

Roger Allan, TECHNOLOGY EDITOR

BIOMETRICS WIELDS A DOUBLE-EDGED SWORD

More than ever before, we need to verify our identities. But the trend toward biometrification raises some worrisome issues about others invading our personal lives.

Identity theft, terrorism, and fraud permeate our society. Biometrics addresses the urgent need for identification with a number of impressive technological advances. But what about privacy issues? Do we really want “Big Brother” tapping into our lives

without permission?

Databases of biometric information could be misused if they fall into the wrong hands. Many security, law-enforcement, border-control, medical, and banking organizations maintain vast biometric databases that are available to government agencies and business entities.

Consumer electronics, on the other hand, don't have such databases. They use encrypted personal information tied to a name or personal identification number (PIN). The consumer device then mathematically compares the last information entered against the encrypted personal information.

Despite the concerns, the implementation of biometrics is soaring. National projects in many countries have focused on developing smart cards that do more than serve as credit cards. These cards also will be used as work permits, health cards, national identification, passports, and applications for military security access.

Adding more impetus to the market, the U.S. government is pressuring 26 visa-waiver nations to embed biometric data into their passports. Next-generation smart cards in Europe, Asia, and Japan promise to include biometrics for identification, passport, visa, and driver's license purposes. Needless to say, the scramble is on among smart-card chip manufacturers to cash in on this projected growth.

According to the International Biometric Group, the market for biometric methods that identify or verify a person's identity using a behavioral or physiological characteristic is projected to grow into the billions of dollars by 2008 (Fig. 1). Market-research firm Frost and Sullivan pegs the genetic testing market of biometrics for biomedical applications at \$1 billion by 2007.

HOW SECURE ARE WE?

Biometrics uses various means of personal identification and verification, each providing different levels of authenticity. Fingerprinting, the most common

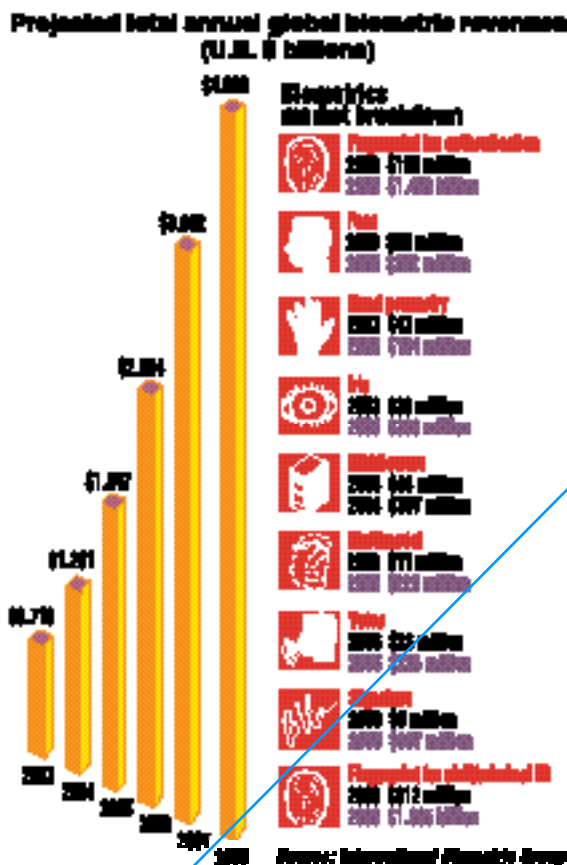
method, is turning in some impressive advances via capacitive, thermal, and optical means. Other biometric methods include facial feature recognition, eye iris scans, voice recognition, and even vein recognition.

Some of these techniques combine with personal data stored on databases, which are sometimes encrypted to increase system effectiveness. Other systems rely on implantable chips with RFID capability. This raises many red flags for privacy advocates, even though the technology can be very helpful in health-care services.

