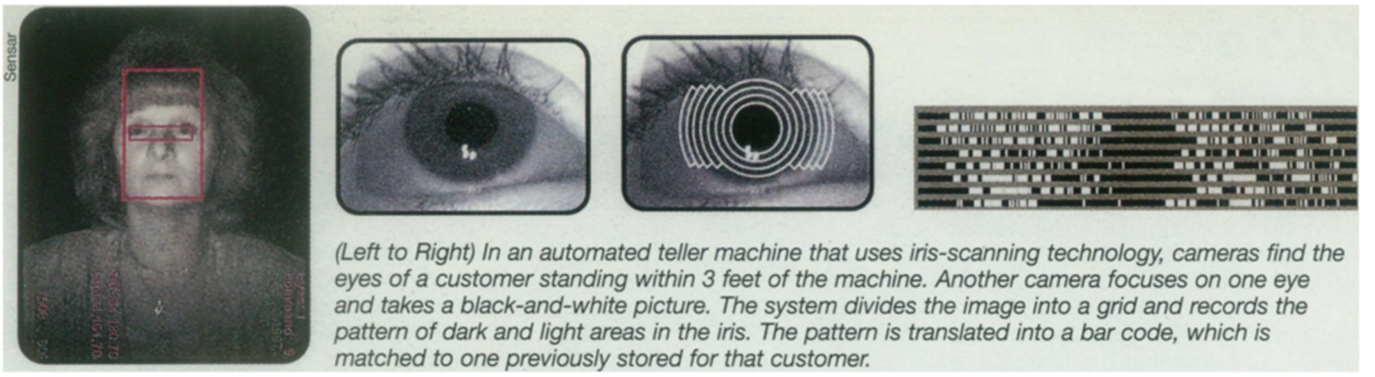
Sensar in Moorestown, N.J., has incorporated iris scanning into ATMs. Eye scans ordinarily require a person to look directly into a camera and therefore can be intrusive. Sensar has combined the iris-scanning system with an advanced camera setup that can detect the customer's eye from 1 to 3 feet away. Sensar licensed the camera technology from Sarnoff Corp., in Princeton, N.J. which originally designed it for the military so that high-flying helicopters could take pictures of tanks on the ground.

As a customer walks up to an ATM, a system of three cameras identifies his or her torso, head, and eyes, then zooms in on the iris, says Michael Negin, Sensar's chief technology officer and vice president. One of the cameras takes several pictures, which are then divided into a grid-like pattern and translated into a bar code. The entire process takes only a few seconds.

Contact lenses don't affect the image, and the software corrects for reflections from eyeglasses, says Negin. However, "scratches [on the eyeglasses] do distort the image and reduce comparison values."

The researchers also took advantage of another unique trait of the iris: the constant dilation and contraction that adjust the size of the pupil. "Initially, people discouraged us because the pupil moves all the time," says Flom. "How do you attack a moving target?" The system now detects that subtle movement, to ensure that a live human being and not just a picture of an iris is in front of the camera.

Even identical twins don't have the same iris, though they may have the same face shape or fingerprint, says Negin. Proponents of other biometric technologies, such as face recognition, argue that this is a minor concern, since in the real world, most crimes aren't committed by an evil twin. Even in James Bond's universe, the impostor needed a surgical eye implant to bypass the system.



(Left to Right) In an automated teller machine that uses iris-scanning technology, cameras find the eyes of a customer standing within 3 feet of the machine. Another camera focuses on one eye and takes a black-and-white picture. The system divides the image into a grid and records the pattern of dark and light areas in the iris. The pattern is translated into a bar code, which is matched to one previously stored for that customer.

Nearly 140 biometric identification products exist now, although "not all are key players," says David Harper of the International Computer Security Association (ICSA) in Carlisle, Pa. The proliferation of so many new and largely untested technologies begs for some systematic way of sorting out the claims. Researchers at the National Biometric Test Center at San Jose (Calif.) State University are working to do just that. "We're trying to establish a science to evaluate biometric devices and technologies," says director James Wayman.

A good biometric has two basic characteristics: stability and distinctiveness. A stable biometric doesn't change over time. "Clearly, hair length would not be a good biometric identifier," says Wayman. A distinctive biometric is unique to an individual. Iris patterns fulfill these requirements, as do—to varying degrees—fingerprints, face shapes, hand geometries, voices, and signatures. Some biometrics, like fingerprints, "may be stable and distinctive but can be temporarily damaged," says Wayman.

