Appendix I

Biometrics

JUNE 2005 • VERSION 1

Introduction

Humans have used body characteristics such as face, voice, gait, etc, for thousand of years to recognize each other. The term uses for that type of identification is biometric. What biological measurements qualify to be a biometric? Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- *Universality:*
  Each person should have the characteristic;
- *Distinctiveness:*
  Any two persons should be sufficiently different in terms of the characteristics;
- *Permanence:*
  The characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;
- *Collectability:*
  The characteristic can be measured quantitatively

However, in a practical biometrics system (i.e., a system that employs biometric for personal recognition), there are a number of other issues that should be considered, including:

- *Performance:*
  Refers to the recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed;
- *Acceptability:*
  Indicates the extent to which people are willing to accept the use of a particular biometrics identifier (characteristic) in their daily lives.
- *Circumvention:*
  reflects how easily the system can be fooled using fraudulent methods.

A practical biometrics system should meet the specified recognition accuracy, speed and resource requirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system.

Biometrics, strictly speaking, refers to a science involving the statistical analysis of biological characteristics. Today, the term "biometrics" usually refers to technologies that analyze human characteristics for security purposes. The statistical science of biometrics continues in the background and should be treated separately. A de facto definition of security-based biometrics has been circulating for a number of years:

A biometric is a unique, measurable characteristic or trait of a human being for automatically recognizing or verifying identity.

Biometrics System

A biometrics system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature of the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode.

A. In Verification Mode

The system validates a person's identity by comparing the captured biometric data with her own biometric template stored system database. In such a system, an individual who desires to be recognized claims an identity, usually via a PIN (Personal Identification Number), a user name, a smart card, etc., and the system conducts a one-to-one comparison to determine whether is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

B. In Identification Mode

The system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity. Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience. While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.

Throughout this article, we will use recognition where we do not wish to make a distinction between verification and identification. The block diagrams of a verification system and an identification system are depicted in Figure 1; user enrollment, which is common to both the tasks, is also graphically illustrated.

A biometric system is designed using the following 4 main modules. (See Figure 1):

- *Sensor module:* A module that captures the biometric data of an individual;
- *Feature extraction module:* A module in which the acquired biometric data is processed to extract a set of salient or discriminatory features;
- *Matcher module:* A module in which the features during recognition are compared against the stored templates to generate matching scores. The matcher module also encapsulates a decision-making module, in which a user's claimed identity is confirmed (verification) or a user's identity is established (identification) based on the matching score.

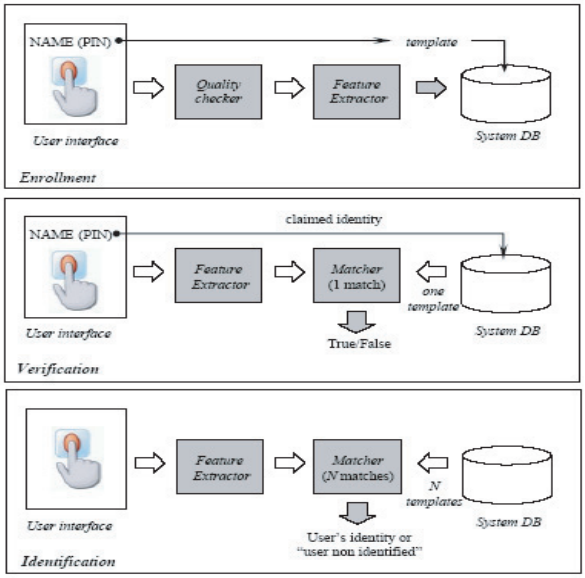


Figure 1. Block diagrams of enrollment, verification and identification tasks are shown using the four main modules of a biometric system, i.e., sensor, feature extraction, matcher, and system database.

