An Introduction to Biometric Authentication Systems

1

James Wayman, Anil Jain, Davide Maltoni and Dario Maio

1.1 Introduction

Immigration cards holding both passport number and measures of the user's hand [1]; fingerprints taken as a legal requirement for a driver license, but not stored anywhere on the license [2]; automatic facial recognition systems searching for known card cheats in a casino [3]; season tickets to an amusement park linked to the shape of the purchaser's fingers [4]; home incarceration programs supervised by automatic voice recognition systems [5]; and confidential delivery of health care through iris recognition [6]: these systems seem completely different in terms of purpose, procedures, and technologies, but each uses "biometric authentication" in some way. In this book, we will be exploring many of the technologies and applications that make up the field of "biometric authentication" – what unites them and what differentiates them from each other. In this chapter, we want to present a systematic approach to understanding in a unified way the multitude of technologies and applications of the field.

We start with a narrow definition, designed as much to limit the scope of our inquiry as to determine it.

> "Biometric technologies" are automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic [7, 8].

There are two key words in this definition: "automated" and "person". The word "automated" differentiates biometrics from the larger field of human identification science. Biometric authentication techniques are done completely by machine, generally (but not always) a digital computer. Forensic laboratory techniques, such as latent fingerprint, DNA, hair and fiber analysis, are not considered part of this field. Although automated identification techniques can be used on animals, fruits and vegetables [9], manufactured goods and the deceased, the subjects of biometric authentication are living humans. For this reason, the field should perhaps be more accurately called "anthropometric authentication".

The second key word is "person". Statistical techniques, particularly using fingerprint patterns, have been used to differentiate or connect

groups of people [10, 11] or to probabilistically link persons to groups, but biometrics is interested only in recognizing people as individuals. All of the measures used contain both physiological and behavioral components, both of which can vary widely or be quite similar across a population of individuals. No technology is purely one or the other, although some measures seem to be more behaviorally influenced and some more physiologically influenced. The behavioral component of all biometric measures introduces a "human factors" or "psychological" aspect to biometric authentication as well.

In practice, we often abbreviate the term "biometric authentication" as "biometrics", although the latter term has been historically used to mean the branch of biology that deals with its data statistically and by quantitative analysis [12].

So "biometrics", in this context, is the use of computers to recognize people, despite all of the across-individual similarities and within-individual variations. Determining "true" identity is beyond the scope of any biometric technology. Rather, biometric technology can only link a person to a biometric pattern and any identity data (common name) and personal attributes (age, gender, profession, residence, nationality) presented at the time of enrollment in the system. Biometric systems inherently require no identity data, thus allowing anonymous recognition [4].

Ultimately, the performance of a biometric authentication system, and its suitability for any particular task, will depend upon the interaction of individuals with the automated mechanism. It is this interaction of technology with human physiology and psychology that makes "biometrics" such a fascinating subject.

1.2 A Quick Historical Overview

The scientific literature on quantitative measurement of humans for the purpose of identification dates back to the 1870s and the measurement system of Alphonse Bertillon [13–17]. Bertillon's system of body measurements, including such measures as skull diameter and arm and foot length, was used in the USA to identify prisoners until the 1920s. Henry Faulds, William Herschel and Sir Francis Galton proposed quantitative identification through fingerprint and facial measurements in the 1880s [18–20]. The development of digital signal processing techniques in the 1960s led immediately to work in automating human identification. Speaker [21–26] and fingerprint recognition [27] systems were among the first to be explored. The potential for application of this technology to high-security access control, personal locks and financial transactions was recognized in the early 1960s [28]. The 1970s saw development and deployment of hand geometry systems [29], the start of large-scale testing [30] and increasing interest in government use of these "automated personal identification" technologies [31]. Retinal [32, 33] and signature verification [34, 35] systems came in the 1980s, followed by face [36–42] systems. Iris recognition [43, 44] systems were developed in the 1990s.

1.3 The "Best" Biometric Characteristic

Examples of physiological and behavioral characteristics currently used for automatic identification include fingerprints, voice, iris, retina, hand, face, handwriting, keystroke, and finger shape. But this is only a partial list as new measures (such as gait, ear shape, head resonance, optical skin reflectance and body odor) are being developed all of the time. Because of the broad range of characteristics used, the imaging requirements for the technology vary greatly. Systems might measure a single one-dimensional signal (voice); several simultaneous one-dimensional signals (handwriting); a single two-dimensional image (fingerprint); multiple two-dimensional measures (hand geometry); a time series of two-dimensional images (face and iris); or a three-dimensional image (some facial recognition systems).

Which biometric characteristic is best? The ideal biometric characteristic has five qualities: robustness, distinctiveness, availability, accessibility and acceptability [45, 46]. By "robust", we mean unchanging on an individual over time. By "distinctive", we mean showing great variation over the population. By "available", we mean that the entire population should ideally have this measure in multiples. By "accessible", we mean easy to image using electronic sensors. By "acceptable", we mean that people do not object to having this measurement taken from them.

Quantitative measures of these five qualities have been developed [47–50]. Robustness is measured by the "false non-match rate" (also known as "Type I error"), the probability that a submitted sample will not match the enrollment image. Distinctiveness is measured by the "false match rate" (also known as "Type II error") – the probability that a submitted sample will match the enrollment image of another user. Availability is measured by the "failure to enroll" rate, the probability that a user will not be able to supply a readable measure to the system upon enrollment. Accessibility can be quantified by the "throughput rate" of the system, the number of individuals that can be processed in a unit time, such as a minute or an hour. Acceptability is measured by polling the device users. The first four qualities are inversely related to their above measures, a higher "false non-match rate", for instance, indicating a lower level of robustness.

