

MEDIA FOR

LaserFocusWorld



Security concerns drive biometrics into the mainstream

Kathy Kincade

Face recognition has become the leading contender for large-population surveillance applications.

Traditionally defined as "the statistical analysis of biological observations and human phenomena," the concept of biometrics has been around for centuries. One of the first recorded examples was a form of ink-based hand and foot printing used by Chinese merchants in the 14th century to distinguish young children from one another. In the late 1800s, Alphonse Bertillion developed a method of body measurement to identify criminals who adopted aliases to escape detection. About the same time, Richard Edward Henry of Scotland Yard developed the fingerprinting method still used in law enforcement and forensics.

Today the field of biometrics includes several approaches for recording and comparing human characteristics (eye, hand, face, ear, gait, voice, signature) for identification, verification, and analytical purposes (see "Biometrics center looks beyond security applications," p. 98). While biometric applications actually range from law enforcement to the study of biological phenomena, the events of Sept. 11, 2001, have shifted commercial development of this technology to security applications.¹

This trend, which is being echoed globally, has opened up the market for physical biometrics and identity management. According to the International Biometric Group (New York, NY), global biometric revenues are expected to reach \$4 billion by 2007, although it is unclear how much of this growth will encompass optical technologies. But from optical sensors for fingerprinting to infrared detectors and high-speed CCD cameras for iris and face recognition, optoelectronics is being increasingly deployed to meet the demand for faster image acquisition, better resolution, and more accurate matching.

The best approach

For security applications, physical biometrics is important because certain human features are nearly impossible to falsify. Fingerprints, face, hand geometry, iris, palm prints, signature, and voice can be used to identify and verify individuals for access control (entry to buildings, computers, cell phones, and so forth) and for surveillance (finding or monitoring a specific individual in a public place). In each approach, the process comprises three main steps: the image is captured, converted into a template, and the template is matched against a database of stored records for authentication (one-to-one matching) or identification (one-to-many matching). Only finger, iris, and face biometrics are capable of performing one-to-many matching, an important distinction for security and forensics applications.

"Each application area requires different considerations," said Frances Zelazny, director of corporate communications for Identix (Minnetonka, MN), a developer of fingerprint and face recognition

systems. "Most of the criticism is really hitting on the surveillance aspect, which has the most variables affecting performance. The very nature of surveillance is that you are trying to catch people who do not want to be identified, in contrast to access control, in which someone is trying to get into their computer or office building and is willing to be an active participant."

As a result, face recognition (FR) has emerged as the leading contender for surveillance applications—such as trying to locate a potential terrorist at an airport—largely because it requires no conscious participation from the individual being sought and because it is often easier to obtain a photo of someone than a fingerprint or iris scan. And although FR technology is criticized as not yet accurate enough for large-scale security applications, cameras, computers, and image-processing algorithms have evolved to the point at which commercially available systems are fast, relatively inexpensive, easy to install, and unobtrusive. More important, ongoing R&D efforts are yielding additional advances in the accuracy of FR, most notably the ability to accommodate changes in environmental and human variables such as lighting, distance, angle, weight, age, eyewear, and facial hair.



FIGURE 1. Two-dimensional face recognition is being used increasingly for access control in buildings and public transportation because lighting, pose, and expression can be controlled and the subjects are willing participants.

A typical FR system works by first enrolling a subject—acquiring several facial images (ideally at various angles with different facial expressions) using a high-resolution camera; measuring unique characteristics of the face, such as the distance between the eyes, the length of the nose, and the angle of the jaw; creating a computerized template based on 30 or so such markers; and comparing the template to an image database (see Fig. 1). Image acquisition is particularly important in facial recognition because overall outcomes are closely tied to image quality; low-quality images are more likely to result in enrollment and matching errors, making variables such as lighting and pose critical.

"If you don't have enough resolution in the camera, you are only going to see a face a certain way," said David Tunnell, vice president of government solutions at Genex Technologies (Kensington, MD), which has been developing 3-D technologies for more than eight years. "And if you don't have the right optics, detectors, and sensors, you are going to be limited in what you can do."

