

Biometric Identification

by Eric J. Lerner

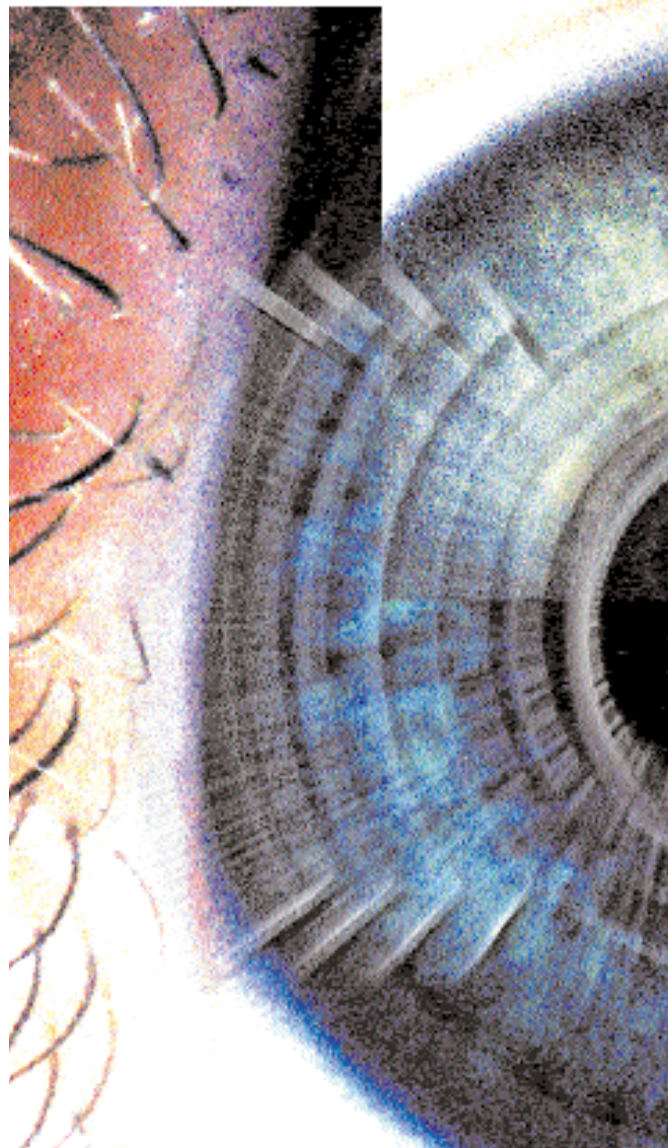
Biometric recognition systems enter the marketplace but stir fears of Big Brother

The old saying puts necessity as the mother of invention, but in today's world, the relationship is sometimes reversed. Technological advances often come first and drive the search for commercial applications. This situation is true in the field of biometric identification—the automated identification of people by biological characteristics such as their fingerprints or iris patterns.

In the past two years, rapid decreases in price and better performance have made biometric technology practical for consumer applications such as accessing automatic teller machines (ATMs) and for governmental purposes such as confirming the identities of welfare recipients. But a sharp debate is emerging over whether biometric technology offers society any significant advantages over conventional forms of identification, and whether it constitutes a threat to privacy and a potential weapon in the hands of authoritarian governments.

The use of biological features for identification is of course not new—fingerprinting was developed in the 19th century—nor is automation of the process. Beginning in the late 1970s, defense and national security agencies that could afford it started using automatic biometric systems to check identities as a more secure alternative to photo-IDs. But more widespread applications did not emerge until greater computer power dropped the price of biometric systems. For example, a fingerprint scanner that cost \$3,000 five years ago, with software included, and \$500 two years ago, costs \$100 today. Similar price reductions have occurred in other leading biometric technologies, such as iris scanners.