Having identified the required qualities and measures for each quality, it would seem a straightforward problem to simply run some experiments, determine the measures, and set a weighting value for the importance of each, thereby determining the "best" biometric characteristic. Unfortunately, for all biometric characteristics, all of the desired qualities have been found to be highly dependent on the specifics of the application, the population (both their physiological and psychological states), and the hardware/software system used [51–54]. We cannot predict performance metrics for one application from tests on another. Further, the five metrics, which are correlated in a highly complex way, can be manipulated to some extent by administration policy.

System administrators might ultimately be concerned with: (1) the "false rejection rate", which is the probability that a true user identity claim will be falsely rejected, thus causing inconvenience; (2) the "false acceptance rate", which is the probability that a false identity claim will be accepted, thus allowing fraud; (3) the system throughput rate, measuring the number of users that can be processed in a time period; (4) the user acceptance of the system, which may be highly dependent upon the way the system is "packaged" and marketed; and (5) the ultimate total cost savings realized from implementing the system [55]. These latter, more practical, measures depend upon the basic system qualities in highly complex and competitive ways that are not at all well understood, and can be controlled only to a limited extent through administrative decisions [56, 57]. Predicting the "false acceptance" and "false rejection" rates, and system throughput, user acceptance and cost savings for operational systems from test data, is a surprisingly difficult task.

For the users, the questions are simple: "Is this system easier, faster, friendlier and more convenient than the alternatives?". These issues, too, are highly application-, technology- and marketing-specific.

Consequently, it is impossible to state that a single biometric characteristic is "best" for all applications, populations, technologies and administration policies. Yet some biometric characteristics are clearly more appropriate than others for any particular application. System administrators wishing to employ biometric authentication need to articulate clearly the specifics of their application. In the following sections, we look more carefully at the distinctions between applications.

1.4 The Applications

The operational goals of biometric applications are just as variable as the technologies: some systems search for known individuals; some search for unknown individuals; some verify a claimed identity; some verify an unclaimed identity; and some verify that the individual has no identity in the system at all. Some systems search one or multiple submitted samples against a large database of millions of previously stored "templates" – the biometric data given at the time of enrollment. Some systems search one or multiple samples against a database of a few "models" – mathematical representations of the signal generation process created at the time of enrollment. Some systems compare submitted samples against models of both the claimed identity and impostor identities. Some systems search one or multiple samples against only one "template" or "model".

And the application environments can vary greatly – outdoors or indoors, supervised or unsupervised, with people trained or not trained in the use of the acquisition device.

To make sense out of all of the technologies, application goals and environments, we need a systematic method of approach – taxonomies of uses and applications.

1.5 A Taxonomy of Uses

A biometric system can be designed to test one of only two possible hypotheses: (1) that the submitted samples are from an individual known to the system; or (2) that the submitted samples are from an individual not known to the system. Applications to test the first hypothesis are called "positive identification" systems (verifying a positive claim of enrollment), while applications testing the latter are "negative identification" systems (verifying a claim of no enrollment). All biometric systems are of one type or the other. This is the most important distinction between systems, and controls potential architectures, vulnerabilities and system error rates.

"Positive" and "negative" identification are "duals" of each other. Positive identification systems generally[1] serve to prevent multiple users of a single identity, while negative identification systems serve to prevent multiple identities of a single user. In positive identification systems, enrolled template or model storage can be centralized or decentralized in manner, including placement on optically read, magnetic stripe or smart cards. Negative identification systems demand centralized storage. Positive identification systems reject a user's claim to identity if no match between submitted samples and enrolled templates is found. Negative identification systems reject a user's claim to no identity if a match is found. Regardless of type of system, false rejections are a nuisance to users and false acceptances allow fraud.

An example of a positive identification system is the use of biometrics for employee access control at San Francisco International Airport. Hand geometry has been used since the early 1990s to control access by employees to secured airport areas. There are currently 180 readers used by about 18,000 enrolled users. Employees activate the system by swiping a magnetic stripe identity card through a reader. The purpose of the system is to limit use of the identification card to the enrolled owner, thereby prohibiting use of the card by multiple users. Although the 9-byte template could be stored on the magnetic stripe, in this case it is stored centrally to allow updating upon successful use. The stored hand shape template indexed to the card is transmitted from the central server to the access control device. The user then places the right hand in the hand geometry reader, making the implicit claim, "I am the user who is enrolled to use this card". If the submitted hand sample is found to be "close enough" to the stored template, the user's claim is accepted.

Santa Clara County, located in California near the San Francisco International Airport, requires the fingerprints of both left and right index fingers

1 Surveillance systems are also "positive" and "negative", but do not seek to prevent either multiple users of a single identity or multiple identities of a single user. A surveillance system for positive identification tests the hypothesis that all persons are on a list of authorized personnel. A negative system tests the hypothesis that no person is on the list of forbidden personnel.

from all applicants for social service benefits. Citizens are only eligible for benefits under a single identity and must attest upon enrollment that they are not already enrolled in the system. Consequently, this biometric system is for "negative identification". When an applicant applies for benefits, he or she places the index fingers on an electronic scanner with the implicit claim, "I am not known to this system". The submitted fingerprints are searched against the entire centralized database of enrolled persons – although to facilitate the search, the prints in the database might be partitioned by gender. If no match is found, the claim of non-identity in the system is accepted.

Use of biometrics in positive identification systems can be voluntary because alternative methods for verifying a claimed identity exist. Those electing not to use biometrics can have their identity verified in other ways, such as by presentation of a passport or driver's license. Use of biometrics in negative identification systems must be mandatory for all users because no alternative methods exist for verifying a claim of no known identity.

Those wishing to circumvent a positive identification system need to create a false match by impersonating an enrolled user. The possibility of biometric mimicry and forgery has been recognized since the 1970s [47, 58, 59]. Those wishing to circumvent a negative identification system need to submit altered samples not matching a previous enrollment. Table 1.1 summarizes these differences.

