Chapter Two

A PRIMER ON BIOMETRIC TECHNOLOGY

Here we provide a primer on biometric technology.[1] In particular, this chapter introduces the technical terminology and the major concepts related to biometric applications. We first define the terms, "biometrics" and "biometric authentication." Next, we discuss three universal components present in the operation of all biometric technologies, including the difference between applications that identify, or verify the claimed identity of, an individual. We then discuss some mainstream biometrics and their applications. We conclude with a table comparing salient characteristics of mainstream biometric technologies.

A DEFINITION OF BIOMETRICS AND BIOMETRIC AUTHENTICATION

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.

Measurable means that the characteristic or trait can be easily presented to a sensor and converted into a quantifiable, digital format.

[1]For those interested in a more detailed discussion about biometric technology, see Appendix A. This chapter does not cover standards for interoperability because this subject is tangential to RAND's project. In researching and writing this chapter, the authors relied heavily on the following sources: Hawkes and Hefferman (1999); Wayman (1999c); and Wayman (2000) (an updated version of "Testing and Evaluating Biometric Technologies: What the Customer Needs To Know" originally published in *Proceedings of the CardTech/SecurTech Conference '98*, May 1998). See also Dunn (1998).

This allows for the automated matching process to occur in a matter of seconds.

The *robustness* of a biometric is a measure of the extent to which the physical characteristic or personal trait is subject to significant changes over time. Such changes may occur because of the effects of an individual's exposure to chemicals, aging, or injury. A highly robust biometric is not subject to large changes over time, while a low degree of robustness indicates a biometric that could change considerably over time. For example, iris patterns, which change very little over a lifetime, are more robust than voices.

Distinctiveness is a measure of the variations or differences in the biometric pattern among the general population. The highest degree of distinctiveness implies a unique identifier, while a low degree of distinctiveness indicates a biometric pattern found frequently among the general population. The purpose of the biometric application determines the degree of robustness and distinctiveness required.

Identification differs significantly from *verification*. Identification is when the device asks and attempts to answer the question, "Who is X?" When biometrics are used to identify an individual, the biometric device reads a sample and compares that sample against every template in the database. This is called a "one-to-many" search (1:N). The device will either find a match and subsequently identify the person or not find a match and fail to identify the person.

Verification is when the device asks and attempts to answer the question, "Is this X?" after the user claims to be X. When biometrics are used to verify the claimed identity of an individual, the biometric device first requires input from the user. For example, the user claims his identity by using a password, token, or user name (or any combination of the three). The device also requires a biometric sample. It then compares the sample against the user-defined template (pointed to by the password, token, and/or user name) in the database. This is called a "one-to-one" search (1:1). The device will either find or not find a match between the two.

In general, there are three different approaches to recognizing an individual for security purposes, known as authentication. Presented in order of least secure and convenient to most secure and

convenient, the first approach uses something you have, such as a token, card, or key. The second approach uses something you know, such as a password or PIN. The third uses something you are, a biometric. Any combination of these three further heightens security, while requiring all three provides the highest level of security.[2]

Biometric authentication refers to *automated methods of identifying or verifying* the identity of a *living person in real time* based on a *physical characteristic or personal trait*. The phrase, "living person in real time" is used to distinguish biometric authentication from forensics, which does not involve real-time identification of a living individual.

Biometric authentication technologies are used in two ways:

- To prove who you are or who you claim you are.
- To prove who you are not (for example, to resolve a case of mistaken identity).

KEY ELEMENTS OF ALL BIOMETRIC SYSTEMS

All biometric systems consist of three basic elements:

- enrollment,
- templates, and
- matching.

Enrollment is the process of collecting biometric samples from a person and the subsequent generation of a template. Typically, the device takes three samples of the same biometric and then averages them to produce an enrollment template. Templates are the data representing the enrollee's biometric. They are created by the biometric device, which uses a proprietary algorithm to extract "features" appropriate to that technology from the enrollee's sam-

[2]Security also depends on such factors as the care taken to apply security measures properly, insofar as safeguarding tokens and passwords and ensuring that transmissions of biometric data are adequately protected.

ples.[3] These features are also referred to as minutiae points for some technologies, such as fingerprint systems. Because templates are only a record of distinguishing features of a person's biometric characteristic or trait (and not an image or complete record of the actual fingerprint or voice), the template is usually small and allows for the near-instantaneous processing time characteristic of biometric authentication. The small size of some templates allows for storage on magnetic stripes or bar codes placed on plastic cards or smart cards.[4] An example of the formation of a template for a fingerprint is shown in Figure 2.1.

