Biometric Authentication

Alfred C. Weaver
University of Virginia

Biometric authentication is here to stay, and so is the controversy it engenders regarding invasion of privacy.

In this age of digital impersonation, biometric techniques are being used increasingly as a hedge against identity theft. The premise is that a biometric—a measurable physical characteristic or behavioral trait—is a more reliable indicator of identity than legacy systems such as passwords and PINs. That's why you see fingerprint-based payment systems being installed in grocery stores and at passport control stations at border crossings. It's also why Canada is investing $10 million to capture fingerprints and iris scans for its 120,000 airport workers.

There are three general ways to identify yourself to a computer system, based on what you know, what you have, or who you are. "What you know" approaches such as passwords and PINs are low-reliability techniques because they can be lost, stolen, or guessed. "What you have" technologies such as RFID cards and e-tokens—identity information encrypted on a flash memory card—also can be stolen. Thus, developers usually implement these systems as part of a "two-factor" identification scheme that pairs a what-you-have technique (e-token) with a what-you-know technique (password).

Biometrics belong to the "who you are" class and can be subdivided into behavioral and physiological approaches. Behavioral approaches include signature recognition, voice recognition, keystroke dynamics, and gait analysis. Physiological approaches include fingerprints; iris and retina scans; hand, finger, face, and ear geometry; hand vein and nail bed recognition; DNA; and palm prints. Here, we focus on the two most popular biometric techniques: fingerprints and iris scans.

COVERING THE BASICS

Before discussing the details, we need to cover some basics. First, how are scanned biometric samples associated with people? This is the purpose of enrollment—an established protocol for gathering a reliable biometric sample and registering it against a claim of identity. At the commercial level, this can be as simple as the convenience store clerk instructing the user to provide three scans of an index finger (for averaging purposes) and then associating that result with identity information taken from a driver's license and banking information read from a check.

The more sensitive the information a biometric technology is going to access, the more rigorous the enrollment process must be. There is no security in a fingerprint-based payment system if the enrollment clerk, by negligence or malign intent, lets me enroll my brother's fingerprints as my own.

Second, how is the sample stored? Biometric samples are reduced to mathematical templates (around 256 bytes for a fingerprint and 512 bytes for an iris scan), and the system stores only this "enrolled template." This reduces the probability of a *replay attack*, whereby someone steals the raw biometric scan and then replays it electronically to impersonate an individual not physically present.

Third, what constitutes a match between the biometric presented—the "bid sample"—and the enrolled template? The system should not require a perfect match because the bid sample and enrolled template most likely will not be identical. For example, in the case of a fingerprint, the samples will differ based on the fingertip area that any particular scan covers and the degree of compression of the ridges that results from varying pressure during the scan.

Instead, whether a match is asserted depends upon the *Hamming distance*—the degree of difference—between the bid sample and the enrolled template. The technology's manufacturer sets the degree of equality required to define a match based on extensive experimentation with the technology in general and the scanning device in particular. The definition of *match* is always a probabilistic concept—just as it is with human comparison of fingerprints.

Two other characteristics are important:

- *false acceptance rate* (FAR), the fraction of access attempts by an unenrolled individual that are nevertheless deemed a match; and
- *false rejection rate* (FRR), the fraction of access attempts by a legitimately enrolled individual that are nevertheless rejected.

Clearly, the FAR must be very, very low to provide any confidence in the technology, and the FRR must be sufficiently low that the user will not abandon the technique due to frustration.

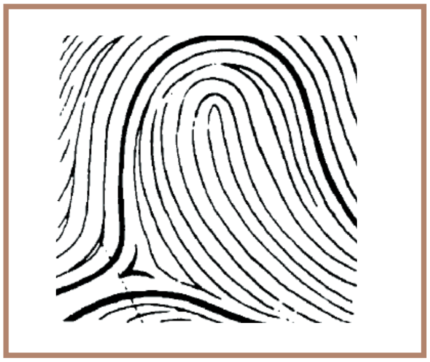

Figure 1. Fingerprint with ridge patterns and minutia points—the tiny, unique characteristics of fingerprint ridges.