Historically, a distinction has been made between systems that verify a claimed identity and those that identify users without a claim of identity, perhaps returning a result that no identity was found. Some systems compare a single input sample to a single stored template or model to produce a "verification", or compare a single input sample to many stored templates to produce an "identification". Identification systems are said to compare

Table 1.1 Identification: "positive" and "negative".

Positive	Negative
To prove I am someone known to the system	To prove I am not someone known to the system
To prevent multiple users of a single identity	To prevent multiple identities of a single user
Comparison of submitted sample to single claimed template – "one-to-one" under the most common system design	Comparison of submitted sample to all enrolled templates – "one-to-many"
A "false match" leads to "false acceptance"	A "false match" or a "failure to acquire" leads to a "false rejection"
A "false non-match" or a "failure to acquire" leads to a "false rejection"	A "false non-match" leads to a "false acceptance"
Alternative identification methods exist	No alternative methods exist
Can be voluntary	Must be mandatory for all
Spoofed by submitting someone else's biometric measures	Spoofed by submitting no or altered measures

samples from one person to templates from many persons, with verification being the degenerate case of "many" equal to one. In the mid-1990s, several companies began to promote "PIN-less verification" systems, in which verification was accomplished without a claim to identity. The "verification/identification" dichotomy has been further clouded by the development of surveillance and modern "few-to-many" access control systems, which cannot be consistently classified as either "verification" or "identification". The uses and search strategies of biometric systems have expanded to the point where these distinctions of "verification/identification" and "one-to-one/one-to-many" are no longer fully informative.

Ultimately, a biometric system can only link a submitted sample to an enrolled template or model: that record created upon first use of the system by a person. That enrollment template/model need not be connected with any identifying information, such as a name or registration number. In fact, biometric measures and the enrollment templates/models derived from them contain no information about name, age, nationality, race or gender. Consequently, use of a biometric system without linkages of stored data to common identifiers allows for anonymous authentication. If system administrators have a need to connect the stored biometric data to other information, such as a name, that must be done by the presentation and human certification of trusted identifying credentials at the time of enrollment. Subsequent identification by the biometric system is no more reliable than this source documentation. But once that link has been made, subsequent identifications can be made without reference to the original source documents.

1.6 A Taxonomy of Application Environments

In the early 1990s, as we gained experience with the use of biometric devices, it became apparent that variations in the application environment had a significant impact on the way the devices performed. In fact, accurate characterization of the operational environment is primary in selecting the best biometric technology and in predicting the system's operational characteristics. In this section, we will present a method for analyzing a proposed operational environment by differentiating applications based on partitioning into six categories beyond the "positive" and "negative" applications already discussed.

1.6.1 Overt Versus Covert

The first partition is "overt/covert". If the user is aware that a biometric identifier is being measured, the use is overt. If unaware, the use is covert. Almost all conceivable access control and non-forensic applications are overt. Forensic applications can be covert.

1.6.2 Habituated Versus Non-Habituated

The second partition, "habituated/non-habituated", applies to the intended users of the application. Users presenting a biometric trait on a daily basis can be considered habituated after a short period of time. Users who have not presented the trait recently can be considered "non-habituated". A more precise definition will be possible after we have better information relating system performance to frequency of use for a wide population over a wide field of devices. If all the intended users are "habituated", the application is considered a "habituated" application. If all the intended users are "non-habituated", the application is considered "non-habituated". In general, all applications will be "non-habituated" during the first week of operation, and can have a mixture of habituated and non-habituated users at any time thereafter. Access control to a secure work area is generally "habituated". Access control to a sporting event is generally "non-habituated".

1.6.3 Attended Versus Non-Attended

A third partition is "attended/unattended", and refers to whether the use of the biometric device during operation will be observed and guided by system management. Non-cooperative applications will generally require supervised operation, while cooperative operation may or may not. Nearly all systems supervise the enrollment process, although some do not [4].

1.6.4 Standard Versus Non-Standard Environment

A fourth partition is "standard/non-standard operating environment". If the application will take place indoors at standard temperature (20 °C), pressure (1 atm), and other environmental conditions, particularly where lighting conditions can be controlled, it is considered a "standard environment" application. Outdoor systems, and perhaps some unusual indoor systems, are considered "non-standard environment" applications.

1.6.5 Public Versus Private

A fifth partition is "public/private". Will the users of the system be customers of the system management (public) or employees (private)? Clearly, attitudes toward usage of the devices, which will directly affect performance, vary depending upon the relationship between the end-users and system management.

1.6.6 Open Versus Closed

A sixth partition is "open/closed". Will the system be required, now or in the future, to exchange data with other biometric systems run by other management? For instance, some US state social services agencies want to be able to exchange biometric information with other states. If a system is to be open, data collection, compression and format standards are

required. A closed system can operate perfectly well on completely proprietary formats.

This list is open, meaning that additional partitions might also be appropriate. We could also argue that not all possible partition permutations are equally likely or even permissible.

1.6.7 Examples of the Classification of Applications

Every application can be classified according to the above partitions. For instance, the positive biometric identification of users of the Immigration and Naturalization Service's Passenger Accelerated Service System (INSPASS) [1, 60], currently in place at Kennedy, Newark, Los Angeles, Miami, Detroit, Washington Dulles, Vancouver and Toronto airports for rapidly admitting frequent travelers into the USA, can be classified as a cooperative, overt, non-attended, non-habituated, standard environment, public, closed application. The system is cooperative because those wishing to defeat the system will attempt to be identified as someone already holding a pass. It will be overt because all will be aware that they are required to give a biometric measure as a condition of enrollment into this system. It will be non-attended and in a standard environment because collection of the biometric will occur near the passport inspection counter inside the airports, but not under the direct observation of an INS employee. It will be non-habituated because most international travelers use the system less than once per month. The system is public because enrollment is open to any frequent traveler into the USA. It is closed because INSPASS does not exchange biometric information with any other system.