For any biometric technology, a small percentage of the population will be unable to produce a usable template. This failure to enroll (or acquire) is the failure of the technology to extract adequate distinguishing features appropriate to that technology. For example, a small fraction of the population cannot be fingerprinted either because their prints are not distinctive enough (e.g., no bifurcations that can be picked up by the system) or because of the individual's occupation or age, which can alter distinguishing features.

Matching is the process of comparing a submitted biometric sample against one (verification) or many (identification) templates in the system's database.

In general, verification applications provide more security than identification applications because a biometric and at least one other piece of input (e.g., PIN, password, token, user name) are required to match a template. Verification provides a user with control over his own data and over the biometric authentication process, provided

[3]Image files of fingerprints also may be of interest to the Army because of their law enforcement, forensic, and technical applications. In the case of fingerprints, the Army may want to keep both electronic image files of the fingerprints as well as the biometric templates. While the image files are too large to be used for biometric applications, they would be useful for criminal investigation and other forensic purposes. Moreover, the Army might want to store image files to provide greater technical flexibility. For example, if the Army did not keep image files of enrollees, it might have to physically reenroll each individual if the Army decided to change to a different proprietary biometric system. Any image file is also referred to as raw data or the *corpus*.

[4]Appendix A includes a detailed discussion about template storage.

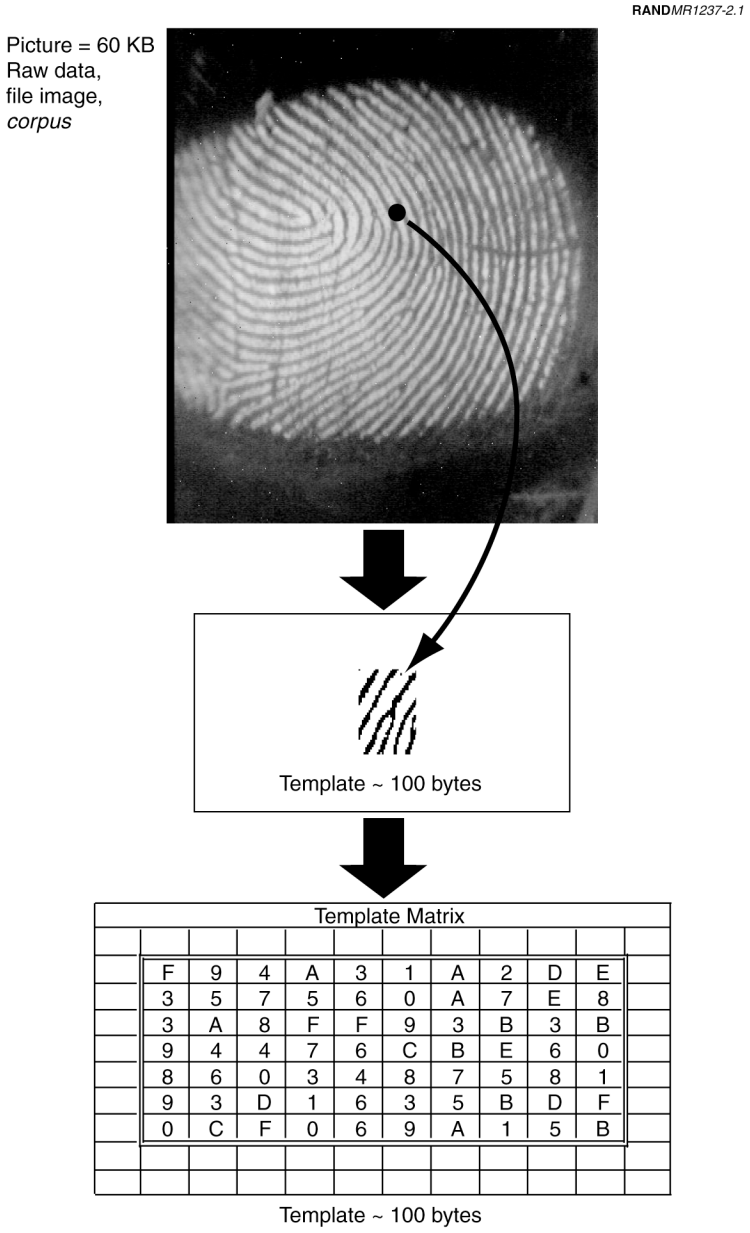

Figure 2.1—Example of the Formation of a Template for a Fingerprint

that the template is stored only on a card. That is, such a system would not allow for clandestine, or involuntary, capture of biometric data because the individual would know if he were providing the card. Because the search seeks only a match against one template in the database, verification applications require less processing time, less memory, and less cost than identification applications.