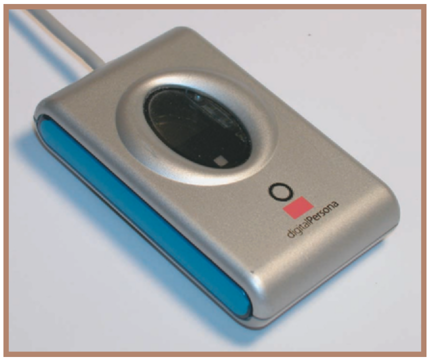

Figure 2. Digital Persona U.are.U Pro fingerprint scanner. Fingerprint scanners can be attached to USB ports as an external peripheral or they can be embedded within devices.

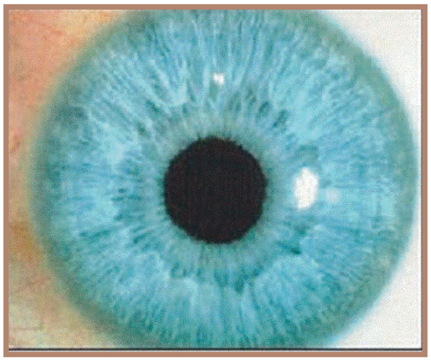

Figure 3. Pupil and surrounding iris. Iris scans analyze the iris's vein patterns, potentially providing even more accurate identification than fingerprints because the iris has about 260 degrees of freedom with regard to its vein patterns.

FINGERPRINTS

Fingerprints have been used to secure commercial transactions since the days of ancient Babylon, where fingerprints have been found among the ruins on clay seals attached to business documents. Each fingerprint contains global features, which can be seen with the naked eye, and local features, also called minutia points, the tiny, unique characteristics of fingerprint ridges. As Figure 1 shows, ridge patterns can be loops, arches, or whorls; minutia types associated with a ridge pattern include ridge endings, bifurcations, divergences (ridges so small that they appear as dots or islands), and enclosures (ridges that bifurcate and reunite around a ridgeless area).

While two or more fingerprints can have the same global features, no known pair, at least since the first criminal fingerprint identification was made in 1892, have the same minutia. Fingerprint scanners detect ridge patterns and minutia and then characterize the minutia based upon orientation (the direction the minutia are facing), spatial frequency (how far apart the ridges are around a particular mark), curvature (rate of orientation change), and position (*X*,*Y* location relative to some fixed point). There are about 60 to 70 minutia points on each finger, and even identical twins have different minutia points.

These data describing the minutia provide the essential components of the template computed from the enrollment and bid samples. Whereas police fingerprinting stores the entire image, fingerprint scanning systems store only the template. An original image cannot be constructed from its data template alone.

Fingerprint scanners such as the Digital Persona U.are.U Pro model shown in Figure 2 are increasingly common. This unit has an advertised FAR of 0.01 percent and an FRR of 1.4 percent. Fingerprint scanners can be attached to USB ports as an external peripheral or they can be embedded within devices, as in the HP iPAQ 5550 and the IBM Thinkpad T42.

IRIS SCANS

Figure 3 shows the iris—the colored part of the eye surrounding the pupil. Iris scans, which analyze the iris's vein pattern, have the potential to be even more accurate than fingerprints because the iris has about 260 degrees of freedom with regard to its vein patterns. Using an iris scanner requires aligning the eye with a colored LED inside the camera, then moving the person's head forward or back until the LED changes color, signaling that the distance is correct for proper imaging. The system then makes the scan, analyzes the image, and stores the template.

Just as a person has 10 different fingerprints, each human has two distinct iris patterns, even identical twins; thus, it is impossible to enroll with the left eye and authenticate with the right. Even though the visible portion of the iris changes as a function of pupil dilation, this does not adversely affect authentication. Eyeglasses and contact lenses do not reduce accuracy as long as the iris is clearly visible.

Biometric authentication is here to stay, and so is the controversy it engenders regarding invasion of privacy. Critics say that biometric data gathered for one purpose—say, fingerprints taken from noncitizens who enter the US under the US-VISIT program—are too easily repurposed for applications such as criminal identification. Proponents say that current "best practices" such as not storing the fingerprint or iris scan, but only its data template, are adequate for protecting personal privacy.

As is usual with new technologies, members of the public must decide for themselves whether the reliability and convenience of biometric-based services are worth leaving behind a digital trace of their identity. ■

Alfred C. Weaver is a professor of computer science at the University of Virginia. Contact him at weaver@cs.virginia.edu.