- *System database module:* A module which is used by the biometric system to store the biometric templates of the enrolled users. The enrollment module is responsible for enrolling individuals into the biometric system database. During the enrollment phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a digital representation (feature values) of the characteristic. The data capture during the enrollment process may or may not be supervised by a human depending on the application. A quality check is generally performed to ensure that the acquired sample can be reliably processed by successive stages. In order to facilitate matching, the input digital representation is further processed by a feature extractor to generate a compact but expressive representation, call a template. Depending on the application, the template may be stored in the central database of the biometric system or be recorded on a smart card issued to the individual. Usually, multiple templates of an individual are stored to account for variations observed in the biometric trait and the templates in the database may be updated over time.

Biometric technologies, therefore, are concerned with the physical parts of the human body or the personal traits of human beings. The term "automatic" essentially means that a biometric technology must recognize or verify a human characteristic quickly and automatically, in real time. The most common physical biometrics is the eye (iris and retina), face, finger image, hand and voice. Behavioral biometrics includes typing rhythm (keystroke dynamics) and signature.

Comparison of Various Biometrics

A number of biometric characteristics exist and are in use in various applications. Each biometric has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet the requirements of all the applications. In other words, no biometric is 'optimal'. The match between a specific biometric and an application is determined depending upon the operational mode of the application and the properties of the biometric characteristic. A brief introduction of the commonly used biometrics is given below:

1. **Fingerprint**

Fingerprint

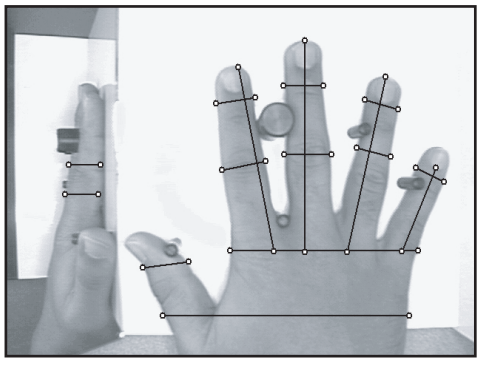
In recent years, fingerprints have rallied significant support as the biometrics technology that will probably be most widely used in the future. In addition to general security and access control applications, fingerprint verifiers are installed at military facilities, including the Pentagon and government labs. Today, the largest application of fingerprint technology is in automated fingerprint identification systems (AFIS) used by police forces throughout the U.S. and in over 30 foreign countries.

The fingerprint's strength is its acceptance, convenience and reliability. It takes little time and effort for somebody using a fingerprint identification device to have his or her fingerprint scanned. Studies have also found that using fingerprints, as an identification source is the least intrusive of all biometrics techniques.

Verification of fingerprints is also fast and reliable. Users experience fewer errors in matching when they use fingerprints versus many other biometrics methods. In addition, a fingerprint identification device can require very little space on a desktop or in a machine. Several companies have produced capture units smaller than a deck of cards.

2. **Hand geometry**

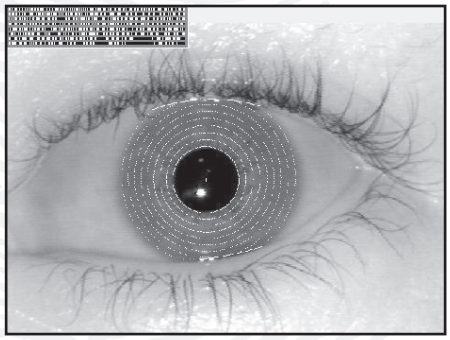
Currently, hand geometry is employed at over 8,000 locations, including the Colombian legislature, San Francisco International Airport, day care centers, welfare agencies, hospitals and immigration facilities. The advantages of a palm print are similar to the benefits of a fingerprint in terms of reliability, although palm print readers take up more space. The most successful device, the Handkey, looks at both the top and side views of the hand using a built-in video camera and compression algorithms.