Accuracy and error rates must be examined by the end-user when choosing biometric devices. When discussing errors, we prefer to use the terms, false match rate (FMR), and false nonmatch rate (FNMR). A false match occurs when a sample is incorrectly matched to a template in the database. A false nonmatch occurs when a sample is incorrectly not matched to a truly matching template in the database (i.e., a legitimate match is denied). These two terms are often misnamed "false acceptance rate" and "false rejection rate," respectively, but these terms are application-dependent in meaning. FMR and FNMR are application-neutral terms to describe the matching process between a live sample and a biometric template.

Identification applications require a highly robust and distinctive biometric, otherwise the error rates falsely matching and nonmatching users' samples against templates breaches security and inhibits convenience. Applications where the end-user wants to identify criminals (immigration, law enforcement, etc.) or other types of "wolves in sheep's clothing" must use an identification application. Other types of applications may require a verification application. In many ways, deciding whether to use verification or identification requires a balance between the end-user's needs for security and convenience.

Template management is an integral component of balancing privacy, security, and convenience issues. All biometric systems face a common issue: The template database must be stored somewhere. Biometric templates must be protected to prevent identity fraud and maintain user privacy. Possible solutions include storage on the biometric device itself, a central computer that is remotely accessed, a plastic card or token with a bar code or magnetic stripe, Radio Frequency Identification Device (RFID) cards and tags, optical memory cards, PCMCIA (Personal Computer Memory Card International Association) cards, and smart cards.

Smart cards are the size of credit cards and have a microchip or microprocessor chip embedded in them. The chip can store a variety of electronic data, including a biometric template that can be protected using biometric authentication. Smart cards come in two types: contact and contactless smart cards. A contact smart card must be inserted into a smart card reader to be used. A contactless smart card need only be placed near an antenna to carry out a transaction.

An important security issue with regard to template database management is whether the database will serve a unique purpose or if it will be used for multiple purposes. For example, a facilities manager might use a fingerprint reader to control building access. He might also want to use the same fingerprint template database to identify employees logging onto their computer network. The manager should consider several important questions, such as should separate databases be used for these different purposes and is it an acceptable risk to access employee fingerprints from a remote location for multiple purposes? The transmission of data across wires to a central database presents risks that the biometric template might be captured or stolen.

An additional privacy and security concern is what additional personal information will be stored about each user with his biometric template and whether his biometric is used to link to other personal information about him.

MAINSTREAM BIOMETRICS AND THEIR APPLICATIONS

Of the many possible biometrics, at least eight mainstream biometric authentication technologies have been deployed or pilot-tested in applications in the public and private sectors. These are fingerprint, hand/finger geometry, facial recognition, voice recognition, iris scan, retinal scan, dynamic signature verification, and keystroke dynamics.[5] Each is discussed briefly below.

---

[5]For a comprehensive examination of mainstream biometrics, see Jain, Bolle, and Pankanti (1998).

Fingerprint

The fingerprint biometric is an automated digital version of the old ink-and-paper method used for more than a century for identification, primarily by law enforcement agencies. The biometric device involves a user placing his finger on a platen for the fingerprint to be read. The minutiae are then extracted by the vendor's particular algorithm to create a template. Fingerprint biometrics have three main application arenas: large-scale Automated Finger Imaging Systems (AFIS) for law enforcement uses, fraud prevention in entitlement programs, and access control for facilities or computers.

Hand/Finger Geometry

Hand or finger geometry is an automated measurement of many dimensions of the hand and fingers. Neither of these methods take prints of the palm or fingers. Rather, only the spatial geometry is examined as the user lays his hand on the sensor's surface and uses guiding poles between the fingers to place the hand properly and initiate the reading. Finger geometry typically uses two or three fingers. During the 1996 Summer Olympics, hand geometry secured access to the athletes' dorms at Georgia Tech. Hand geometry is a well-developed technology that has been thoroughly field-tested and is easily accepted by users.

Facial Recognition

Facial recognition is an automated method to record the spatial geometry of distinguishing features of the face. Different methods of facial recognition among various vendors all focus on measures of key features. Noncooperative behavior by the user and environmental factors, such as lighting conditions, can degrade performance for facial recognition technologies. Facial recognition has been used in projects designed to identify card counters in casinos, shoplifters in stores, criminals in targeted urban areas, and terrorists overseas.

