BEYOND FINGERPRINTING

Security systems based on anatomical and behavioral characteristics may offer the best defense against identity theft

By Anil K. Jain and Sharath Pankanti

If you are like many people, navigating the complexities of everyday life depends on an array of cards and passwords that confirm your identity. But lose a card, and your ATM will refuse to give you money. Forget a password, and your own computer may balk at your command. Allow your cards or passwords to fall into the wrong hands, and what were intended to be security measures can become the tools of fraud or identity theft. Biometrics—the automated recognition of people via distinctive anatomical and behavioral traits—has the potential to overcome many of these problems.

Compared with a physical token such as a bank card or with the knowledge of a secret such as a PIN, biometric traits are profoundly more difficult to forge, copy, share, misplace or guess. Indeed, they offer the only way of determining whether a person has been issued multiple official documents, such as a driver’s license or passport, under different names. Yet they are quite easy to use as proof of identity. For these reasons, biometric systems have been gaining popularity in recent years. Laptops and mobile phones that can recognize a fingerprint, for instance, are now commercially available. In some countries biometric security is employed to safeguard items such as ATM cards and passports, to determine whether a person can rightfully enter a building or to ensure that someone is entitled to welfare payments. These systems are far from perfect. But with inexpensive sensors and powerful microprocessors now available, biometric technology is certain to become more pervasive.

Measures of Man

Biometrics is not a new idea. In 1879 Alphonse Bertillon, a French police inspector, proposed a complicated system of body measurements—arm and foot length among them—to identify repeat offenders. Over the next decade British scholars established that each print of a finger exhibits a unique pattern that persists over time, setting the stage for the development of the fingerprint classification system in 1896. Shortly thereafter, Scotland Yard began collecting fingerprints left at crime scenes to pinpoint criminals. And today almost every law-enforcement organization in the world relies on fingerprints to identify wrongdoers, solve crimes and conduct background checks on people applying for sensitive jobs.

But fingerprints are not the metric of choice for every purpose; several other physical and behavioral features have also been incorporated, singly or in tandem, into ID systems. The current emphasis in biometrics is to design fully automatic systems that are extremely fast, accurate, user-friendly and cost-effective and that can be

KEY CONCEPTS

- Biometric identification systems are harder to circumvent and easier to use than are traditional systems based on ID cards and passwords.
- Now that economical and powerful microprocessors are available, the technology is spreading.
- Before these biometric systems can reach their full potential, though, developers will have to lower their error rates.

—The Editors
embedded in existing security infrastructures. In addition to fingerprinting, workers in the past 30 years have developed ID systems based on such characteristics as the face, hand, voice and iris (the colored part of the eye).

Biometric systems require traits with two basic features: they must be unique for each person, and they must not change significantly with time. Some traits promote relatively high accuracy, others greater practicality or relatively low cost. The choice of trait to favor as an identifier therefore depends on the goals of the ID system. No single measurement is optimal for all applications.

Consider the three most popular traits in use today: the fingerprint, the face and the iris. In addition to its use in forensics, fingerprint recognition forms the basis of automated border-control systems in a number of countries. In the U.S. alone, the Department of Homeland Security's US-VISIT program has processed more than 75 million visitors since its debut in 2004. From a commercial standpoint, one of the biggest advantages of using fingerprints is that the sensors for capturing prints are now extremely cheap (around $5) and small enough to be embedded in consumer products such as laptops, mobile phones and even flash-memory sticks. But these compact sensors have higher error rates than their larger, more expensive counter-
[COMPARING TRAITS]

HOW THE METRICS MEASURE UP

The choice of a biometric trait or traits to use in a security system depends on the application; the strengths and weaknesses of each of the four most common biometric identifiers are summarized in the table below. For example, compared with fingerprint recognition, iris recognition allows access to the wrong people less often but currently requires larger and costlier sensors and thus cannot be as easily incorporated into a laptop or other consumer device. Experts concur that in an ideal biometric authentication system, neither the “false accept” rate nor the “false reject” rate should exceed 0.1 percent. In tests conducted by the National Institute of Standards and Technology, however, none of the systems satisfied these error rate requirements.

