What Is Biometrics?

Biometrics is the measurement of the biological characteristics of human beings. The term has gained much attention beyond scientists in the last two decades because of its increasing use in information technology applications, primarily to authenticate users. Although biometrics can be used to measure any human characteristic or the characteristics of a group of people, in information technology, it is usually applied to unique human features like voice and fingerprint to prove that the individual being measured is genuine.

Biometrics in Authentication

Biometrics is increasingly used to authenticate individuals for granting access to secured information or facilities. It is one of the stronger types of authentication, especially when compared to passwords or photo identification. Common facilities that use biometrics include computer rooms, health clubs, and military sites.

The technology supporting biometrics in authentication has significantly improved in the last decade and is affordable to most organizations, partly because of the increasing capacity and decreasing prices of personal computers and accessories. However, this technique is not widely used and has not surpassed passwords and smart cards in popularity because of a number of concerns not directly related to technology, one of which is privacy.

How Biometrics Works

For a person to be authenticated using biometrics, the physical feature being used must first be captured in a file. Data may be gathered with a scanner for fingerprint, a recorder for voice, or a scale for weight. It is then digitized and stored in a file, which should be tightly protected. In other words, the file contains a digitized image of the designated feature for each user. It is not necessary for the digital information to be precise enough to reconstruct the actual image, but it must have sufficient detail to make the stored value unique to each user and avoid duplicates. This process is called registration. Registering an individual involves more than scanning the designated feature; the authenticity of the person also has to be established.

When a user accesses a resource that is controlled with biometrics, s/he has to show the body feature to be scanned or recorded. The access control device will capture the image, digitize it, and compare it with the stored value. If there is match, the user is granted access. This process is similar to using a PIN to gain access to an ATM, where the number keyed in by the users is recorded, encrypted, and compared to the encrypted PIN on the card.
Accuracy

Because unique human features are used, biometrics is more reliable than traditional authentication methods like passwords. However, it is not foolproof. The margin of error has more to do with the mechanics in recognizing human features, rather than the probability of identical features between two people.

For most applications, letting the good guys in is just as important as keeping the bad guys out. The probability that a biometric device won't recognize a good guy is called the false rejection rate. This ranges from 0.00066% to 1.0%. A low false rejection rate is very important for most applications, since users will become extremely frustrated if they are denied access by a device that has previously recognized them.¹

The probability that a biometric device will allow a bad guy to pass is called the false acceptance rate. This figure must be sufficiently low to present a real deterrent. False acceptance rates claimed for today's biometric access systems range from 0.0001% to 0.1%. The biometric hand readers at the front entrances of 60% of the nuclear power plants in the U.S. have a false accept rate of 0.1%.¹

Common Types of Biometrics for Authentication

Fingerprint

This is arguably the easiest to implement and use. It is increasingly used for physical access to computer rooms, sports clubs, PCs, Web sites, and facilities that store valuables. Many vendors sell products that can be attached to devices, as well as portable products. For example, fingerprint mice are now affordable to even home users. Early technology could not detect whether the finger is "live." That problem has been overcome by designing sensors to test the temperature and pulse of a finger before accepting it.

Hand Geometry

This is similar to fingerprint but less precise and cannot provide uniqueness, as there are palms that are identical in shape and size. However, when used with another medium like an access card or code, this biometric can significantly enhance access control. Hand geometry can involve selected fingers or the entire palm.

Weight

Because body weight is not unique, it cannot be used as an identifier. However, it can be used to prevent unauthorized access to facilities when collaborating with other mechanisms. For example, a computer control room might use finger print authentication...
and a person-trap with a scale to detect whether the authorized person is carrying someone whose finger is not being scanned.

**Retina Scan**

This is as accurate as fingerprint and unique to individuals. It requires more expensive equipment than fingerprint scanners. An advantage is that it does not involve physical contact, which can make it more convenient; it won’t spread germs. A disadvantage is that the view of the scanner can be obstructed by passersby and moving objects.

**Facial Recognition**

This is similar to retina scan in that there is no physical contact. Although there is no uniqueness, reliability is higher than that of hand geometry. One drawback is that the person being scanned may have to take off a hat or other material that covers part of a face.

**Keystroke**

A user can be authenticated based on the way keystrokes are hit, taking into account speed and force. This does not provide uniqueness like fingerprint so it should be used in conjunction with other measures like passwords. To be authenticated, the user can be asked to key in the password along with a string of characters.