Hand geometry

3. **Iris**

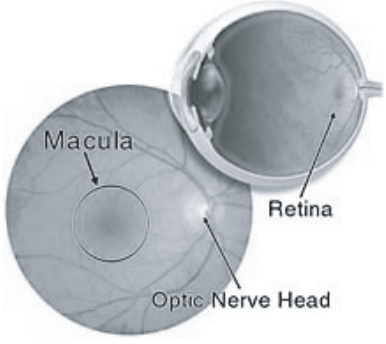
The advantage of iris scanners is that they do not require the user to focus on a target, because the patterns of flecks on the iris are on the eye's surface. In fact, a video image of the eye can be taken from up to three feet away, which allows for the use of iris scanners at ATM machines. In visually impaired persons with intact irises, the iris can still be captured and encoded with iris imaging products that have active iris capture (e.g., the ATM application). Since cataracts are a malady of the lens, which is behind the iris, cataracts do not affect iris scanning in any way.



Iris

4. **Retinal**

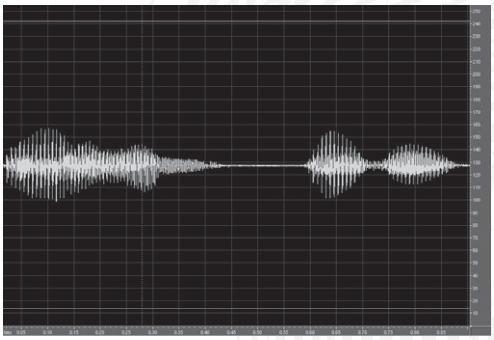
Retinal scans are performed by directing a low-intensity infrared light through the pupil to the blood vessel pattern on the back of the eye. Most uses of retinal scanners involve high-security access control, since they offer one of the lowest false reject rates and a nearly 0% false acceptance rate. However, since retinal imaging requires a clear view of the back of the eye, cataracts can negatively impact the retinal image quality.



Retina

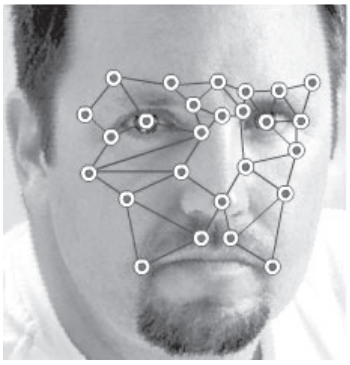
Comparison of Various Biometrics

5. **Voice**
The appeal of voice verification is its acceptability to users. A common concern about this biometrics approach is impersonations. However, this is not a serious problem, since the devices focus on different characteristics of speech than people do. Speech patterns are formed by a combination of physiological and behavioral factors. Currently, voice verification is being used to control access to medium-security offices, labs, and computer facilities. Several providers of home confinement systems use voice verification to confirm that early parolees are at home. While voice recognition is convenient, it is not as reliable as other biometrics techniques. A person with a cold or laryngitis, for example, may have problems using a voice recognition system.



Voice wave

6. **Face**
Facial verification and recognition is one of the fastest growing sectors of the biometrics industry. Its appeal lies in the fact that it most closely resembles the way we as humans identify one another. Most commercial efforts have been stimulated by the fast rise in multimedia video technology that is placing more cameras in the home and workplace. However, most developers have had difficulty achieving high levels of performance. Nevertheless, specific applications, such as screening welfare databases for duplicates and airport lounges for terrorists, are likely to appear in the future.