<table>
<thead>
<tr>
<th>Property</th>
<th>Fingerprint</th>
<th>Face</th>
<th>Iris</th>
<th>Voice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distinctiveness</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Permanence</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>How well trait can be sensed</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Speed and cost efficiency of system</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Willingness of people to have trait used</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Difficulty of spoofing the trait</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>False reject rate*</td>
<td>0.4 percent</td>
<td>1.0–2.5 percent</td>
<td>1.1–1.4 percent</td>
<td>5–10 percent</td>
</tr>
<tr>
<td>False accept rate*</td>
<td>0.1 percent</td>
<td>0.1 percent</td>
<td>0.1 percent</td>
<td>2–5 percent</td>
</tr>
</tbody>
</table>

*Error rates depend on testing environment, sensors used and composition of users in the population.

Parts common in law enforcement, because they scan a smaller portion of the finger and the image they record is lower in resolution.

Face recognition is gaining popularity as a security feature for computers and mobile phones, partly because it can take advantage of the built-in cameras that are becoming ubiquitous components of these devices. ID systems based on face recognition are quite accurate when the images are captured under controlled conditions—with the subject facing forward in indoor lighting and bearing a neutral expression, for example. They falter, however, when the original image and the newer one differ because of changes in pose, lighting, expression, age, and facial accessories such as glasses or a beard. This sensitivity to routine variations is particularly problematic for video surveillance, in which subjects do not present themselves in front of the camera in predetermined poses. Perhaps within 10 years the technology will have advanced sufficiently to permit fully automated, real-time face matching in video surveillance.

As for the iris—whose complex, textured pattern is thought to be unique to each person as well as permanent—recognition is extremely
accurate and swift. The subject simply looks into a scanner for a few seconds; the captured pattern is then analyzed and recorded. Matching is done by comparing a person's bit sequence to the sequences in a database. The speed and accuracy of this approach have driven the recent development of large-scale ID systems based on the iris, including the Iris Recognition Immigration System (IRIS) in the U.K. Travelers enrolled in the system's database can sidestep the usual immigration channels at the airport, thereby cutting down on travel wait time.

Iris recognition has its downsides, however. The method depends, for instance, on the use of algorithms that represent the random patterns in the iris as a sequence of bits—no known human experts can determine whether or not two iris images match. Hence, iris data are unsuitable for use as evidence in a court of law.

**Imperfect Matches**

Developers of biometric systems face other difficulties as well. Unlike ID systems requiring a password or a physical token, biometric systems generally have to make decisions on the basis of imperfect matches. Any system of comparison can lead to two basic types of error. In a "false accept" error, the system incorrectly declares a successful match between the input pattern and a pattern in the database that does not really match it. In a "false reject" error, the system incorrectly pronounces a failed match between the input pattern and a genuine match in the database.

Experts generally agree that neither the false accept rate nor the false reject rate of a biometric authentication system should exceed 0.1 percent (that is, one mistake in 1,000 assertions of a match and one mistake in 1,000 assertions of a nonmatch). But in evaluations conducted by the National Institute of Standards and Technology between 2003 and 2006, error rates for systems based on the fingerprint, face, iris and voice—an (commonly used biometric trait—all exceeded the 0.1 percent level [see box on opposite page].

Increasing the threshold score for a match can lower the false accept rates, but at the expense of increasing the false rejects. Reducing both error rates simultaneously will require developing biometric sensors that generate higher-quality images and refining the feature extractors and matchers. Designers will also need to ensure that the systems are protected against sabotage: ideally, it should be impossi-

---

**MORE TO EXPLORE**


---

**The Privacy Conundrum**

The use of biometrics raises important privacy concerns. Who owns the data—the individual or the service providers? Will these data be used for an unintended purpose—to deduce something about a person's health, for instance? Biometric systems of the future will probably operate unobtrusively, capturing biometric traits without the active involvement of the user. Such stealth further confounds the privacy issue.

At present we see no concrete, viable solutions on the horizon for addressing the entire spectrum of privacy concerns. We believe these problems can be resolved through public discussion and policy making, however. They will have to be. It is only a matter of time before continued improvements to biometric tools will move them center stage in efforts to combat the rampant problems of security and identity fraud that our society faces.