The negative identification systems for preventing multiple identities of social service recipients can be classified as non-cooperative, overt, attended, non-habituated, open, standard environment systems.

Clearly, the latter application is more difficult than the former. Therefore we cannot directly compare hand geometry and facial recognition technologies based on the error rates across these very different applications.

1.7 A System Model

Although these devices rely on widely different technologies, much can be said about them in general. Figure 1.1 shows a generic biometric authentication system divided into five subsystems: data collection, transmission, signal processing, decision and data storage. We will consider these subsystems one at a time.

1.7.1 Data Collection

Biometric systems begin with the measurement of a behavioral/physiological characteristic. Key to all systems is the underlying assumption that the

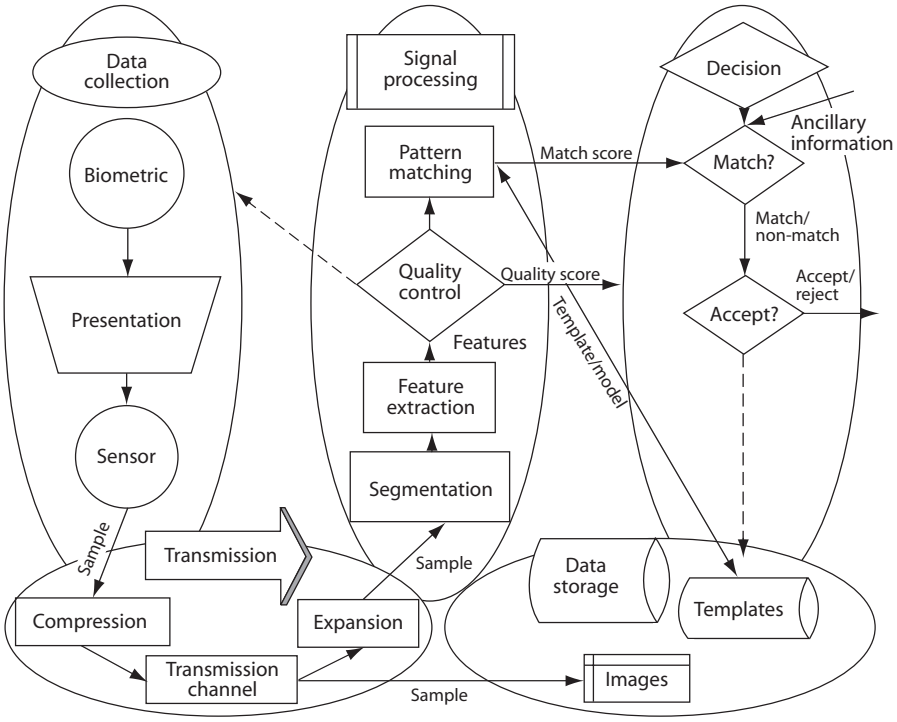

Figure 1.1 A generic biometric system.

measured biometric characteristic is both distinctive between individuals and repeatable over time for the same individual. The problems in measuring and controlling these variations begin in the data collection subsystem.

The user's characteristic must be presented to a sensor. The presentation of any biometric characteristic to the sensor introduces a behavioral (and, consequently, psychological) component to every biometric method. This behavioral component may vary widely between users, between applications, and between the test laboratory and the operational environment. The output of the sensor, which is the input data upon which the system is built, is the convolution of: (1) the biometric measure; (2) the way the measure is presented; and (3) the technical characteristics of the sensor. Both the repeatability and the distinctiveness of the measurement are negatively impacted by changes in any of these factors. If a system is to be open, the presentation and sensor characteristics must be standardized to ensure that biometric characteristics collected with one system will match those collected on the same individual by another system. If a system is to be used in an overt, non-cooperative application, the user must not be able to willfully change the biometric or its presentation sufficiently to avoid being matched to previous records.

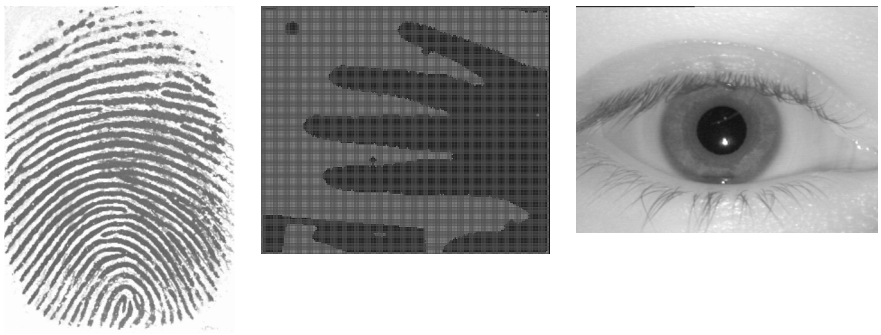

Figure 1.2 Fingerprint, hand and iris system input images.

Figure 1.2 shows input images from fingerprint, hand geometry and iris recognition systems.

1.7.2 Transmission

Some, but not all, biometric systems collect data at one location but store and/or process it at another. Such systems require data transmission. If a great amount of data is involved, compression may be required before transmission or storage to conserve bandwidth and storage space. Figure 1.1 shows compression and transmission occurring before the signal processing and image storage. In such cases, the transmitted or stored compressed data must be expanded before further use. The process of compression and expansion generally causes quality loss in the restored signal, with loss increasing with increasing compression ratio. The compression technique used will depend upon the biometric signal. An interesting area of research is in finding, for a given biometric technique, compression methods with minimum impact on the signal-processing subsystem.

If a system is to be open, compression and transmission protocols must be standardized so that every user of the data can reconstruct the original signal. Standards currently exist for the compression of fingerprints (Wavelet Scalar Quantization), facial images (JPEG), and voice data (Code Excited Linear Prediction).

