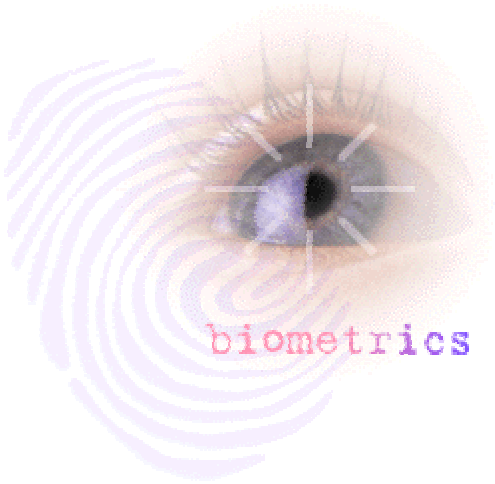
Wireless Data Networking Standards
Biometrics Technologies

Foreword: The Public Safety Wireless Network (PSWN) Program is conducting an ongoing assessment of wireless data standards. The scope of this assessment is to identify emerging and current wireless data standards, technologies, and applications for potential public safety use. This particular study concentrates on biometric technologies and applications, both wireline and wireless, and how these technologies and applications can be used in the public safety community.



Overview

Every human being possesses more than one biological characteristic that can provide nearly infallible identification. The term "biometrics" has been coined to refer to the emerging field of technology devoted to the identification of individuals using biological traits. Biometrics examples include fingerprints, iris and retinal scans, hand geometry, and other measures of physical characteristics and personal traits. Technology has advanced biometrics to a highly automated process through which identification or verification occurs almost instantaneously.

Many definitions exist for the term biometrics, and although all the definitions are similar, each adds unique facets.

According to the Biometric Consortium,[1] biometrics are "automated methods of recognizing a person based on a physiological or behavioral characteristic." A discussion paper entitled "Consumer Biometric Applications"[2] gives a more formal definition—a biometric is a "unique, measurable characteristic or trait of a human being for automatically recognizing or verifying identity." This definition uses several pertinent words that are vital to understanding biometrics.

- **Unique**—For something to be *unique*, it must be different from all others and have no equal.

- **Measurable**—For identification to be accurate and reliable, the item being measured must be easily quantifiable and dependable (i.e., hair color would not be *measurable* because it can be easily changed).

- **Characteristic or Trait**—Identity is verified through who a person is or what a person does. *Characteristics* or *traits* can be divided into physiological (i.e., fingerprints, eyes, and voice) and behavioral (i.e., signature and keystroke) patterns. The characteristic or trait should be measurable by a sensor and converted into a quantifiable, digital format.

---

1 The Biometric Consortium is located at http://www.biometrics.org. The Biometric Consortium serves as the U.S. Government's focal point for research, development, test, evaluation, and application of biometric-based personal identification and verification technology.

2 "Consumer Biometric Applications: A Discussion Paper" is located on the Ontario, Canada, Web site of the Information and Privacy Commissioner at http://www.ipc.on.ca.

- **Automatic**—In terms of biometrics, *automatic* refers to recognizing or verifying a characteristic or trait quickly and with minimal human interaction.

- **Recognition**—A person is *recognized* when he or she can be identified as being known. A biometric technology attempts to identify a person based on characteristics or traits. In other words, the system compares submitted biometric information presented by the actual person against a group of stored biometric samples. This process is frequently called a one-to-many match.

- **Verification**—*Verification* is achieved by establishing accuracy or correctness. A biometric technology accomplishes verification by comparing a stored biometric sample previously given by that individual (and identified as such at the previous time) with the actual person. This process is often called a one-to-one match.

- **Identity**—*Identity* is the condition of being the actual person and being able to link specific data (e.g., fingerprints, voice, eye patterns, etc.) to oneself.

According to the nonprofit institution RAND,[3] a biometric is "any measurable, robust, distinctive, physical characteristic or personal trait of an individual that can be used to identify or verify the claimed identity of, that individual." In addition to the defining language above, RAND's definition introduces additional language critical to understanding biometrics—

- **Robustness**—The measure of the extent to which the characteristic or trait is subject to significant changes over time. A highly *robust* biometric is not subject to significant changes over time; a low degree of robustness indicates a biometric that could change significantly over time.

- **Distinctiveness**—The measure of the variations in a biometric pattern compared with the general population. A high degree of *distinctiveness* implies a unique identifier; a low degree of distinctiveness indicates a common biometric pattern.