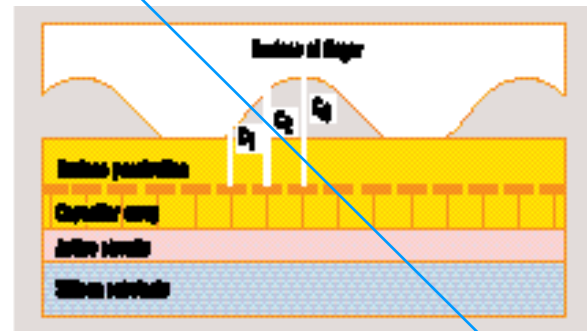
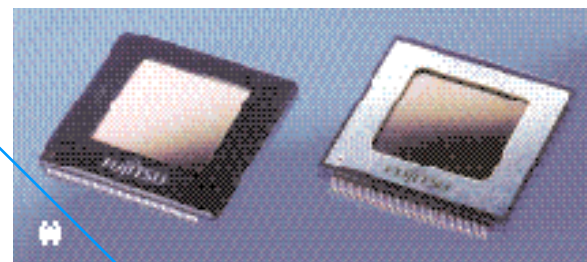
One recent innovation, Fujitsu's MBF200 sensor, relies on capacitance sensing (Fig. 2). According to the company, this sensor is well suited for scanning latent fingerprints and matching them against the prints of several thousand people on a watch list.

Products from Atmel use thermal-swipe sensing, which measures the temperature differences between ambient conditions and a fingerprint's valleys and ridges. Kinetics Sciences' products employ an optical-swipe method, which includes a light source, a prism, a focusing lens, and dual linear arrays of light sensors for low-cost sensing with forensic-quality images that feature resolutions up to 1000 dots/in.

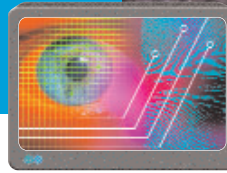
AuthenTec's optical TruePrint technology provides “true” identity capability (Fig. 3). The company claims that it is the only system in mass production with an accurate fingerprint technology.



1. Projected global annual biometric revenues show fingerprinting for authentication and for civil/criminal applications as the fastest growing segment among all biometrics markets by 2008. (Source: The International Biometric Group's Market and Industry Report, 2004-2008)



2. Fujitsu's MBF200 fingerprint sensor (a) uses capacitive sensing technology that's integrated on top of a silicon substrate (b).



INSIDE THE INDUSTRY



EVAN SCOTT
President,
Evan Scott Group International

BIOMETRICS BRING NEW BENEFITS AND CHALLENGES

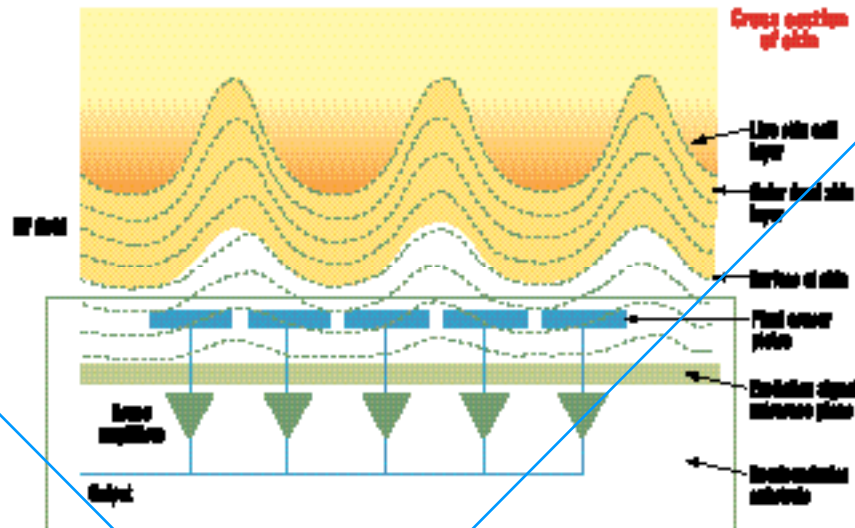
Fingerprint scanning—the main method of biometric verification for many years—is no longer the only means of identifying a person. Now there's iris and facial recognition, voice recognition, vein recognition, embedded RFID chips, and smart ID cards. Down the road, embedded genetic chips will identify us to the most exacting levels. All of this new technology has emerged due to the need for greater security for our citizens, government, and financial institutions.

