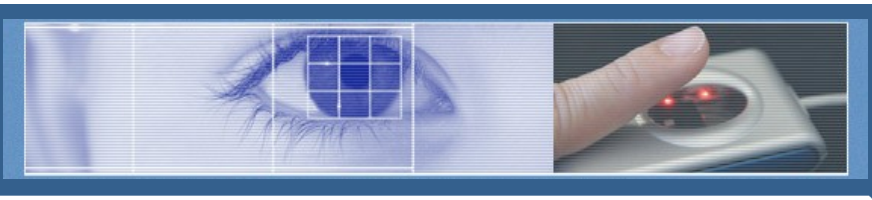
Biometrics

Contributors: Bichlien Hoang
Ashley Caudill



Originally published on the IEEE Emerging Technology portal, 2006 - 2012.
Visit: http://www.ieee.org/go/emergingtech

Biometric technology is used for automatic personal recognition based on biological traits—fingerprint, iris, face, palm print, hand geometry, vascular pattern, voice—or behavioral characteristics—gait, signature, typing pattern. Fingerprinting is the oldest of these methods and has been utilized for over a century by law enforcement officials who use these distinctive characteristics to keep track of criminals.

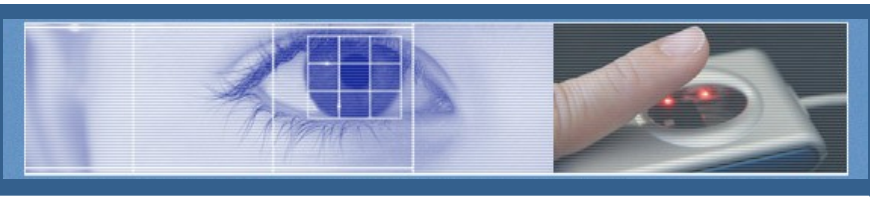
The National Science and Technology Council provides the following overview of biometric system components: "A typical biometric system is comprised of five integrated components: A sensor is used to collect the data and convert the information to a digital format. Signal processing algorithms perform quality control activities and develop the biometric template. A data storage component keeps information that new biometric templates will be compared to. A matching algorithm compares the new biometric template to one or more templates kept in data storage. Finally, a decision process (either automated or human-assisted) uses the results from the matching component to make a system-level decision." [1]

Authentication systems can be based on three measures: what you know-a password, what you have-a token or passcard, or what you are-biometrics. Passwords, keys and tokens can be forgotten, lost, stolen or otherwise compromised. Biometric identifiers also carry risks. Engineering professor, Tsutomu Matsumoto, demonstrated this point by using a digital camera, a PC, and gelatin to fashion a fake finger which fooled biometric scanners 80% of the time. [2] However, new applications can detect fakes by identifying sweat pores, measuring conduction properties, and determining the differences in how a live finger and a dummy finger deform the surface of a sensor. [3]

Biometric systems are vulnerable to two types of failures: a false-positive, in which a system falsely identifies an imposter as the valid user, and a false-negative, in which the system fails to make a match between a valid user and the stored template. Because no single identifier is fool-proof, using more than one method, such as a biometric measure in addition to a personal identification number, can enhance security.

Research and Consultancy Outsourcing Services estimates that the market for biometric products will reach $3.4 billion in 2007 with finger-scanning technology accounting for 60 percent of the market. [3] Current commercial uses include voice identification for telephone banking and fingerprint recognition for payment in hundreds of supermarkets, where customers pay for their groceries by pressing their finger to a sensor located near the cash register. Fingerprint sensors act as locks for cell phones and are used to replace text-based logins on laptops. Fingerprint technology could also be used to enhance the security of credit card purchases, both on-line and off.