Biometric technologies exist that exemplify the above definitions. These technologies include fingerprint, hand and finger geometry, face, voice/speaker, iris scan, retinal scan, dynamic signature verification, and keystroke dynamics. Table 1 provides a comparison of the eight primary biometric technologies.

Mainstream Biometrics Applications

Although many possible biometrics exist, developers have deployed or pilot-tested at least eight mainstream biometric authentication applications in commercial applications in the public and private sectors. These mainstream biometric authentication technologies include: facial recognition, digital fingerprinting, hand and finger geometry, dynamic signature or handwriting verification, iris scan, retinal scan, keystroke dynamics, voice/speaker.

Facial recognition is an automated method to record the spatial geometry of distinguishing features of the face. The two main types of facial recognition systems use video and thermal imaging, respectively. Video face recognition analyzes the unique shape, pattern, and positioning of facial features by mapping those features to create

[3] RAND is located at http://www.rand.org. RAND (a contraction of the term research and development) helps improve policy and decision-making through research and analysis.

Table 1
Comparison of Biometric Technologies[4]

Biometric	Use	Level of Robustness	Level of Distinctiveness	Level of Intrusiveness
Fingerprint	Identify or Verify	Moderate	High	Touching
Hand and Finger Geometry	Verify	Moderate	Low	Touching
Face	Identify or Verify	Moderate	Moderate	12+ inches
Voice or Speaker	Verify	Moderate	Low	Remote
Iris Scan	Identify or Verify	High	High	12+ inches
Retinal Scan	Identify or Verify	High	High	1-2 inches
Dynamic Signature Verification	Verify	Low	Moderate	Touching
Keystroke Dynamics	Verify	Low	Low	Touching

a three-dimensional map. Thermal imaging produces a facial thermogram by using an infrared camera to scan a person's face and then digitizing the thermal patterns. An early application of facial recognition systems was in casino industry, where facial recognition was used to identify card counters in casinos.

Automated digital fingerprinting employs two major techniques—one that analyzes the unique marks on a person's finger (called "minutiae") and another one that examines the uniquely placed pores of the finger. Both these techniques are digital rather than the traditional fingerprinting technique of placing a person's finger into ink and then onto paper. Both of these techniques analyze the unique markings. Fingerprint technologies include large-scale Automated Finger Imaging Systems (AFIS) for law enforcement uses, fraud prevention in entitlement programs, and access control for facilities or computers.

Hand and finger geometry biometrics are automated measurements of hand and finger dimensions taken from a three-dimensional image. A reader or camera captures features of the hand such as the shape, width, length of fingers, and knuckles. This method is similar to facial recognition, in that it examines the spatial geometry of the hand and fingers. For biometrics intended to capture finger geometry only, the biometric uses the characteristics of only two or three fingers. Hand and finger geometry applications include verifying air travelers' identity, parents picking up children from school, and season ticket holders.

Dynamic signature verification and handwriting verification are automated methods of examining a person's signature, both the manner in which it is signed and the shape of the signature. This biometric analyzes the identity of a person by examining the dynamics of the signature. Signature dynamics include speed, direction, pressure of writing, the total time of the signature, and how often the pen is lifted from the paper. Banking and insurance firms use this type of biometric.

Iris scanning biometrics measure the iris pattern in the colored part of the eye. Iris scanning involves using a camera to capture a digital image of the eye. This type of biometric is especially accurate because each eye has a unique iris pattern that cannot be duplicated. In fact, even the right and left eyes of the same person have different iris patterns. Applications for iris scanning technologies include identification for automated teller machines (ATM) and

[4] http://www.rand.org

identification at a checkout counter in a grocery store.

Retinal scanning biometrics measure the blood vessel patterns in the back of the eye using a beam of light to capture these characteristics. This type of biometric is not commonly used today because some consider this type of biometric to be intrusive—retinal scans can detect such things as pregnancy. Retinal scanning biometrics are more commonly used in high-security facilities.

Keystroke dynamics is an automated biometric method that analyzes the way a person types on a keyboard. The premise behind keystroke dynamics is that each person has a distinctive rhythm or cadence for typing. Other keystroke dynamics that can be analyzed include speed, typing pressure, and the length of time that individual keys are held down. This type of biometric can be useful to verify identities on devices that have keypads such as personal computers (PC), ATMs, and telephones.

The voice/speaker biometric is an automated method of using a microphone to measure vocal characteristics to identify a person. Although background noise affects this biometric, characteristics such as cadence, tone, and pitch can be verified. Examples of voice/speaker technologies include telephone-based applications and online PC security systems. (The PC must have a built-in or external microphone.)