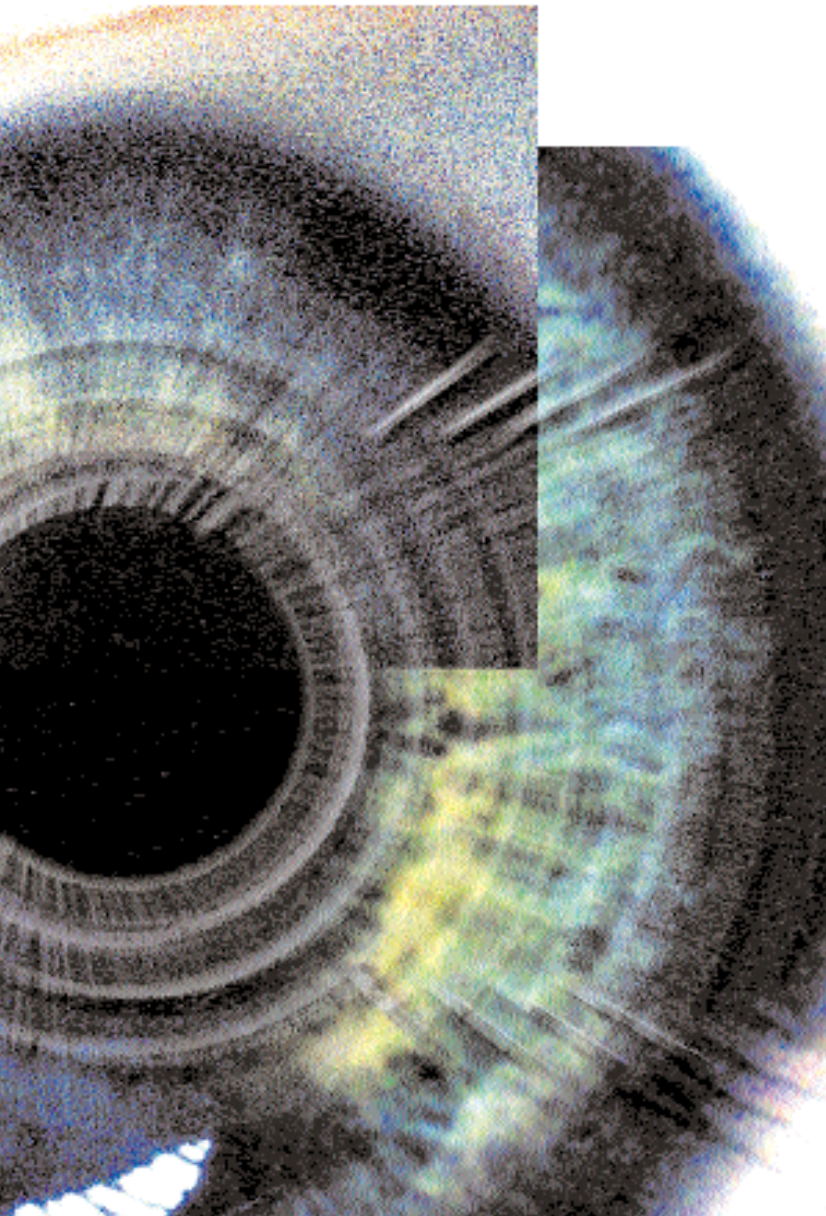
With lower prices, biometric identification systems are moving into two main application areas—banking and governmental agencies—and they have spurred growth in the new industry to nearly \$250 million a year in annual sales. Several banks around the world, including Bank United (Houston, TX) and Nationwide Building Society in the United Kingdom, have tested iris scanners as an alternative to personal identification number (PIN) codes for ATM access. On a larger scale, the state of Connecticut began to use fingerprint scanning in 1996 as a way to identify welfare recipients, and the U.S. Army, Air Force, and Social Security Administration are looking at various biometric recognition systems. Both the Department of Defense and the Department of Veterans Affairs plan to



use finger images to verify the identity of employees and those seeking retirement benefits.

For banking, the advantages of biometric scanners are mainly convenience rather than security. “Customers like the ease of just going up to the ATM and staring at it for a few seconds,” says Joe Arbona, communications coordinator for Bank United. “They don’t need to remember their PIN.” Although biometric technology protects against a thief who can guess a carelessly chosen PIN code, it does nothing to prevent the more common hold-ups in which an ATM customer is robbed near the machine or forced at gunpoint to withdraw money.