Contributors: Bichlien Hoang
Ashley Caudill



Originally published on the IEEE Emerging Technology portal, 2006 - 2012.
Visit: http://www.ieee.org/go/emergingtech

Government uses of biometrics include the US-VISIT program, in which visa-issuing consular offices collect biometric data, fingerscans and photographs, which are checked against a database of known criminals and suspected terrorists. The traveler's identity is verified at entry and exit of the country. Integrated Automated Fingerprint Identification System (IAFIS), the FBI's national fingerprint and criminal history system, the Transportation Workers Identification Credentials (TWIC) program, and the Registered Traveler (RT) program are other government uses of biometrics.

The following information from the National Science and Technology Council presents four types of biometric standards: technical interfaces, data interchange formats, application profile standards, and performance testing and reporting.

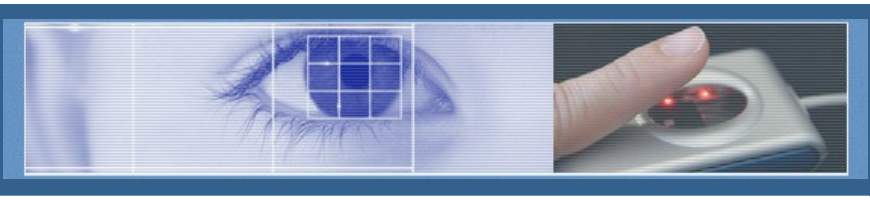
"Technical interface standards specify interfaces and interactions between biometric components and sub-systems, including the possible use of security mechanisms to protect stored data and data transferred between systems; and specify the architecture and operation of biometric systems in order to identify the standards that are needed to support multi-vendor systems and their applications.

"Data Interchange Formats specify the content, meaning, and representation of formats for the interchange of biometric data, e.g., Finger Pattern Based Interchange Format, Finger Minutiae Format for Data Interchange, Face Recognition Format for Data Interchange, Iris Interchange Format, Finger Image Based Interchange Format, Signature/Sign Image Based Interchange Format, and Hand Geometry Interchange Format; and specify notation and transfer formats that provide platform independence and separation of transfer syntax from content definition.

"Application Profile Standards specify one or more base standards and standardized profiles, and where applicable, the identification of chosen classes, conforming subsets, options, and parameters of those base standards or standardized profiles necessary to accomplish a particular function.

"Performance Testing and Reporting standards specify biometric performance metric definitions and calculations, approaches to test performance, and requirements for reporting the results of these tests." [4]

Descriptions of specific standards can be found on the websites of the InterNational Committee for Information Technology Standards (INCITS) M1, the National Institute of Standards, Joint Technical Committee 1 (JTC 1)/ Subcommittee 37 (SC 37), and the Organization for the Advancement of Structured Information Standards (OASIS).



Originally published on the IEEE Emerging Technology portal, 2006 - 2012.
Visit: http://www.ieee.org/go/emergingtech

There are several concerns surrounding the use of biometrics for identification. If a credit card or key is lost or stolen, the card can be cancelled, the locks can be changed and replaced. However, if biometric data is compromised, there are a finite number of replacements, as a person has only 10 fingers, two eyes, etc. Another concern is the possibility that sensors which require contact could be unsanitary. Ensuring the privacy and security of biometric data is also of concern, as users will be unlikely to accept the technology if information could potentially be tampered with, stolen or otherwise misused. [5]

References

[1] "Biometrics Overview." National Science and Technology Council. http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Biometrics%20Overview.pdf.
[2] "Doubt cast on fingerprint security." BBC News, May 17, 2002.
[3] Jain, Anil K. and Sharathchandra Pankanti. "A Touch of Money." IEEE Spectrum, July 2006. p. 22-27.
[4] "Biometrics Standards." National Science and Technology Council. http://www.biometricscatalog.org/NSTCSubcommittee/Documents/biometrics%20standards.pdf.
[5] Prabhakar, S.; Pankanti, S.; Jain, A.K. "Biometric recognition: security and privacy concerns." Security & Privacy Magazine, IEEE Volume 1, Issue 2, Mar-Apr 2003, p. 33-42.