1.7.3 Signal Processing

Having acquired and possibly transmitted a biometric characteristic, we must prepare it for matching with other like measures. Figure 1.1 divides the signal-processing subsystem into four tasks: segmentation, feature extraction, quality control, and pattern matching.

Segmentation is the process of finding the biometric pattern within the transmitted signal. For example, a facial recognition system must first find the boundaries of the face or faces in the transmitted image. A speaker

verification system must find the speech activity within a signal that may contain periods of non-speech sounds. Once the raw biometric pattern of interest has been found and extracted from larger signal, the pattern is sent to the feature extraction process.

Feature extraction is fascinating. The raw biometric pattern, even after segmentation from the larger signal, contains non-repeatable distortions caused by the presentation, sensor and transmission processes of the system. These non-controllable distortions and any non-distinctive or redundant elements must be removed from the biometric pattern, while at the same time preserving those qualities that are both distinctive and repeatable. These qualities expressed in mathematical form are called "features". In a text-independent speaker recognition system, for instance, we may want to find the features, such as the mathematical frequency relationships in the vowels, that depend only upon the speaker and not upon the words being spoken, the health status of the speaker, or the speed, volume and pitch of the speech. There are as many wonderfully creative mathematical approaches to feature extraction as there are scientists and engineers in the biometrics industry. You can understand why such algorithms are always considered proprietary. Consequently, in an open system, the "open" stops here.

In general, feature extraction is a form of non-reversible compression, meaning that the original biometric image cannot be reconstructed from the extracted features. In some systems, transmission occurs after feature extraction to reduce the requirement for bandwidth.

After feature extraction, or maybe even before, we will want to check to see if the signal received from the data collection subsystem is of good quality. If the features "don't make sense" or are insufficient in some way, we can conclude quickly that the received signal was defective and request a new sample from the data collection subsystem while the user is still at the sensor. The development of this "quality control" process has greatly improved the performance of biometric systems in the last few short years. On the other hand, some people seem never to be able to present an acceptable signal to the system. If a negative decision by the quality control module cannot be overridden, a "failure to enroll" error results.

The feature "sample", now of very small size compared to the original signal, will be sent to the pattern matching process for comparison with one or more previously identified and stored feature templates or models. We use the term "template" to indicate stored features. The features in the template are of the same type as those of a sample. For instance, if the sample features are a "vector" in the mathematical sense, then the stored template will also be a "vector". The term "model" is used to indicate the construction of a more complex mathematical representation capable of generating features characteristic of a particular user. Models and features will be of different mathematical types and structures. Models are used in some speaker and facial recognition systems. Templates are used in fingerprint, iris, and hand geometry recognition systems.

The term "enrollment" refers to the placing of a template or model into the database for the very first time. Once in the database and associated

with an identity by external information (provided by the enrollee or others), the enrollment biometric data is referred to as the template or model for the individual to which it refers.

The purpose of the pattern matching process is to compare a presented feature sample to the stored data, and to send to the decision subsystem a quantitative measure of the comparison. An exception is enrollment in systems allowing multiple enrollments. In this application, the pattern matching process can be skipped. In the cooperative case where the user has claimed an identity or where there is but a single record in the current database (which might be a magnetic stripe card), the pattern matching process might only make a comparison against a single stored template. In all other cases, such as large-scale identification, the pattern matching process compares the present sample to multiple templates or models from the database one at a time, as instructed by the decision subsystem, sending on a quantitative "distance" measure for each comparison. In place of a "distance" measure, some systems use "similarity" measures, such as maximum likelihood values.

The signal processing subsystem is designed with the goal of yielding small distances between enrolled models/templates and later samples from the same individual and large distances between enrolled models/templates and samples of different individuals. Even for models and samples from the same individual, however, distances will rarely, if ever, be zero, as there will always be some non-repeatable biometric-, presentation-, sensor- or transmission-related variation remaining after processing.

1.7.4 Storage

The remaining subsystem to be considered is that of storage. There will be one or more forms of storage used, depending upon the biometric system. Templates or models from enrolled users will be stored in a database for comparison by the pattern matcher to incoming feature samples. For systems only performing "one-to-one" matching, the database may be distributed on smart cards, optically read cards or magnetic stripe cards carried by each enrolled user. Depending upon system policy, no central database need exist, although in this application a centralized database can be used to detect counterfeit cards or to reissue lost cards without re-collecting the biometric pattern.

The database will be centralized if the system performs one-to-*N* matching with *N* greater than one, as in the case of identification or "PIN-less verification" systems. As *N* gets very large, system speed requirements dictate that the database be partitioned into smaller subsets such that any feature sample need only be matched to the templates or models stored in one partition, or indexed by using an appropriate data structure which allows the templates to be visited in an advantageous order during the retrieval [61]. These strategies have the effect of increasing system speed and decreasing false matches, at the expense of increasing the false non-match rate owing to partitioning errors. This means that system error rates do not remain constant with increasing database size and identification

systems do not scale linearly. Consequently, database partitioning/indexing strategies represent a complex policy decision [56].

If it may be necessary to reconstruct the biometric patterns from stored data, raw (although possibly compressed) data storage will be required. The biometric pattern is generally not reconstructable from the stored templates or models, although some methods [41] do allow a coarse reconstruction of patterns from templates. Further, the templates themselves are created using the proprietary feature extraction algorithms of the system vendor. The storage of raw data allows changes in the system or system vendor to be made without the need to re-collect data from all enrolled users.