No biometric is perfect, says Nanavati, and the one chosen for a particular use depends on a variety of practical considerations. Nanavati, along with his brother and partner Samir, analyzes biometric technologies by their cost, intrusiveness, accuracy, and ease of use. The relative importance of these factors depends on the application. For ATMs, rapid identity checking is essential, but for employees at a nuclear facility, for example, a lengthier and more intrusive process would be acceptable, he says.

Biometrics fall roughly into one of two categories: physiological and behavioral, says Wayman.

Fingerprinting, used widely in forensics and in government databases, is the most well-known physiological biometric. Finger-scanning devices avoid the messy ink associated with fingerprinting by having users touch a glass plate or silicon chip, which records an image of the fingertip's ridges and valleys.

Hand geometry devices take an image and measure the three-dimensional shape of the fingers and knuckles. "Your hand is a pretty big and stable object," says Wayman, although it doesn't definitively differentiate one person from another. "My estimate is that if you checked 50 to 100 people, you'd find someone with a similar hand geometry." For many purposes, such as controlling access to a building, that's good enough, he adds. Also, hand shape is less easily changed than fingerprint pattern.

Face recognition is being tapped for applications such as controlling access to a personal computer. A digital camera can take a picture of the person sitting in front of the screen, and comparison software can make sure it matches the owner.

Iris and retina scanning are the most intrusive and expensive technologies, yet the most accurate. People tend to feel wary about exposing their eyes to a camera, harmless as it may be. By eliminating the need for a person to stare into a lens, Negin says, Sensar's machines reduce that intrusiveness. Sensar is currently reengineering the devices to bring down their cost, he adds.

Voice recognition technology is the obvious choice for phone-based systems. Experts in the field disagree over whether voice is a physiological or a behavioral biometric, says Wayman, but it does contain a behavioral component, since a person's voice changes with mood. Voice recognition is one of the cheapest technologies because it uses existing phone equipment, but it is less accurate than other methods.

Dynamic signature verification, a behavioral biometric, assesses the style and speed with which a person signs his or her name. Signatures are already widely used to certify identity, which makes this one of the least intrusive biometrics; however, it is also one of the least accurate.

The ICSA is trying to establish a simple method of certification for biometric technologies and has formally tested eight or nine products, says Harper. The group will release the results at the CardTech/SecurTech Conference in Washington, D.C., later this month.

Testing biometric technologies is complicated, says Wayman. "Data is very expensive [to acquire] because it involves human beings. We're trying to estimate errors at very low levels from very limited amounts of data." Moreover, he adds, "predicting from those error rates how an actual system will perform is not trivial."

Take iris scanning, for example. IriScan claims, based on the number of possible iris patterns, that the probability of two irises producing the same code is vanishingly small. The company provided Wayman with test results showing no false matches in 5,000 tests. However, that doesn't mean the error rate is zero, he says, because "we don't have enough files yet."

Wayman is working with statisticians from the University of California, Berkeley on this problem. "It's slow and painstaking," he says.

Requiring an exact match, even if possible, might be counterproductive. Unlike a PIN or password, the performance of a biometric technology depends a lot on the person using it. Growing a beard or wearing a different type of makeup could trip up a face recognition system. Even pressing a finger down on a glass plate too hard could alter a fingerprint, causing the device to cry impostor.

"Some days, you're just not yourself," Wayman notes.

To accommodate those off days, biometric systems can be made to be somewhat forgiving. They can be set to require that only a certain percentage of the pattern match.

Biometrics also bring up legal and privacy issues that will have to be addressed as these technologies come into popular use. Consumers already concerned about widespread distribution of personal information are likely to be suspicious of data banks that record encoded details of their body parts.

In a poll, the International Biometric Group asked about 100 people how they would react to a finger scan at a bank. About 60 percent of the people who only heard a description of the procedure reacted positively toward the idea, says Nanavati, but "once they tried it, favorability shot up to 90 percent. If it makes a transaction easier and cheaper, customers are more apt to use it."

Much of the wariness may come from the strangeness of a new technology, Nanavati suspects. ATMs suffered from the same problem when they made their first appearance 2 decades ago. If biometrics do find their way into computers, automobiles, and cash machines, perhaps their familiarity will also breed content. □