Voice Recognition

Voice recognition is an automated method of using vocal characteristics to identify individuals using a pass-phrase. The technology

itself is not well-developed, partly because background noise affects its performance. Additionally, it is unclear whether the technologies actually recognize the voice or just the pronunciation of the passphrase (password) used to identify the user. The telecommunications industry and the National Security Agency (NSA) continue to work to improve voice recognition reliability. A telephone or microphone can serve as a sensor, which makes this a relatively cheap and easily deployable technology.

Iris Scan

Iris scanning measures the iris pattern in the colored part of the eye (although the color has nothing to do with the scan). Iris patterns are formed randomly. This means no two iris patterns are the same; the iris pattern of one's left eye is different from the iris pattern of the right eye. Iris scans can be used for both identification and verification applications. ATMs ("Eye-TMs"), grocery stores (for checking-out), and the Charlotte/Douglas International Airport (physical access) use iris scanning in test applications. During the 1998 Winter Olympic Games in Nagano, Japan, an iris scanning identification system controlled access to the rifles used in the biathlon.

Retinal Scan

Retinal scans measure the blood vessel patterns in the back of the eye. The device involves a light source shined into the eye of a user who must stand very still within inches of the device. Because the retina can change with certain medical conditions, such as pregnancy, high blood pressure, and AIDS, this biometric has the potential to reveal more about individuals than only their identity. Because users perceive the technology to be intrusive, retinal scanning has lost popularity with end-users.

Dynamic Signature Verification

Dynamic signature verification is an automated method of examining an individual's signature. It uses a stylus and surface on which a person writes. This technology examines dynamics, such as speed, direction, and pressure of writing; time that the stylus is in and out of

contact with the "paper"; total time of the signature; and where the stylus is raised and lowered onto the "paper."

Keystroke Dynamics

Keystroke dynamics is an automated method of examining an individual's keystrokes on a keyboard. The technology uses a keyboard compatible with PCs. This technology examines such dynamics as speed and pressure, total time of typing a particular password, and the time a user takes between hitting certain keys. Keystroke dynamics has the potential for continuous authentication of identity while a person is using a computer.

SALIENT CHARACTERISTICS OF MAINSTREAM BIOMETRICS

Table 2.1 compares the eight mainstream biometrics in terms of several characteristics, ranging from how robust and distinctive they are to what they can be used for (i.e., identification or verification or verification alone).[6]

When we compare how mainstream biometrics can be used, we find that about half can be used reliably for either identification or verification purposes. The other half are best only for verification purposes. In particular, hand geometry has only been used for verification applications, such as physical access control and time and attendance. Biometrics that can only be used for verification purposes present fewer privacy concerns because they are not trackable.

The robustness and distinctiveness of biometrics vary considerably. Fingerprinting is moderately robust, and, although it is distinctive, a small percentage of the general population at any given time has unusable prints. While hand/finger geometry is moderate on the

[6]This table is an effort to assist the reader in categorizing biometrics along important dimensions. Because this industry is still establishing standards and the technology is changing rapidly, it is difficult to make unequivocal assessments. The table represents our assessment based on discussions with technologists, vendors, and program managers. This table is compiled from various sources, including Jain, Bolle, and Pankanti (1998) and various presentations made at the SJB Biometrics 99 Workshop, November 9-11, 1999, particularly Hawkes and Hefferman (1999).

robustness scale, it is not very distinctive. Facial recognition is neither highly robust nor distinctive. As for voice recognition, assuming the voice and not the pronunciation is what is being measured, this biometric is moderately robust and distinctive. Iris scans are both highly robust, because they are not susceptible to day-to-day changes or damages, and distinctive, because they are randomly formed. Retinal scans are also fairly robust and very distinctive. Finally, neither dynamic signature verification nor keystroke dynamics are particularly robust or distinctive.

As the table shows, the biometrics vary in terms of how intrusive they are, ranging from those biometrics that require touching to others that can recognize an individual from a distance.

Table 2.1

Comparison of Mainstream Biometrics

Biometric	Identify versus Verify	How Robust	How Distinctive	How Intrusive
Fingerprint	Either	Moderate	High	Touching
Hand/Finger Geometry	Verify	Moderate	Low	Touching
Facial Recognition	Either	Moderate	Moderate	12+ inches
Voice Recognition	Verify	Moderate	Low	Remote
Iris Scan	Either	High	High	12+ inches
Retinal Scan	Either	High	High	1–2 inches
Dynamic Signature Verification	Verify	Low	Moderate	Touching
Keystroke Dynamics	Verify	Low	Low	Touching