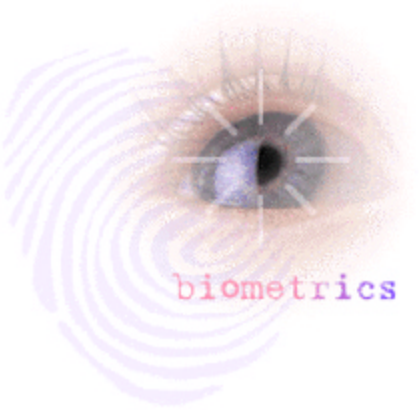


Biometric Authentication Technology: From the Movies to Your Desktop

by Fernando L. Podio[1] and Jeffrey S. Dunn[2],

A door silently opens, activated by a video camera and a face recognition system. Computer access is granted by checking a fingerprint. Access to a security vault is allowed after an iris check. Are these scenes from the latest Hollywood spy thriller? Perhaps, but soon it could be in your office or on your desktop. Biometric authentication technologies such as face, finger, hand, iris and speaker recognition are commercially available today and are already coming into wide use. Recent advances in reliability and performance and cost drops make these technologies attractive solutions for many computer and network access, protection of digital content and physical access control problems.

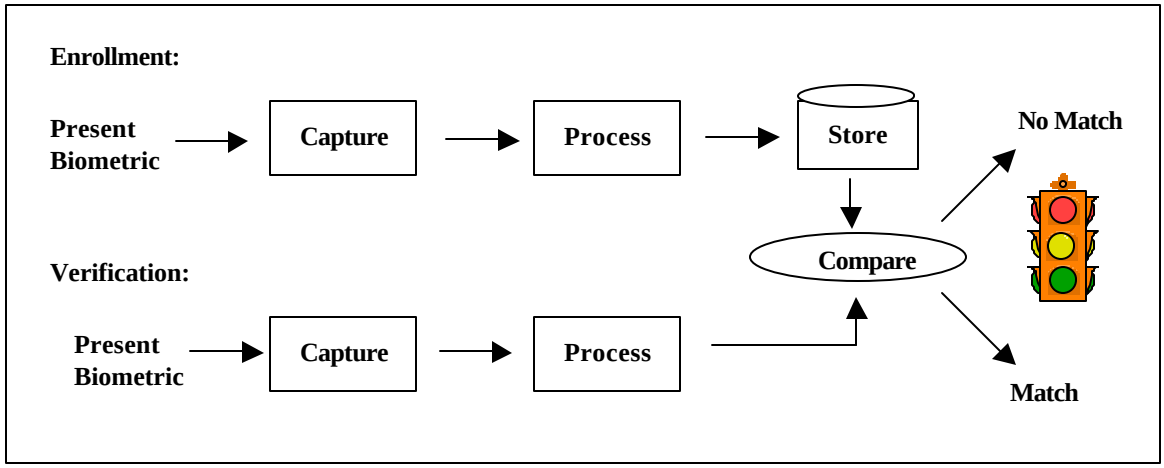
What are Biometrics?

Biometrics are automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics, and iris recognition. Behavioral characteristics are traits that are learned or acquired. Dynamic signature verification, speaker verification, and keystroke dynamics are examples of behavioral characteristics.

Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login). During **Enrollment**, as shown in the picture below, a sample of the biometric trait is captured, processed by a computer, and stored for later comparison.

Biometric recognition can be used in **Identification** mode, where the biometric system identifies a person from the entire *enrolled* population by searching a database for a match based solely on the biometric. For example, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called "one-to-many" matching. A system can also be used in **Verification** mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching. In most computer access or network access environments, verification mode would be used. A user enters an account, user name, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user.

[1] Project Manager, Biometrics Project, Convergent Information Systems Division, Information Technology Laboratory, National Institute of Standards and Technology, Co-Chair, Biometric Consortium
[2] Technical Director, Secure Network Technology Office, National Security Agency, Co-Chair, Biometric Consortium



Uses for Biometrics

Biometric-based authentication applications include workstation and network access, single sign-on, application logon, data protection, remote access to resources, transaction security, and Web security. The promises of e-commerce and e-government can be achieved through the utilization of strong personal authentication procedures. Secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Biometric technologies are expected to play a key role in personal authentication for large-scale enterprise network authentication environments, Point-of-Sale and for the protection of all types of digital content such as in Digital Rights Management and Health Care applications. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics are anticipated to pervade nearly all aspects of the economy and our daily lives. For example, biometrics is used in various schools such as in lunch programs in Pennsylvania [1], and a school library in Minnesota [2]. Examples of other current applications include verification of annual pass holders in an amusement park, speaker verification for television home shopping, Internet banking, and users' authentication in a variety of social services.