1.7.5 Decision

The decision subsystem implements system policy by directing the database search, determines "matches" or "non-matches" based on the distance or similarity measures received from the pattern matcher, and ultimately makes an "accept/reject" decision based on the system policy. Such a decision policy could be to reject the identity claim (either positive or negative) of any user whose pattern could not be acquired. For an acquired pattern, the policy might declare a match for any distance lower than a fixed threshold and "accept" a user identity claim on the basis of this single match, or the policy could be to declare a match for any distance lower than a user-dependent, time-variant, or environmentally linked threshold and require matches from multiple measures for an "accept" decision. The policy could be to give all users, good guys and bad guys alike, three tries to return a low distance measure and be "accepted" as matching a claimed template. Or, in the absence of a claimed template, the system policy could be to direct the search of all, or only a portion, of the database and return a single match or multiple "candidate" matches. The decision policy employed is a management decision that is specific to the operational and security requirements of the system. In general, lowering the number of false non-matches can be traded against raising the number of false matches. The optimal system policy in this regard depends both upon the statistical characteristics of the comparison distances coming from the pattern matcher, the relative penalties for false match and false non-match within the system, and the *a priori* (guessed in advance) probabilities that a user is, in fact, an impostor. In any case, in the testing of biometric devices, it is necessary to decouple the performance of the signal processing subsystem from the policies implemented by the decision subsystem.

1.8 Biometrics and Privacy

Whenever biometric identification is discussed, people always want to know about the implications for personal privacy. If a biometric system is used, will the government, or some other group, be able to get personal

information about the users? Biometric measures themselves contain no personal information. Hand shape, fingerprints or eye scans do not reveal name, age, race, gender, health or immigration status. Although voice patterns can give a good estimation of gender, no other biometric identification technology currently used reveals anything about the person being measured. More common identification methods, such as a driver's license, reveal name, address, age, gender, vision impairment, height and even weight! Driver's licenses, however, may be easier to steal or counterfeit than biometric measures.

Biometric measures can be used in place of a name, Social Security number or other form of identification to secure anonymous transactions. Walt Disney World sells season passes to buyers anonymously, then uses finger geometry to verify that the passes are not being transferred. Use of iris or fingerprint recognition for anonymous health care screening has also been proposed. A patient would use an anonymous biometric measure, not a name or Social Security number, when registering at a clinic. All records held at the clinic for that patient would be identified, linked and retrieved only by the measure. No one at the clinic, not even the doctors, would know the patient's "real" (publicly recognized) identity.

The real fear is that biometric measures will link people to personal data, or allow movements to be tracked. After all, credit card and phone records can be used in court to establish a person's activities and movements. There are several important points to be made on this issue.

Phone books are public databases linking people to their phone number. These databases are even accessible on the Internet. Because phone numbers are unique to phone lines[2], "reverse" phone books also exist, allowing a name to be determined from a phone number. Even if a number is unlisted, all information on calls made from that number may be available to law enforcement agencies through the subpoena process. There are no public databases, however, containing biometric identifiers, and there are only a few limited-access government databases. Five US states have electronic fingerprint records of social service recipients (Arizona, California, Connecticut, New York and Texas); six states (California, Colorado, Georgia, Hawaii, Oklahoma and Texas) maintain electronic fingerprints of all licensed drivers[3]; nearly all states maintain copies of driver's license and social service recipient photos; the FBI and state governments maintain fingerprint databases on convicted felons and sex offenders; and the federal government maintains hand geometry records on those who have voluntarily requested border crossing cards [62]. General access to this data is limited to the agencies that collected it,

2 In the days of multi-user "party lines" this was not true, and phone numbers did not uniquely map to phone lines and households. Such "party lines" are now mostly gone, allowing phone numbers to indicate a user household or business uniquely.

3 West Virginia maintains a voluntary fingerprint database on drivers who wish to use biometric identification.

but like credit card and phone "toll records", this information can be released or searched by law enforcement groups acting under court order.

Unlike phone books, however, databases of biometric measures cannot generally be reversed to reveal names from measures because biometric measures, although distinctive, are not unique. Fingerprint, retinal and iris databases may be exceptions, allowing reversal if the biometric data was carefully collected. But general biometric measures do not serve as useful pointers to other types of data. The linking of records is always done by unique identifiers such as Social Security and credit card numbers. Biometric measures are not generally useful in this regard, even if databases linking information to measures were to exist. For these reasons, biometric measures are not useful for tracking the movements of people, as is already possible using telephone and credit card numbers.

Databases of biometric images, and the numerical models or templates derived from them, are often encrypted with the intention of inhibiting their compromise in bulk. But compromise of individual measures cannot always be prevented by protecting databases and transmission channels because biometric measures, although privately owned, are sometimes publicly observable (e.g. a photo of a person's face can be taken with a camera or downloaded from a web page). In general, biometric measures are not secret, even if it might be quite complicated to acquire usable copies (e.g. a retinal map) without the cooperation of the owner. When used for security, biometric characteristics are more like public keys than private keys. Unlike public keys, however, biometric measures cannot be revoked if stolen or mimicked. The industry is currently working on methods for "live-ness testing" and revocation, hoping to ameliorate these problems [63–65].

Table 1.2 summarizes the privacy issues raised by the use of biometrics.

Table 1.2 Biometrics and privacy.

1. Unlike more common forms of identification, biometric measures contain no personal information and are more difficult to forge or steal.
2. Biometric measures can be used in place of a name or Social Security number to secure anonymous transactions.
3. Some biometric measures (face images, voice signals and "latent" fingerprints left on surfaces) can be taken without a person's knowledge, but cannot be linked to an identity without a pre-existing invertible database.
4. A Social Security or credit card number, and sometimes even a legal name, can identify a person in a large population. This capability has not been demonstrated using any single biometric measure.
5. Like telephone and credit card information, biometric databases can be searched outside of their intended purpose by court order.
6. Unlike credit card, telephone or Social Security numbers, biometric characteristics change from one measurement to the next.
7. Searching for personal data based on biometric measures is not as reliable or efficient as using better identifiers, like legal name or Social Security number.
8. Biometric measures are not always secret, but are sometimes publicly observable and cannot be revoked if compromised.