The creation of the U.S. Department of Homeland Security has challenged the federal government's ability to bring cohesive security solutions to our nation's infrastructure and computer networks. Major investments are being made in protecting our private and commercial networks and in how organizations use information. The advent of the U.S. Congress' Oxley Sarbanes Act and the attendant need to build a careful accounting trail is further fueling the need for valid biometric identification and verification.

As a result of these efforts, Americans face many issues of privacy versus protection of their physical and monetary assets. We face a world where corporate corruption has forced unparalleled controls upon companies. The terrorist attacks of September 11, 2001 have opened our citizens up to greater scrutiny as well.

While the protection of individual rights is always in jeopardy, I believe that we must trust our systems of checks and balances to keep our country the strongest and most free nation on earth. Some might argue that it's no longer safe to trust our government, or "Big Brother," given recent revelations of government scandals at all levels—municipal, county, state, and federal. But what other means do we have to keep our nation strong? In the long run, our system of checks and balances will prevail and ensure our freedom.

ED Online 10604



3. TruePrint fingerprint optical sensing technology developed by AuthenTec relies on pixel sensor plates that recognize fingerprint patterns deep below the skin's surface for accurate verification of individual identities.

In a different twist, South Korea's Techsphere opts for vein sensing as a means of identification. The idea is based on the fact that each person has a unique vein pattern, like fingerprints. Infrared cameras can capture this pattern when subjects hold their hand up to a scanner. This is popular in South Korea and Japan, mainly for cultural reasons, due to concerns about hygiene issues involving touching a sensor with fingertips.

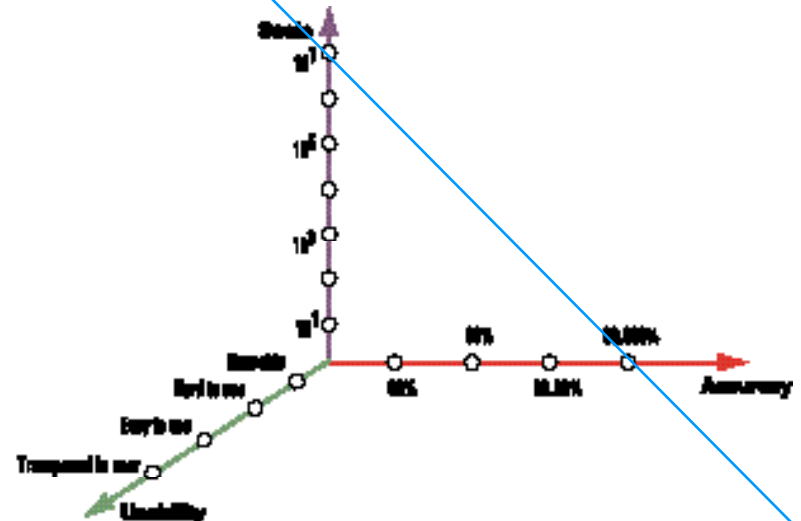
The Beepcard Company designed a credit card that works only when it recognizes its owner's voice. The card has a tiny microphone, a loudspeaker, and a speech-recognition chip that compares the spoken password with a recorded sample. It combines this with encrypted personal data from the user's previ-

ous registration. But as impressive as speech recognition is today, it must be refined further to achieve the needed accuracy and reliability levels.

Researchers at Michigan State University, who have investigated all kinds of biometric approaches, concluded that the grand challenge is a biometric system that would operate simultaneously on the extremes of all three axes of usability, accuracy, and scalability (Fig. 4). They caution that no biometric system is 100% foolproof, though. Currently, they're developing a system that fuses together several biometrics to enhance accuracy.