The advantages for government agencies are clearer, as biometrics makes the creation of false identities harder. But this is precisely what concerns some privacy and



efforts are under way to develop automatic signature-identification and voice-identification systems.

Iris scanning

Of these systems, iris scanning has made the most spectacular move from development to commercialization in the past two years and has generated the greatest interest. As an identifying body part, the human iris—the colored protein of the eye—has several advantages. It is an integral part of the body, so it is not amenable to easy modification. Unlike fingerprints, the iris can be imaged from about 1 m away. Yet, like fingerprints, iris patterns are unique to individuals. Even identical twins don't have identical patterns, nor do one person's right and left eyes. The patterns are stable throughout life and only change in a highly predictable manner as the pupil opens and closes in reaction to light.

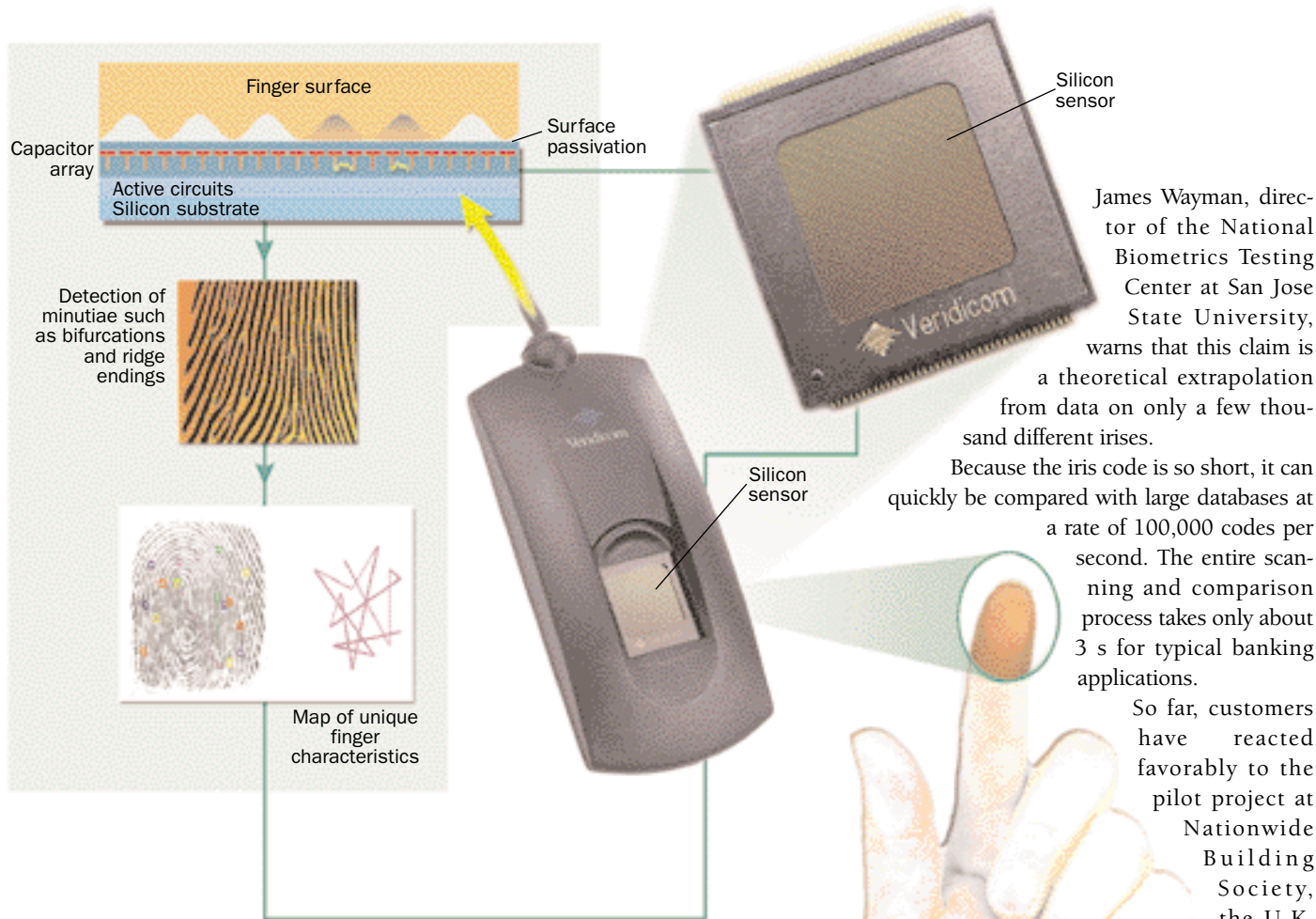
The algorithm used in iris identification was developed beginning in 1980 by University of Cambridge computer scientist John Daugman and was first implemented in the laboratory in 1989. Since then, Daugman and his colleagues, American ophthalmologists Aran Safir and Leonard Flom, have made substantial improvements in the technique as