Currently, most face-recognition systems work in two dimensions using eigenface, local feature analysis, neural-network mapping, or automatic face-processing algorithms. Although they are well suited to forensics and access-control applications, 2-D FR systems are limited when it comes to surveillance.

In particular, they have difficulty accommodating variables such as poor lighting, distance from the

camera, changes in facial expression, or angle of view.^{2, 3}

"The fundamental core algorithms of modeling logic and computer vision are the limiting factors," said Mohamed Lazzouni, vice president of engineering for Viisage (Littleton, MA). "This industry has a tendency to take one model, such as rigid body motion, and stretch it so it applies to many things. People expect that if it works well for complete face movement, it will work well for a smile. But the rules governing the two are very different."

2-D vs. 3-D

These issues have prompted several R&D and commercial groups to turn to three-dimensional modeling to improve face recognition. Proponents contend that 3-D imaging can better adjust for variables such as angle, pose, movement, aging, and light. Genex Technologies, for example, is using 3-D enrollment images to improve the performance of existing 2-D facial recognition (see Fig. 2). Working from a single 3-D image, the company has developed an algorithm that creates a variety of 2-D images, accurately displaying the face as if several 2-D photos had been taken from different angles under different lighting conditions.

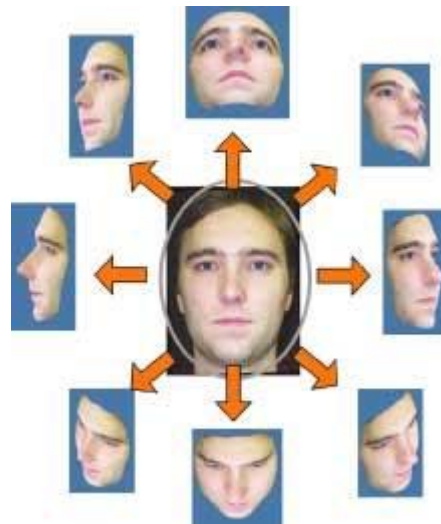


FIGURE 2. Because 2-D facial recognition does not work well when the enrolled image is different from the probe image in pose, lighting, and/or expression, companies such as Genex Technologies have developed software that can convert a 2-D picture into a 3-D face image for enrollment.

"Rather than force the infrastructure to change by purchasing all-new surveillance cameras and software, the goal is to improve 2-D facial recognition using existing 2-D infrastructure," Tunnell said. "We also have 3-D morphing capabilities that can change the face almost limitlessly, which is very valuable in predicting what a face will do over time."

The next step, he says, is to correct for the lighting in an image, then to be able to capture 3-D data accurately from a distance and develop true 3-D algorithms that can match a face in 3-D. "This is where we see FR in the next few years: 3-D enrollment cameras, 3-D surveillance cameras, and 3-D

facial-recognition algorithms," Tunnell said.

3DBiometrics (Boulder, CO) believes it already has true 3-D face-recognition technology. According to the company, most 3-D facial recognition companies use neural networks to generate 3-D images, measuring only 200 or so points on a face. 3DBiometrics says its system can take tens of thousands of points on the face in less than one second, creating a "mask" of the face that can be rotated during matching to yield higher accuracy and less dependence on factors such as lighting, angle, and facial characteristics.

"We are talking about measuring volume, not flat surfaces, which can make a big difference if the camera is off a few degrees or you don't get a full face shot," said Jack Earl, president of 3DBiometrics.

Another commercial venture, A4Vision (Cupertino, CA), is also developing 3-D technologies for face recognition. The company's system includes a 3-D surface scanner that utilizes a near-infrared laser and structured lighting method; it works by projecting near IR light through an optic with a grid pattern on it that is transferred onto the subject, then capturing the resulting images and transferring them to the computer for matching (see Fig. 3).