The system first uses a pair of cameras to gauge a person's height. At this point, a closeup of the face is taken. Next, software analyzes and enhances this

4. According to researchers at Michigan State University, no biometrics method is 100% foolproof. However, a biometrics approach can be very accurate and effective when accuracy, scale factor, and usability issues are maximized in a biometrics system's design.



data to determine the subject's eye color, gender, and ethnicity. Then the data is combined with primary biometric, hand geometry, and face-recognition and fingerprint data.

APPLICATIONS APPEAR

Biometrics is so commonplace, it's being designed into consumer electronics like notebook computers, DVDs, cell phones, and disk drives. AuthenTec's EntréPad 1530, one of the smallest fingerprint sensors, is used on many LG Electronics and NTT Docomo cell phones (Fig. 5). The company's sensors also are finding their way into Toshiba's ultra-portable Protégé and mini Libretto U100 notebook computers.

Customers at the Edeka German supermarket chain soon will be able to pay for their shopping by placing their fingerprints on a scanner at the checkout counters. The company has piloted the technology since last November, and it is now ready to equip all of its stores. Several supermarket chains in the U.S. have piloted similar systems (see "Biometric Identification: How Safe Are Your Fingers?" April 28, p. 19, ED Online 10190).

Medical uses have sparked some controversy, too. Last October, the U.S. Food and Drug Administration (FDA) approved Applied Digital Solutions' implantable VeriChip. The device gives medical personnel instant access to a patient's medical records via RFID technology (Fig. 6). Privacy advocates question the need for such a device, wondering what problem the technology actually solves. They also question patients' needs to give medical personnel "carte blanche" and instant access to their medical records, because they're purportedly the only people legally authorized to provide access to those records after being asked.



5. Biometrics sensors are finding greater use in consumer electronics items like cell phones. LG Electronics' 3550 and 3800 cell phones (a) and NTT Docomo's 900iC cell phones (b) are just a couple of examples. These phones use AuthenTec's EntréPad 1530 optical sensor.

WHAT'S IN THE WORKS?

With research on nanotechnology proceeding at a breakneck pace, we may well be in for some surprises in a few more years. Nanotechnology scientists at Lucent Technologies' New Jersey Nanotechnology Consortium, in collaboration with the University of Illinois, are attempting to get an entire human genome on a chip or CD. The project includes \$1.6 million in funding from the U.S. Defense Advanced Research

Projects Agency (DARPA). The device can sequence a person's DNA in seconds. The genome decoder would require a speedy sensor that can identify biological agents. According to its developers, customers will eventually be able to walk into a clinic, provide a DNA sample, and then for a few walk out moments later with a CD bearing their genetic data. One thing is clear. There's no stopping the biometrics boom. Prepare for some sort of backlash, though, as personal privacy becomes a potential target for abuse.



6. Applied Digital Solutions' VeriChip, which is smaller than a penny, can be embedded under a patient's skin. Using RFID technology, this biometric chip gives medical personnel instant access to a patient's medical records.

Portable power

LITHIUM ION Rechargeable
3.6V cylindrical or prismatic types, higher energy density provide more power in a smaller and lighter cell.



NICKEL METAL HYDRIDE

Rechargeable
1.2V cylindrical type, higher capacity and greater rapid charge capabilities than NiCd.



NICKEL CADMIUM

Rechargeable
1.2V, a wide range of sizes and capacities, excellent power performance value.



LITHIUM COIN

Rechargeable
Available in four different chemistries, 3 voltages (1.5V, 2.5V, 3V), and a variety of sizes and tab configurations.



LITHIUM COIN Primary

5V, available in either BR or CR types with a wide variety of sizes and tab configurations. Wider operating temperature windows of the BR type are also available.



LITHIUM CYLINDRICAL Primary

3V and 6V, available in BR and CR types for user replaceable or memory back up applications.



VOLTAE REGULATED LEAD ACID

Rechargeable 12V and 6V versions in a wide range of capacities for trickle or cycle use.



Parasource
Ideas for life

Toll Free 1-877-726-2228 (1-877-PANASONIC)
e-mail: pan_batteries@na.panasonic.com
url: www.panasonic.com/na/batteries