1.9 The Road Ahead

Market estimates put the total hardware sales for the industry at US$6.6 million in 1990 and nearly US$200 million in 2000 [66]. Whether the next decade will result in a similar 2500% increase will depend upon user demand for positive identification biometrics. That demand will be created by imaginatively created systems designed for convenience, friendliness, cost-effectiveness and ease of use.

The use of negative identification biometrics will be fueled by government requirements to limit citizens to a single identity in driver licensing, social service and other civil applications [67, 68]. That demand will require the development of stronger criteria for cost/benefit assessment, security assurance, and privacy protection. Although we cannot predict the future rate of growth of the industry with any certainty, we do know that long-term growth is inevitable. With this book, we hope to stimulate further inquiry into the technologies, applications and issues that will shape this industry in the years to come.

References

[1] B. Wing, Overview of all INS biometrics projects. *Proc. CTST'98*, pp. 543–552.
[2] G. Slagle, Standards for the driver's license. *Proc. CTST'99*, pp. 891–902.
[3] J. Walters, Casinos must tell customers that police are scanning faces. *Toronto Star*, February 27, 2001, Edition 1.
[4] G. Levin, Real world, most demanding biometric system usage. *Proc. Biometrics Consortium, 2001/02*, Crystal City, VA, February 14–15, 2002.
[5] J. Markowitz, Voice biometrics: speaker recognition applications and markets 1999. *Voice Europe 1999: European Symposium on Voice Technologies*, London.
[6] J. Perkins, FT-IT: New services will keep eye on security: biometrics. *Financial Times* (London), February 21, 2001, Wednesday Surveys ITC1.
[7] B. Miller, Everything you need to know about biometric identification. *Personal Identification News 1988 Biometric Industry Directory*, Warfel & Miller, Inc., Washington DC, January 1988.
[8] J. Wayman, A definition of biometrics *National Biometric Test Center Collected Works 1997–2000*, San Jose State University, 2000.
[9] R. M. Bolle, J. H. Connell, N. Haas, R. Mohan and G. Taubin, VeggieVision: a produce recognition system. *Workshop on Automatic Identification Advanced Technologies*, November 1997, pp. 35–38.
[10] R. Jantz, Anthropological dermatoglyphic research. *Ann. Rev. Anthropol.*, **16**, 161–177, 1987.
[11] R. Jantz, Variation among European populations in summary finger ridge-count variables. *Ann. Human Biol.*, **24**(2), 97–108, 1997.
[12] *Webster's New World Dictionary of the American Language*, College Edition. World Publishing Co., New York, 1966.
[13] C. Beavan, *Fingerprints: The Origins of Crime Detection and the Murder Case that Launched Forensic Science*. Hyperion, New York, 2001.
[14] S. Cole, What counts for identity?: the historical origins of the methodology of latent fingerprint identification. *Fingerprint Whorld*, **27**, 103, January 2001.

[15] S. Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Harvard University Press, 2001.
[16] C. Reedman, Biometrics and law enforcement. Available from http://www.dss.state.ct.us/digital/biometrics%20and%20law%20enforcement.htm (accessed May 31, 2004).
[17] http://www.cimm.jcu.edu.au/hist/stats/bert/index.htm
[18] H. Faulds, On the skin furrows of the hand. *Nature*, **22**, 605, October 28, 1880.
[19] W. Herschel, Skin furrows of the hand. *Nature*, **23**, 76, November 25, 1880.
[20] F. Galton, Personal identification and description. *Nature*, June 21 and 28, 1888, pp. 173–177, 201–202.
[21] S. Pruzansky, Pattern-matching procedure for automatic talker recognition. *J. Acoust. Soc. Am.*, **35**, 354–358, 1963.
[22] K. P. Li, J. E. Dammann and W. D. Chapman, Experimental studies in speaker verification using an adaptive system. *J. Acoust. Soc. Am.*, **40**, 966–978, 1966.
[23] J. Luck, Automatic speaker verification using cepstral measurements. *J. Acoust. Soc. Am.*, **46**, 1026–1031, 1969.
[24] K. Stevens, C. Williams, J. Carbonell and B. Woods, Speaker authentication and identification: a comparison of spectrographic and auditory presentation of speech material. *J. Acoust. Soc. Am.*, **44**, 596–607, 1968.
[25] B. Atal, Automatic recognition of speakers from their voices. *Proc. IEEE*, **64**(4), 460–474, 1976.
[26] A. Rosenberg, Automatic speaker recognition: a review. *Proc. IEEE*, **64**(4), 475–487, 1976.
[27] M. Trauring, Automatic comparison of finger-ridge patterns. *Nature*, **197**, 938–940, 1963.
[28] M. Trauring, On the automatic comparison of finger-ridge patterns. *Hughes Laboratory Research Report No. 190*, 1961.
[29] R. Zunkel, Hand geometry based verifications, in A. Jain, *et al.* (eds) *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Press, 1999.
[30] A. Fejfar and J. Myers, The testing of 3 automatic ID verification techniques for entry control. *2nd Int. Conf. on Crime Countermeasures*, Oxford, 25–29 July, 1977.
[31] National Bureau of Standards, Guidelines on the evaluation of techniques for automated personal identification. *Federal Information Processing Standards Publication 48*, April 1, 1977.
[32] H. D. Crane and J. S. Ostrem, Automatic signature verification using a three-axis force-sensitive pen. *IEEE Trans. on Systems, Man and Cybernetics*, **SMC-13**(3), 329–337, 1983.
[33] V. S. Nalwa, Automatic on-line signature verification. *Proc. IEEE*, **85**(2), 215–239, 1997.
[34] J. R. Samples and R. V. Hill, Use of infrared fundus reflection for an identification device. *Am. J. Ophthalmol.*, **98**(5), 636–640, 1984.
[35] R. H. Hill, Retina identification, in A. Jain, *et al.* (eds) *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Press, 1999.
[36] L. D. Harmon, M. K. Khan, R. Lasch and P. F. Ramig, Machine recognition of human faces. *Pattern Recognition*, **31**(2), 97–110, 1981.
[37] A. Samal and P. Iyengar, Automatic recognition and analysis of human faces and facial expressions: a survey. *Pattern Recognition*, **25**, 65–77, 1992.
[38] R. Chellappa, C. L. Wilson and S. Sirohey, Human and machine recognition of faces: a survey. *Proc. IEEE*, **83**(5), 705–740, 1995.
[39] L. Sirovich and M. Kirby, Low-dimensional procedure for the characterization of human faces. *J. Optical Soc. Am.*, **4**, 519–524, 1987.