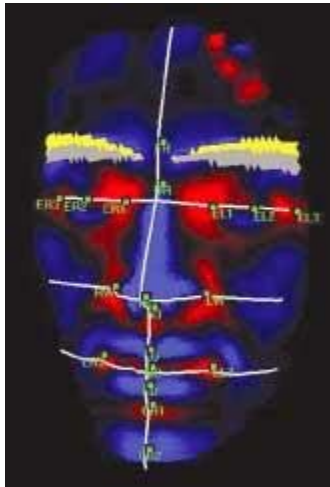


FIGURE 3. Three-dimensional facial biometrics is based on anthropometric data—precise measurements of the cranial structure. Research has shown that only 14 facial features are required to uniquely identify a target in a population of 4 million subjects.

"All 3-D systems project their own light—flashed, pulsed, static laser, colored rainbow; we use near infrared," said Grant Evans, A4Vision CEO. "The advantage is that we can work at night, while 2-D systems cannot function without lots of light. The disadvantage we have with near IR is distance; our system can go about 6 ft, which drives us to a particular application: short-distance ID."

But even at short distances, Evans believes his company's machine-vision approach, which includes

real-time video feed from a single camera to create a 20,000-point grid of the face, offers several advantages over other biometric identification methods. "Instead of a static image running against a database, we take 5 to 20 frames per second, so there is constant verification," he said. "As far as I know, we are the only company that has an identification engine in 3-D."

In the long run, however, most biometrics developers believe that a multimodality approach that combines two or more techniques will prove to be the best, especially for verification and authentication. Under new laws being implemented in the United States and Europe, for example, passports and visas will now be required to include both finger-scanning and face-recognition biometrics, while identity cards now being issued in Britain will contain both finger and iris scans.

REFERENCES

1. "Prepare to be scanned," *The Economist* (Dec. 4, 2003).
2. S. Berinato, "Face recognition hype is over," *CIO Magazine* (Nov. 1, 2003).
3. www.frvt.org

Biometrics center looks beyond security

While current culture has spurred the development of biometrics for security applications, the term is actually derived from the Greek words bio ("life") and metric ("to measure"). With \$1.3 million in initial funding, the newly established Center for Unified Biometrics and Sensors (CUBS) at the University at Buffalo (New York) is taking a cross-disciplinary approach to biometrics that is expected to push the technology well beyond its current applications—even into protein analysis for disease detection.

"Because of 9/11, biometrics has come to mean the identification of people," said Alex Cartwright, associate professor of electrical engineering at the University at Buffalo. "But we see it as the identification of any biological phenomenon. We are looking not just at homeland security but comfort and convenience applications."

According to CUBS director Venu Govindaraju, UB professor of computer science and engineering and CUBS director, the application should dictate the kinds of sensors needed, how they should be packaged, the level of "intelligence" they require, and how much security is required to transmit the information. This approach differs from other biometrics research efforts, where a single technology is developed and marketed for a range of applications.

Researchers at CUBS are already developing new biometrics, such as chemical and biological sensors designed to detect and quantify the presence of various pharmaceuticals and their metabolites, toxins, blood type, and even chemical residues on the skin. Other potential projects include an integrated biometric platform that uses multiple miniaturized sensors to acquire various biometrics, such as face, speech, fingerprints, gait, and writing habits; pathobiometric systems that can track illnesses in livestock, such as mad cow disease, by analyzing aerial images of large herds; and methods that automatically flag suspicious patterns among patients entering the emergency medical system, providing clues to terrorist attacks or epidemics of new diseases such as SARS. –KK

Laser Focus World February, 2004

Interested in a subscription to *Laser Focus World Magazine*?
[Click here](#) to subscribe!

Links referenced within this article

Click here

<http://www.ameda.com/cgi-win/lfw.cgi?add&p=webedit>

Find this article at:

[http://lfw.pennnet.com/Articles/Article_Display.cfm?](http://lfw.pennnet.com/Articles/Article_Display.cfm?Section=ARCHI&Subsection=Display&ARTICLE_ID=199267&KEYWORD=genex&p=12)

[Section=ARCHI&Subsection=Display&ARTICLE_ID=199267&KEYWORD=genex&p=12](http://lfw.pennnet.com/Articles/Article_Display.cfm?Section=ARCHI&Subsection=Display&ARTICLE_ID=199267&KEYWORD=genex&p=12)

Uncheck the box to remove the list of links referenced in the article.

MEDIA FOR