**Applications**

Biometrics can be used to control access to any systems or facilities. Its applications are increasingly present in everyday life—when entering a health club, crossing a border, and accessing government services for citizens. Here are some examples:

- The Royal Canadian Mounted Police (RCMP) and Public Works and Government Services Canada will be equipped to use fingerprint scanning at airports.
- The City of Toronto is considering using biometrics to combat welfare fraud.
- Biometrics can be used to keep track of in and out times for shift workers. This will also ensure that payroll is supported by actual hours worked (or at least hours on-site.)
- The RCMP in British Columbia has installed the Computerized Arrest and Booking System. The integrated imaging and offender management system streamlines the booking process by capturing necessary images like faces, scars, tattoos, and other distinguishing characteristics.
- BioPay, an American biometrics vendor, is piloting a system that lets consumers pay for purchases by using their fingertip; no cheque, ID card, or cash is required. Funds are securely transferred from the customer’s bank account to the merchant. The
transaction is performed like a normal cheque payment, but settlement is performed electronically and the fingerprint acts as the signature.

- The First Tennessee Bank uses hand geometry to authenticate owners of safety deposit boxes.
- Health care organizations in the United States are increasingly using biometric mice to authenticate users who access patient information.

### Inhibitors

The obvious issue is one of cost. Adding biometrics to existing security solutions or replacing them entirely will require purchasing the hardware and/or software, installing, training the end users, testing the systems, and ongoing support. But this is true of any new technology and is probably not a serious factor.

It is more likely that biometrics have not been implemented because of the privacy issues affecting the end user. The fear arises from the association of biometrics, primarily fingerprints, with criminality. Fingerprints have historically been used by law enforcement agencies to track down those suspected of committing criminal acts. For this reason, fingerprints have raised concerns over loss of dignity and privacy. Furthermore, the central retention of fingerprints and multiple access by different arms of government tends to evoke images of "big brother" surveillance.

When considering the privacy concerns associated with biometrics, an important distinction must be made between identification and authentication. A computer system can be designed to identify a person based on a biometric characteristic and used by the police to identify criminals, as well as by governments to identify qualified recipients for benefit-itlement programs and registration systems such as voting, driver's licenses, and other applications. Authentication, on the other hand, involves a "one-to-one" search whereby a live biometric presented by a person is compared to a stored sample (on a smart card, for example) previously given by that individual, and the match confirmed. The eligibility of the person for the service or benefit has been previously established. The matching of the biometric is all that is necessary to authenticate the individual as an eligible user. There is no searching or matching to a central database.

When identifiable, biometrics can act as a powerful unique identifier that can bring together disparate pieces of personal information about an individual. If used in this manner, individuals can be pinpointed and tracked. It also creates the potential for personal information from different sources to be linked together to form a detailed personal profile about that individual, unbeknownst to him or her. This represents a clear invasion of privacy, one to which most people would object. Threats to privacy can arise from the use of identifiable (raw image) biometrics that can function as a unique identifier. As with all unique identifiers, it is the secondary uses of personal information that cause the greatest concern, and the subsequent linkages that may be achieved through the use of the unique identifier.

Another issue inhibiting widespread implementation of biometrics is a fear by some of its untested-in-real-life status. They weigh convenience against security and ask: "How well do
biometrics really work? Can you be absolutely certain that a biometric device will work as claimed? Will it securely keep the bad guys out, while effortlessly letting the good guys in? In real life, security versus convenience turns out to be pretty much a non-issue, since the combination of biometric identification plus a keypad code provides virtually unbreakable security.

Biometric devices can be adjusted to favour security or user convenience. Think of a car alarm. When your car alarm is very sensitive, the probability of the bad guys stealing it is low. Yet the chance of your accidentally setting off the alarm is high. Reduce the sensitivity, and the number of false alarms goes down, but the chance of someone stealing your car increases.

The security requirements of a national defense contractor might demand that the device at the front door be adjusted to keep the bad guys out, for example. On the other hand, if hundreds of employees will clock in using a biometric reader at a low-security facility, you'll want to adjust the unit's sensitivity to let the good guys in. People like things that work. If the biometric doesn't allow employees effortless access, frustration will quickly rise and the biometric may never be accepted. Fortunately, this is extremely unlikely.

**How It Works with Other Technologies**

Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security, and Web security. Trust in these electronic transactions is essential to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys, and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives.

Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or PINs). This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), it is convenient (nothing to carry or remember), it is accurate (it provides for positive authentication), it can provide an audit trail, and it is becoming socially acceptable and inexpensive.

Also, once biometrics becomes more widespread, there will be nothing preventing the use of biometrics as a complement to current technologies rather than replacing them entirely. One clear advantage of this is to minimize the risk associated with adopting a security technology that has not as yet been tested in a large, real-life implementation.

Already commonly used is encryption to protect the transmission of biometrics between a reader and the authentication server.

**Note**

1. [www.findbiometrics.com](http://www.findbiometrics.com).