[40] M. Turk and A. Pentland, Eigenfaces for recognition. *J. Cognitive Neuroscience*, **3**(1), 71–86, 1991.
[41] J. Zhang, Y. Yan and M. Lades, Face recognition: eigenface, elastic matching and neural nets. *Proc. IEEE*, **85**(9), 1423–1436, 1997.
[42] J. D. Daugman, High confidence visual recognition of persons by a test of statistical independence, *IEEE Trans. Pattern Analysis and Machine Intelligence*, **15**(11), 1148–1161, 1993.
[43] R. P. Wildes, Iris recognition: an emerging biometric technology, *Proc. IEEE*, **85**(9), 1348–1364, 1997.
[44] A. Jain, R. Bolle and S. Pankati, Introduction to biometrics, in A. Jain, *et al.* (eds) *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Press, 1999.
[45] J. Wayman, Fundamentals of biometric authentication technologies. *Int. J. Imaging and Graphic*s, **1**(1), 2001.
[46] J. L. Wayman, Technical testing and evaluation of biometric identification devices, in A. Jain, *et al.* (eds) *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Press, 1999.
[47] D. E. Raphael and J. R. Young, *Automated Personal Identification*. SRI International, 1974.
[48] W. Haberman and A. Fejfar, Automatic identification of personnel through speaker and signature verification – system description and testing. *Proc. 1976 Carnahan Conference on Crime Countermeasures*, Lexington, KY, May 1976, pp. 23–30.
[49] R. L. Maxwell, General comparison of six different personnel identity verifiers. *Sandia National Laboratories, Organization 5252 Report*, June 20, 1984.
[50] A. J. Mansfield and J. L. Wayman, *Best Practices in Testing and Reporting Biometric Device Performance*, version 2.0. U.K. Biometrics Working Group. Available online at `http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf`
[51] J. P.Phillips, A. Martin, C. Wilson and M. Przybocki, An introduction to evaluating biometric systems. *IEEE Computer*, February 2000, p. 56–63.
[52] D. Maio, D. Maltoni, J. Wayman and A. Jain, FVC2000: Fingerprint verification competition 2000, *Proc. 15th International Conference on Pattern Recognition,* Barcelona, September 2000. Available online at `http://www.csr.unibo.it/research/biolab/`.
[53] A. Mansfield, G. Kelly, D. Chandler and J. Kane, *Biometric Product Testing Final Report*. National Physical Laboratory, London, March 19, 2001. Available online at `http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf`.
[54] D. Blackburn, M. Bone, P. Grother and J. Phillips, *Facial Recognition Vendor Test 2000: Evaluation Report*, January 2001. Available online at `http://www.dodcounterdrug.com/facialrecognition/FRVT2000/documents.htm`.
[55] W. Wilson, Establishing the business case for biometrics. *Proc. Biometric Consortium 2000*, Gaithersburg, MD, September, 2000.
[56] J. L. Wayman, Error rate equations for the general biometric system. *IEEE Automation and Robotics*, **6**(1), 35–48, 1999.
[57] J. Ashbourne, *Biometrics: Advanced Identification Technology*. Springer, 2000.
[58] R. C. Lummis and A. Rosenberg, Test of an automatic speaker verification method with intensively trained mimics. *J. Acoust. Soc. Am.*, **51**, 131(A), 1972.
[59] G. Warfel, *Identification Technologies: Computer, Optical, and Chemical Aids to Personal ID*. Charles C. Thomas, Springfield, IL, 1979.

[60] J. L. Wayman, Report on the evaluation of the INSPASS hand geometry system. In *National Biometric Test Center Collected Works 1997–2000*, San Jose State University, 2000.
[61] R. Cappelli, D. Maio and D. Maltoni, Indexing fingerprint databases for efficient 1:*N* matching. *Int. Conf. (6th) on Control, Automation, Robotics and Vision (ICARCV2000)*, Singapore, December 2000.
[62] J. Wayman, Federal biometric technology legislation. *IEEE Computer*, **33**(2), 76–80, 2000.
[63] R. Derakhshani, S. Schuckers, L. Hornak and L. O'Gorman, Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. *Pattern Recognition*, **17**(2), 2003.
[64] N. Ratha, J. Connell and R. Bolle, Cancelable biometrics. *Proc. Biometrics Consortium 2000*, Gaithersburg, MD, September 13–14, 2000.
[65] J. Cambier, U.C. von Seelen, R. Glass, R. Moore, I. Scott, M. Braithwaite and J. Daugman, Application-specific biometric templates. *Proc. Third Workshop on Automatic Identification and Advanced Technologies*, Tarrytown, New York, March 14–15, 2002.
[66] E. Bowman, Identifying trends: the evolving biometrics market. *ID World*, **1**(5), 7, 1999.
[67] *National Standard for Driver's License/Identification Card*, AAMVA June 30, 2000. Available online at `http://www.aamva.org/`.
[68] D. Mintie, Biometrics for state identification applications – operational experiences. *Proc. CTST'98*, **1**, 299–312.

http://www.springer.com/978-1-85233-596-0

Biometric Systems
Technology, Design and Performance Evaluation
(Eds.)J.L. Wayman; A.K. Jain; D. Maltoni; D. Maio
2005, XIV, 370 p., Hardcover
ISBN: 978-1-85233-596-0