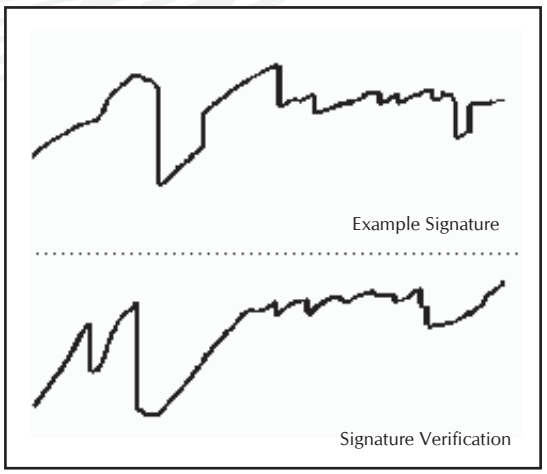
Facial verification

7. **Signatures**
Static signature capture is becoming quite popular as a replacement for pen and paper signing in bank-card, PC and delivery service applications (e.g., Federal Express).

Generally, verification devices use wired pens, pressure-sensitive tablets, or a combination of both.

Devices using wired pens are less expensive and take up less room but are potentially less durable. To date, the financial community has been slow to adopt automated signature verification methods for credit cards and check applications because signatures are still too easily forged. This keeps signature verification from being integrated into high-level security applications.

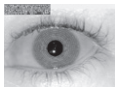
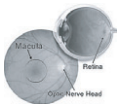
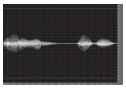
Signature pad & pen



Signature verification

Comparison of Various Biometrics

Note that some of the following ratings are based on current versions (status: March 2004), which could change drastically with new solutions.

Biometric Trait	Comfort	Accuracy	Availability	Costs
Fingerprint 	Good	Good	Good	Low
Signature (dynamic) 	Fair	Fair	Fair	High
Facial Geometry 	Best	Fair	Good	High
Iris 	Fair	Best	Fair	High
Retina 	Fair	Good	Fair	High
Hand Geometry 	Good	Fair	Fair	Fair
Voice 	Fair	Fair	Fair	Fair

Biometric Comparative Market

The applicability of a specific biometric technique depends heavily on the requirements of the application domain. No single technique is admissible and there is no optimal biometric characteristic. It is well known that both the fingerprint-based and iris-based techniques are more accurate than the voice based technique.

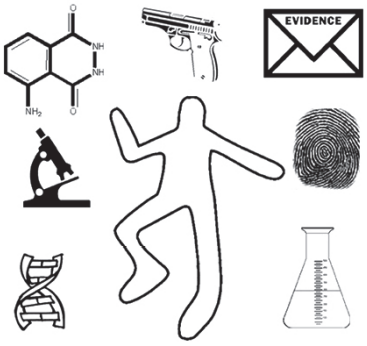
Application of Biometric Systems

The applications of biometrics can be divided into the following 3 main groups:

1. Commercial applications: Computer network login, Internet access, ATM, credit card, physical access control, e-commerce, electronic data security, etc

2. Government application: National ID card, driver's license, social security, border control, passport control, welfare-disbursement, etc.

3. Forensic applications: Corpse identification, criminal investigation, terrorist identification, parenthood determination, missing children, etc.



Traditionally, commercial applications have used knowledge-based systems (eg. PINs and password), government applications have used token-used system (eg. ID cards and badges), and forensic applications have relied on human experts to match biometric features. Thus, biometric systems can be used to enhance user convenience while improving security.

Biometrics System in Commercial Applications

The traditional technologies available to achieve a positive recognition include knowledge-based methods (eg. PINs passwords) and token-based methods (eg. Keys and cards). There are many problems with possession-based personal recognition. For example, password, keys and tokens can be shared, duplicated, lost or stolen. It is significantly more difficult to copy, share and distribute biometrics with as much ease as passwords and tokens.

Biometrics cannot be lost or forgotten and biometrics-based recognition systems require the person to be recognized to be present at the point of recognition. It is difficult to forge biometrics and extremely unlikely for a user to repudiate. Further, all the users of the system have relatively equal security level and one account is not easier to break than any other.

Biometrics introduces incredible convenience for the users, as users are no longer required to remember multiple, long and complex, frequently changing passwords, while maintaining a sufficiently high degree of security. Biometrics provides tools to enforce liable logs of system transactions and to protect an individual's right to privacy.