human rights advocates. "Perfect identity equates to perfect control," says Simon Davies, director of Washington, DC-based Privacy International. In the hands of authoritarian governments, the ability to track citizens with perfect reliability could be a formidable mechanism of repression, he notes.

From a technical standpoint, most biometric systems share a common hardware base. They require reasonably high-resolution scanning devices to acquire and digitize an image of some part of a person's body, and they need a computer to run the pattern-recognition and sorting software for the specific type of identification used. Currently, there are five major types of biometric systems either in use or under investigation that scan a part of the body: fingerprints, iris, retina, face, and hand. In addition,

more computer processing power has become available, and they have formed IriScan, Inc. (Marlton, NJ), to license the technology.

Before the iris can be imaged, it has to be located in the face. Sensor, Inc. (Moorestown, NJ), has developed camera technology that first identifies the head, then the eyes, and then the irises. The IriScan algorithm precisely locates the outer and inner borders of the iris, and detects and excludes the eyelids if they cover part of the iris. The system uses a mathematical technique called wavelet analysis to translate the image of the iris into a 512-byte pattern. Wavelet analysis is a mathematical relative of the more familiar Fourier analysis, and it breaks down an image into a set of spatially limited waves. This pattern, which is called the iris code, is defined in a coor-



When the finger touches the silicon sensor, the pattern of ridges and valleys is determined by the capacitance at any point during a cycle of charging and discharging the capacitor array. The data are scanned at 500 dots per inch, converted to digital form, and a map of unique finger characteristics is created on the basis of minutia detection. This map is then compared with a data bank of known prints.

dinate system that is invariant to changes in pupil contraction and to the size of the image itself.

Once an iris code is prepared, the algorithm compares a specific code against a group of codes previously stored in the computer. The comparison simply calculates the fraction of bits that agree or disagree between two iris codes. If there is no match, the fraction of disagreement, or Hemming distance, should be close to 0.5; and if there is a match, it should be close to 0. Statistical analyses show that there are 266 degrees of freedom in the iris—equivalent to a perfectly random pattern with 266 bits. Daugman claims that his tests show that both false acceptance and false rejections can be kept at a level of less than 1 in a million by requiring that more than 66% of the pattern agree with a stored iris code. However,

James Wayman, director of the National Biometrics Testing Center at San Jose State University, warns that this claim is a theoretical extrapolation from data on only a few thousand different irises.

Because the iris code is so short, it can quickly be compared with large databases at a rate of 100,000 codes per second. The entire scanning and comparison process takes only about 3 s for typical banking applications.

So far, customers have reacted favorably to the pilot project at Nationwide Building Society, the U.K. banking using Iriscan technology at its Swindon branch,

with 9 out of 10 preferring the scanner to a PIN code. In a similar project at Bank United, customer reactions have not been assessed yet. However, the bank says that the iris scan will be offered as an option, and PIN codes will be maintained for those who want them.

Fingerprints in the computer

If iris scanning has attracted the most attention, finger imaging, based on the long-established technology of fingerprinting, is the most widespread biometric technology and the one favored by most government agencies. In this approach, an individual places a finger on an optical scanner, which scans in a digitized image of the person's fingerprint. An alternative method is to use a silicon-based capacitor plate array, which has been developed by Veridicom, Inc., Santa Clara, CA. When an individual places his finger on the sensor, the finger acts as one of the plates of a capacitor. The other plate, on the surface of the sensor, is one of an array of 90,000 on a silicon chip with a sensing circuitry of 500 dots per inch.