Types of Biometrics

Fingerprints: The patterns of friction ridges and valleys on an individual's fingertips are unique to that individual. For decades, law enforcement has been classifying and determining identity by matching key points of ridge endings and bifurcations. Fingerprints are unique for each finger of a person including identical twins. One of the most commercially available biometric technologies, fingerprint recognition devices for desktop and laptop access are now widely available from many different vendors at a low cost. With these devices, users no longer need to type passwords – instead, only a touch provides instant access. Fingerprint systems can also be used in identification mode. Several states check fingerprints for new applicants to social services benefits to ensure recipients do not fraudulently obtain benefits under fake names. New York State has over 900,000 people enrolled in such a system.

Face Recognition: The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission. Facial recognition in visible light typically model key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. Several approaches to modeling facial images in the visible spectrum are Principal Component Analysis, Local Feature Analysis, neural networks, elastic graph theory, and multi-resolution analysis.

Some of the challenges of facial recognition in the visual spectrum include reducing the impact of variable lighting and detecting a mask or photograph. Some facial recognition systems may require a stationary or posed user in order to capture the image, though many systems use a real-time process to detect a person's head and locate the face automatically. Major benefits of facial recognition are that it is non-intrusive, hands-free, continuous and accepted by most users.

Speaker Recognition: Speaker recognition has a history dating back some four decades, where the output of several analog filters were averaged over time for matching. Speaker recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style). This incorporation of learned patterns into the voice templates (the latter called "voiceprints") has earned speaker recognition its classification as a "behavioral biometric." Speaker recognition systems employ three styles of spoken input: text-dependent, text-prompted and text-independent. Most speaker verification applications use text-dependent input, which involves selection and enrollment of one or more voice passwords. Text-prompted input is used whenever there is concern of imposters. The various technologies used to process and store voiceprints includes hidden Markov models, pattern matching algorithms, neural networks, matrix representation and decision trees. Some systems also use "anti-speaker" techniques, such as cohort models, and world models.

Ambient noise levels can impede both collection of the initial and subsequent voice samples. Performance degradation can result from changes in behavioral attributes of the voice and from enrollment using one telephone and verification on another telephone. Voice changes due to aging also need to be addressed by recognition systems. Many companies market speaker recognition engines, often as part of large voice processing, control and switching systems. Capture of the biometric is seen as non-invasive. The technology needs little additional hardware by using existing microphones and voice-transmission technology allowing recognition over long distances via ordinary telephones (wire line or wireless).

Iris Recognition: This recognition method uses the iris of the eye which is the colored area that surrounds the pupil. Iris patterns are thought unique. The iris patterns are obtained through a video-based image acquisition system. Iris scanning devices have been used in personal authentication applications for several years. Systems based on iris recognition have substantially decreased in price and this trend is expected to continue. The technology works well in both verification and identification modes (in systems performing one-to-many searches in a database). Current systems can be used even in the presence of eyeglasses and contact lenses. The technology is not intrusive. It does not require physical contact with a scanner. Iris recognition has been demonstrated to work with individuals from different ethnic groups and nationalities.

Hand and Finger Geometry: These methods of personal authentication are well established. Hand recognition has been available for over twenty years. To achieve personal authentication, a system may measure either physical characteristics of the fingers or the hands. These include length, width, thickness and surface area of the hand. One interesting characteristic is that some systems require a small biometric sample (a few bytes). Hand geometry has gained acceptance in a range of applications. It can frequently be found in physical access control in commercial and residential applications, in time and attendance systems and in general personal authentication applications.

Signature Verification: This technology uses the dynamic analysis of a signature to authenticate a person. The technology is based on measuring speed, pressure and angle used by the person when a signature is produced. One focus for this technology has been e-business applications and other applications where signature is an accepted method of personal authentication.

Why Use Biometrics?