Finally, in commercial applications, addition or replacement of existing personal recognition methods with biometrics-based solutions should be based on cost benefit analysis.

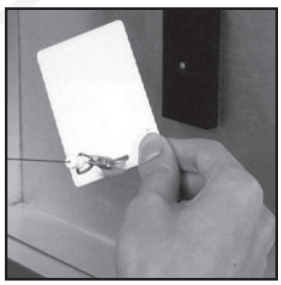
Past Industry Growth

The access control/time and attendance market is an established market for biometrics-based identification solutions. Access control/time and attendance are combined because both applications frequently form a part of the same system. Systems are purchased partly for the sake of worker safety, partly to deter theft, and partly to streamline various aspects of human resource management, such as key issuance and time and attendance procedures. The access control market is defined as the market for biometrics products to control entry into a facility. Time and attendance systems are comprised of both hardware and software products that automatically record the time an employee reports to work and the time the employee leaves the facility.

Physical access control is a traditional application for biometrics. While cards and keypads dominate electronic access control worldwide, biometrics systems have made significant inroads into the market. Falling prices and steadily improving performance are making biometrics a viable option for businesses that would otherwise stay with cards or keypads.

Buddy punching

Manual calculation



Card Access

The rapidly growing time and attendance market is providing excellent opportunities for biometrics. Improved methods for monitoring employee work hours and processing salary payments are in demand. Each year, companies lose substantial sums due to employee misreporting of hours worked. Card-based time and attendance systems, although representing an improvement, have not adequately solved the problem because cards and PINs can be provided to others and used fraudulently.

The problem of "buddy punching" (clocking in for an absent co-worker) costs companies hundreds of millions of dollars every year. Businesses with large

Past Industry Growth

hourly paid work forces are increasingly interested in biometrics-based identification systems as a way of combating this fraud. Currently, biometrics is used in less than 5 percent of time and attendance systems but is anticipated to be used in 25 percent or more within 5 years.

Particularly within the business community, electronic access control systems have been growing in importance over the past ten to fifteen years. Previously, access control systems were rather unsophisticated technology found only in high-end environments such as large corporate office buildings and high-security government installations. Keypads and cards were the most common forms of electronic access control. Most of the business community viewed electronic access control as either too expensive or simply unnecessary.

Increasingly, however, electronic access control is considered to be a necessary part of building architecture. The theft of costly company assets is a continuing probe. Furthermore, in an increasingly competitive economic environment, corporate espionage is a constant concern; conventional lock and key methods seem inadequate safeguards against these problems.

(Source : Frost and Sullivan)

Social Acceptance and Privacy Issues

Human factors dictate the success of a biometric-based identification system to a large extent. The ease and comfort in interaction with a biometric system contribute to its acceptance. For example, is a biometric system is able to measure the characteristic of an individual without touching, such as those using face, voice or iris, it may be perceived to be more user-friendly and hygienic.

Additionally, biometric technologies requiring very little cooperation or participation from the users may be perceived as being more convenient to users. On the other hand, biometric characteristics that do not require user participation can be captured without the knowledge of the user, and many individuals perceive this as a threat to privacy.

In fact, biometrics ensures privacy by safeguarding identity and integrity. It can also be used to limit access to personal information. Nevertheless, many people are uneasy about the use of their personal biological characteristics in corporate or government recognition systems.

To alleviate these fears, companies and agencies that operate biometric systems have to assure the users of these systems that their biometric information remains private and is used only for the expressed purpose for which it was collected. Legislation is necessary to ensure that such information remains private and that is misuse is appropriately punished.

Most of the commercial biometric systems available today do not store the sensed physical characteristics in their original form but, instead, they stored a digital representation (a template) in an encrypted format. This serves two purposes. First, the actual physical characteristic cannot be recovered from the digital template thus ensuring privacy and secondly, the encryption ensures that only the designated application can use this template.