Evolving Biometric Applications

In addition to the eight mainstream biometric applications previously mentioned, other biometric applications are being developed. Among the evolving biometric applications currently being developed are vein patterns, ear shapes, and body odor.

Vein pattern biometrics analyze the pattern of veins on certain parts of the human body. Systems can read vein patterns from places on the body such as the back of the hand, on the wrist, or on the face. This type of identification is similar to the retinal technology, in that it uses infrared light to generate an image of a person's vein pattern.

Ear shape biometrics measures the shape (geometry) of the outer ear. This biometric measures characteristics such as earlobes and the overall bone structure of the ear.

Another evolving biometric application involves body odor. This biometric analyzes human body odors using non-intrusive sensors that capture body odor from parts of the body such as the back of the hand.

Wireless Biometrics

Biometric applications, in general, were initially designed for wired use. However, with recent advancements in wireless data technology, biometrics are becoming feasible over the wireless medium. The main wireless advancements allowing for the wireless biometric applications are increased wireless data rates and bandwidths. This increase allows users to run real-time, data intensive applications wirelessly. Removing the dependence on wires will allow for more flexible biometric applications (e.g., scanning biometric information using handheld devices).

Some wireless biometric applications do not necessarily need increased bandwidth afforded by technological advances. In fact,

some wireless biometric applications do not use the wireless medium at all. For example, biometrics can be used to authenticate a user for a specific wireless device, ensuring that only authorized personnel have access to that device. This is important for wireless devices that access sensitive or proprietary information. Many of these wireless devices give authorized users the ability to access information from behind enterprise firewalls (e.g., e-mail, personal or financial information). Use of biometrics augments sound wireless device security policies by making a wireless device useless to an unauthorized user.

Biometrics for Public Safety

Biometrics can play a significant role within the public safety community and in support of homeland security. Facial recognition biometrics are now being deployed nationwide and at high-profile venues, demonstrating the viability of biometrics for public safety use.

For example, In February 2002, security personnel used a facial recognition biometric system during Super Bowl XXXVI in New Orleans. This system scanned all incoming spectators and personnel to compare those facial scans with known terrorists. The overall heightened security and the application of groundbreaking technology such as facial recognition biometrics during that event gained substantial media attention, publicizing the power of biometrics with the general public.

In Florida, the Pinellas County Sheriff's Office is using facial recognition to assist in criminal investigations. Facial recognition biometrics are also being used to aid in jail operations in Pinellas County.

In the State of Illinois, millions of driver's license images have been scanned for duplicates and fraud, making Illinois' facial recognition system one of the largest (if not the absolute largest) facial recognition databases in the world. U.S. Marshals used the Illinois system to confirm information about 1 of their 15 Most Wanted Fugitives. Using only facial recognition, the Marshals compared a booking photograph of this wanted criminal to the Illinois Department of Motor Vehicles database. The system successfully identified the suspect's driver's license in a database containing more than 8 million images. The driver's license confirmed information that the Marshals had recently discovered using more traditional investigative techniques. This information helped lead to the suspect's arrest.

Facial recognition, as well as other biometrics, can be used to secure the Nation's borders. Security personnel can use biometric systems to scan and capture biological characteristics and traits and compare them with those of known terrorists or suspected criminals. This type of system is used at the International Airport in Fresno, California. Many other airports and ports of entry are considering deploying similar biometric systems.

The Future of Biometrics

The future of biometric technologies is promising. Use of biometric applications continues to grow worldwide, and advances in biometrics are made every day. In the past, the growth in the use of biometrics has been hindered by the costs associated with implementing biometric systems. However, due to recent developments in computer hardware and software, as well as manufacturing, prices will continue to become more reasonable.

New applications and new markets are stimulating growth in the use of biometric technologies. Some biometric technologies once used only by the military and the government are now being seen in everyday life. It is not uncommon to see use of biometric applications in child daycare centers, health facilities, and even universities. With the added advantage of wireless biometrics, it is likely that even more uses for biometrics will be discovered.

References:

http://stat.tamu.edu/Biometrics/
http://www.biometrics.org/
http://et.wcu.edu/aidc/BioWebPages/Biometrics_Home.html
http://www.waspbarcode.com/barcode_education/biometric.asp
http://www.ipc.on.ca/english/pubpres/papers/cons-bio.htm
http://www.engr.sjsu.edu/biometrics/publications_consideration.html
http://www.biocom.tv/
http://www.iwar.org.uk/comsec/resources/senate-biometrics/te111401st-lau.htm