Using biometrics for identifying human beings offers some unique advantages. Biometrics can be used to identify you as you. Tokens, such as smart cards, magnetic stripe cards, photo ID cards, physical keys and so forth, can be lost, stolen, duplicated, or left at home. Passwords can be forgotten, shared, or observed. Moreover, today's fast-paced electronic world means people are asked to remember a multitude of passwords and personal identification numbers (PINs) for computer accounts, bank ATMs, e-mail accounts, wireless phones, web sites and so forth. Biometrics hold the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications.

There is no one “perfect” biometric that fits all needs. All biometric systems have their own advantages and disadvantages. There are, however, some common characteristics needed to make a biometric system usable. First, the biometric must be based upon a distinguishable trait. For example, for nearly a century, law enforcement has used fingerprints to identify people. There is a great deal of scientific data supporting the idea that “no two fingerprints are alike.” Technologies such as hand geometry have been used for many years and technologies such as face or iris recognition have come into widespread use. Some newer biometric methods may be just as accurate, but may require more research to establish their uniqueness.

Another key aspect is how “user-friendly” a system is. The process should be quick and easy, such as having a picture taken by a video camera, speaking into a microphone, or touching a fingerprint scanner. Low cost is important, but most implementers understand that it is not only the initial cost of the sensor or the matching software that is involved. Often, the life-cycle support cost of providing system administration and an enrollment operator can overtake the initial cost of the biometric hardware.

The advantage biometric authentication provides is the ability to require more instances of authentication in such a quick and easy manner that users are not bothered by the additional requirements. As biometric technologies mature and come into wide-scale commercial use, dealing with multiple levels of authentication or multiple instances of authentication will become less of a burden for users. An indication of the biometric

activities.

The Biometric Consortium [3] serves as a focal point for research, development, testing, evaluation, and application of biometric-based personal identification/verification systems. The Biometric Consortium now has over 800 members from government, industry and academia. Over sixty different federal agencies and members from 80 other organizations participate in the Biometric Consortium. Approximately fifty percent of the members are from industry. An electronic discussion list is maintained for Biometric Consortium members. This electronic discussion list provides an on-line environment for technical discussions among the members on all things biometric. The National Institute of Standards and Technology (NIST) [4] and the National Security Agency (NSA) [5] co-chair the Biometric Consortium (BC) and co-sponsor most of the BC activities. Recently NIST and NSA have co-sponsored and spearheaded a number of biometric-related activities including the development of a Common Biometric Exchange File Format (CBEFF) [6], NIST Biometric Interoperability, Performance, and Assurance Working Group [7], a BioAPI Users' and Developers' Seminar [8], and the NIST BioAPI Interoperability Test Bed.

CBEFF describes a set of data elements necessary to support biometric technologies in a common way independently of the application and the domain of use (e.g., mobile devices, smart cards, protection of digital data, biometric data storage). CBEFF facilitates biometric data interchange between different system components or between systems, promotes interoperability of biometric-based application programs and systems, provides forward compatibility for technology improvements, and simplifies the software and hardware integration process. CBEFF was developed by a Technical Development Team, comprised of members from industry, NIST and NSA and in coordination with industry consortiums (BioAPI Consortium [9] and TeleTrusT [10]) and a standards development group (ANSI/ASC X9F4 Working Group [11]). CBEFF is described in detail in NISTIR 6529, "Common Biometric Exchange File Format (CBEFF)", January 3, 2001 [12]. The International Biometric Industry Association (IBIA) [13] is the Registration Authority for CBEFF format owner and format type values for organizations and vendors that require them.

The NIST Biometric Interoperability, Performance and Assurance Working Group supports advancement of technically efficient and compatible biometric technology solutions on a national and international basis. It promotes and encourages exchange of information and collaborative efforts between users and private industry in all things biometric. The Working Group consists of eighty-five organizations representing biometric vendors, system developers, information assurance organizations, commercial end users, universities, government agencies, national labs and industry organizations. The Working Group is currently addressing development of a simple testing methodology for biometric systems as well as addressing issues on biometric assurance. In addition, the Working Group is addressing the utilization of biometric data in smart card applications by developing a smart card format compliant to the Common Biometric Exchange File Format (CBEFF).

NIST and NSA also provide advice to other Government agencies such as the General Services Administration (GSA) Office of Smart Cards Initiatives and DoD's Biometric Management Office. The Biometric Consortium (BC) holds annual conferences for its members and the general public. The 2000 conference was held at NIST, in Gaithersburg, MD and was attended by over 600 attendees. The next annual conference will be held Sept. 12-14, 2001 in Orlando, Florida. This conference (BC2001) will have two and a half days of seminars and technology exhibits on biometrics technologies, applications, case studies, measurement and standards. More information on BC2001 is available at http://www.nist.gov/bc2001.