A software algorithm then searches the fingerprint image for the location of “minutiae,” which are points where a ridge ends or splits in two. In addition, some algorithms categorize the overall patterns of the fingerprint into one of five standard classes, such as a whorl or an arch.

Because fingerprints have fewer degrees of freedom than irises (about 40 versus more than 200), automated fingerprint identification has generally not achieved the same level of accuracy as iris scans. In fact, the false rejection rate—the frequency with which a valid identification is erroneously rejected—is 1% in most systems. False acceptance rates, however, are extremely low, which makes imposture almost impossible. So fingerprint-image systems are being widely adopted for social welfare purposes. In Connecticut, all welfare recipients are fingerprint-scanned, and the fingerprint code is incorporated into an ID card that each recipient must present to receive a monthly welfare check. Using prints from two fingers has reduced false rejection rates.

In addition, Identix, Inc. (Sunnyvale, CA), the largest provider of fingerprint scanning hardware and software, is marketing its device as a computer security aid to replace the use of passwords. Here, the scanner is placed on a pad next to the computer, incorporated into the mouse, or built into the keyboard.

Other biometric techniques are under development, but all of them have significantly greater error rates than either iris scanning or fingerprint imaging. Hand dimensions remain relatively stable but are not sufficiently unique to distinguish people in a large population. There has been considerable research on facial recognition, but faces vary depending on expression and are too easy to alter and disguise. Voice identification is desirable for remote access applications; however, a person’s voice varies with emotion, age, and health, so this approach has not reached the application stage. In some systems, several identification methods are used in combination with fingerprinting. In the Connecticut welfare program, for example, ID cards contain a photograph and signature as well as an encoded fingerprint.

Is Big Brother watching you?

The use of biometric identification by government agencies is causing increasing alarm among human rights and privacy advocates, who fear a government’s ability to trace the activities of individuals. “1984 may have simply been too early a date,” said Barry Steindhardt, associate director of the New York branch of the American Civil Liberties Union, who referred to George Orwell’s satiric novel in a recent *Christian Science Monitor* interview. “We are now approaching a time when we will live in a sur-

veillance society where all our movements and actions will be monitored.”

If biometric identifiers such as fingerprinting or iris scanning are extended to the whole population and used as universal identifiers—to replace easily faked IDs such as Social Security cards—rights advocates expect some major potential problems. For one, any authoritarian government will be able to track dissidents with an unbreakable identity. In Nazi-occupied territories during World War II, false papers were an indispensable tool of resistance fighters, and dissidents hiding from more recent tyrannies, such as the Pinochet regime in Chile, have found false identities essential. Mass biometric identification by present-day repressive regimes could make dissidence or resistance far more difficult. In the United States, government access to a universal biometric identifier that is also used in commercial transactions such as banking could make it much easier to harass those with unpopular views, as the FBI did in the 1960s and 1970s under the COINTELPRO program.

Aside from the potential government abuse of unbreakable identifiers, the existence of such data files could make it difficult for those who legitimately need to change their identities to flee from an abuser or stalker, or even to use a government witness-protection system. Once IDs are stored in a computer database, they become vulnerable to access by people able to hack the system or willing to misuse their authorized access.

Because of such concerns, Congress has repeatedly rejected the use of a universally required ID card. Indeed, a requirement for biometrics identification of the general population is unlikely, at least in the United States. But the current requirement of fingerprinting for some welfare recipients may foreshadow the introduction of biometric IDs for certain segments of the population, such as the poor or immigrants, who could be further stigmatized and lose privacy protections enjoyed by the rest of the society. In addition, Davies and other privacy advocates point out that the widespread use of biometric identifiers in commerce or during employment—for example, for computer access—could easily pave the way for government surveillance as police and security agencies gain access to such records.

Weighed against these dangers, Davies sees the potential advantages of better identification—convenience and protection against fraud—as relatively slight. “We don’t need perfect identity,” he says. “Every free and open society has always had a measure of anonymity.” Whether that anonymity is preserved will in part depend on how biometric identification technology is used in the coming years. ■