Powered by Dialog

Biometrics Rapidly Evolve as Technological Means to Identify People
Jill Kester Locantore
KRTBN KNIGHT-RIDDER TRIBUNE BUSINESS NEWS (RICHMOND TIMES-DISPATCH - VIRGINIA) , November 15, 2001

Imagine you are about to embark on a vacation to Europe. You walk out to the garage and talk to your car. Recognizing your voice, the car doors unlock.

On the way to the airport, you stop at an ATM. A camera mounted on the bank machine looks you in the eye, recognizes the pattern of specks on your iris and allows you to withdraw cash from your account.

When you enter the airport, a hidden camera compares the digitized image of your face to that of known or suspected terrorists.

At the immigration checkpoint, you swipe a card and place your hand on a small metal surface. The geometry of your hand matches the code on the card, and the gate opens. You're on your way.

Sound futuristic? Well, the future is here.

Biometrics are rapidly evolving computerized technologies that identify people based on physical characteristics such as fingerprints, facial features, voice patterns, hand geometry or features of the eye. They already are being used in a variety of situations that normally require keys, passcodes or manned checkpoints.

According to proponents, biometrics increase security and convenience, and soon will be widely available for use at home, in the office and for retail and online purchases. The recent terrorist attacks have many experts calling for increased use of biometrics in airport security and surveillance applications. Some even propose national ID cards encoded with biometric information.

Low-tech biometrics are nothing new. People identify individuals based on their physical characteristics all the time. Recognizing the face, voice or even the gait of a close friend is so effortless we take it for granted. Even infants use characteristics such as voice to recognize their mothers.

Getting a computerized device to recognize a person is a whole different kettle of fish.

The first step in any biometric technology is capturing an image of a body part, or recording a behavior. Often this simply involves taking a picture with a camera. In some cases, just locating the appropriate body part, such as the face or eye, can be the trickiest part for an automated system.

Next, various features of the body part or behavior are recorded -- such as the pattern of specks that characterize an iris, or pitch and cadence patterns that characterize an individual's speech. Through a nifty series of calculations, referred to as an "algorithm," these features are extracted and converted into a sequence of numbers.

This number sequence, or "template," is stored in a computer database or on a "smart card" and later used to identify the individual.

For example, frequent travelers in the Netherlands' Amsterdam airport can have a template of their iris stored on an ID card. Each time they visit the airport, they present their eye to an iris scanner, and if the live template matches the template stored on the card, they are allowed to bypass long immigration lines. The whole process takes only seconds.

The security advantage of biometrics derives from the intimate connection between a person and his or her body. Body parts cannot be forgotten or misplaced, and are difficult to steal or copy.

"It really allows you to associate your identity in a reliable way with some kind of a transaction or an activity," said Lawrence Hornak, coordinator of the biometrics program at West Virginia University.

However, biometrics are not foolproof. A picture of a face or an iris may pass for the real thing. Voice scanners can be fooled by a sophisticated tape recording. And hand and finger scanners might accept a cast of the body part, or more gruesomely, a severed body part.

To counteract these kinds of fraud, some biometrics includes checks for signs of life. For example, face scanners may require the eyes to blink, iris scanners might look for small changes in pupil dilation, and finger scanners might measure blood flow.

Even so, like all computerized systems, biometrics are vulnerable to skilled hackers.

"There's no technology that provides absolute security," Hornak said. "If a person has complete knowledge of the system, they can most likely circumvent it. (Biometrics) raise the level of expertise necessary to do that."

So biometric security measures might be difficult to defeat, but how accurate are they at identifying people? According to Jim Wayman, director of the National Biometric Test Center at San Jose State University in California, the answer is, "It depends."

Biometrics are susceptible to the same kinds of identification errors that people make -- both mistaking a stranger for a known person (false acceptance) or failing to recognize a known person (false rejection). False rejections can be quite annoying. Imagine if 10 percent of the time you went to withdraw money from the ATM, you were rejected because the machine failed to recognize you.

Biometric devices can be calibrated to reduce false rejection rates, but at the cost of increasing false acceptance rates. In other words, there is a tradeoff between convenience and security. High false rejection rates might be more tolerable in situations that demand high security, such as prisons. In consumer-oriented situations, slightly lower security might be tolerated for the sake of convenience.

Many biometrics vendors boast of error rates -- both false acceptance and false rejection -- that are well below 1 percent. However, those figures are usually based on ideal testing situations.

For example, voice recognition can be extremely accurate over the telephone -- if a hardwired, local network telephone is used in a quiet room. Accuracy can drop off precipitously if a cordless telephone is used, or if there is a lot of background noise.

For that reason, it's important to consider the environment in which a biometric will be used. In noisy

situations, face recognition might be more accurate than voice recognition. If the lighting is bad, finger or hand scanning might be more appropriate than face recognition.

Biometric developers also quibble about whether one part of the body is more or less distinctive than others, and therefore better suited for identification purposes. The iris, for instance, is often touted as more distinctive than a fingerprint.

Comparisons of that sort are difficult to make, Wayman said. It's hard to define what makes a body part distinctive. Ultimately, he suggests that "the cleverness in the approach used (to extract and encode features) is more important than distinctiveness of the body part."

Iris recognition is exceptionally accurate, Wayman said, because the feature extraction algorithm developed by John Daugman of Cambridge University is particularly clever. As researchers continue to develop better algorithms, biometric devices are becoming more accurate and better able to deal with varying conditions such as background noise or poor lighting.

No matter how accurate a biometric device is, the true identity of an individual is never completely certain, Wayman points out. An iris scanner might be able to tell you that the iris being scanned matches John Doe's iris. But how do you know who John Doe really is? You must depend on the information known about this John Doe character the first time his iris was scanned.

"It's not this magic bullet," Wayman said. "It's not going to replace trust in all human interactions." But biometrics just might make the world a little bit more secure.