The BC web site is http://www.biometrics.org. It contains a variety of information on biometric technology, research results, federal & state applications and other topics. With over 180,000 hits per month, it is one of the most used reference sources on biometrics. There is no cost to join the Biometric Consortium. Information on joining can be obtained from the web site, sending e-mail to info@biometrics.org, or calling toll-free 866-BIOMETRICS (866- 246-6387).

Summary

Recent advances in biometric technology have resulted in increased accuracy at reduced costs, biometric technologies are positioning themselves as the foundation for many highly secure identification and personal verification solutions. Today's biometric solutions provide a means to achieve fast, user-friendly authentication with a high level of accuracy and cost savings. Many areas will benefit from biometric technologies. Highly secure and trustworthy electronic commerce, for example, will be essential to the healthy growth of the global Internet economy. Many biometric technology providers are already delivering biometric authentication for a variety of web-based and client/server based applications to meet these and other needs. Continued improvements in technology will bring increased performance at a lower cost. Interest in biometrics is growing substantially. Evidence of the growing acceptance of biometrics is the availability in the marketplace of biometric-based authentication solutions that are becoming more accurate, less expensive, faster and easy to use. The Biometric Consortium, NIST and NSA are supporting this growth. While biometric authentication is not a magical solution that solves all authentication concerns, it will make it easier and cheaper for you to use a variety of automated information systems – even if you're not a secret agent.

Certain specific biometric technologies that may have been identified to adequately describe the subject matter in no way imply endorsement by the Biometric Consortium, the National Institute of Standards and Technology, or the National Security Agency, nor does it imply that the technologies identified are the only ones available in the markeplace.

References

[1] "*Fingerprint Technology Speeds School Lunch Lines*", http://www.eschoolnews.com/showstory.cfm?ArticleID=2146, eSchool News online, April 26, 2001.

[2] *"Best Practices – Technology: This Minnesota High School Gives Fingerprint Scanning a Whorl"*, http://www.eschoolnews.com/showstory.cfm?ArticleID=1277, eSchool News online, April 26, 2001.

[3] *Biometric Consortium web site*: http://www.biometrics.org

[4] *National Institute of Standards and Technology web site*: http://www.nist.gov

[5] *National Security Agency web site*: http://www.nsa.org

[6] *Common Biometric Exchange File Format (CBEFF) web site:* http://www.nist.gov/cbeff

[7] *NIST Biometric Interoperability, Performance and Assurance Working Group web site:* http://www.nist.gov/bcwg

[8] *BioAPI Users' and Developers' Seminar web site:* http://www.nist.gov/bioapi-seminar

[9] *BioAPI Consortium web site:* http://www.bioapi.org

[10] *Teletrust web site:* http://www.teletrust.de

[11] *X9. F4 Working Group, ANSI X9* web site: http://www.x9.org

[12] F. Podio, J. Dunn, L. Reinert, C. Tilton, Dr. L. O'Gorman, M. P. Collier, M. Jerde, Dr. B. Wirtz, *Common Biometric Exchange File Format (CBEFF)*, NISTIR 6529, January 3 2000.

[13] International Biometric Industry Association, http://www.ibia.org

About the Authors

Fernando Podio *has been involved in information technology development, measurements and standards development efforts for many years. He is a member of the National Institute of Standards and Technology (NIST), Information Technology Laboratory, Convergent Information Systems Division. He is currently the Project Manager for NIST's Biometrics Project. This project is conducting research into personal authentication architectures utilizing biometrics, the interoperability and performance of biometric subsystems, devices and applications, and the integration of biometrics and smart cards. Mr. Podio serves on the BioAPI Consortium Steering Committee and chairs the BioAPI Consortium's External Liaisons Working Group. He is the Biometric Consortium Co-Chair. Contact: Podio@biometrics.org*

Jeffrey Dunn *is Technical Director of the Secure Network Technology Office at the National Security Agency. This group is researching new technologies to protect access to computer systems in the Department of Defense and other critical systems. During his 20-year career at NSA, he has held a variety of program manager and management positions, concentrating the last 5 years on biometrics research. He frequently provides advice to government policy makers on biometric technologies. He is the Biometric Consortium Co-Chair. Contact: Dunn@biometrics.org*