Biometric Identification

When it comes to working biometric identification technologies, it's not only our fingerprints that do the talking. Now, our eyes, hands, signature, speech, and even facial temperature can ID us.

Questions related to the identity of individuals such as "Is this the person who he or she claims to be?," "Has this applicant been here before?," "Should this individual be given access to our system?" are asked millions of times every day by organizations in financial services, health care, e-commerce, telecommunication, and government. In fact, identity fraud in welfare disbursements, credit card transactions, cellular phone calls, and ATM withdrawals totals over $6 billion each year [5].

For this reason, more and more organizations are looking to automated identity authentication systems to improve customer satisfaction and operating efficiency as well as to save critical resources (see Figure 1). Furthermore, as people become more connected electronically, the ability to achieve a highly accurate automatic personal identification system is substantially more critical [5].

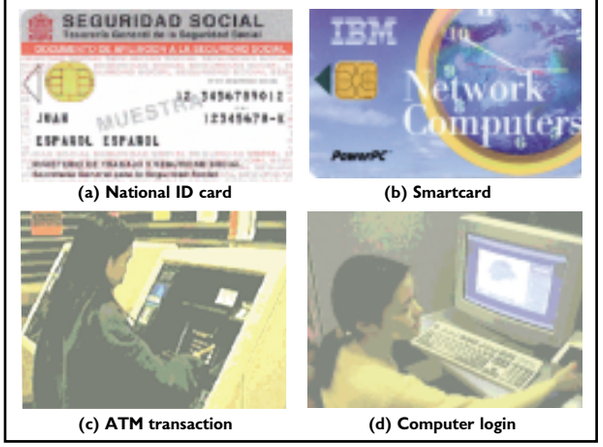
Personal identification is the process of associating a particular individual with an identity. Identification can be in the form of verification (also known as authentication), which entails authenticating a claimed identity ("Am I who I claim I am?"), or recognition (also known as identification), which entails determining the identity of a given person from a database of persons known to the system ("Who am I?"). Knowledge-based and token-based automatic personal identification approaches have been the two traditional techniques widely used [8]. Token-based approaches use something you have to make a personal identification, such as a passport, driver's license, ID card, credit card, or keys. Knowledge-based approaches use something you know to make a personal identification, such as a password or a personal identification number (PIN). Since these traditional approaches are not based on any inherent attributes of an individual to make a personal identification, they suffer from the

WALTER SIPSER

Anil Jain, Lin Hong, and Sharath Pankanti

THE AUTHORS ARE GRATEFUL TO EYEDENTIFY CORP., IRISCAN INC., AND MIKOS LTD. FOR PROVIDING THE PICTURES OF RETINA, SMARTCARD, IRIS, AND THERMOGRAM, RESPECTIVELY

Figure 1. Biometric applications.



(a) National ID card (b) Smartcard

(c) ATM transaction (d) Computer login

obvious disadvantages: tokens may be lost, stolen, forgotten, or misplaced, and a PIN may be forgotten by a valid user or guessed by an impostor. (Surprisingly, approximately 25% of the people appear to write their PIN on their ATM card, thus defeating the protection offered by PIN when ATM cards are stolen [5]!) Because knowledge-based and token-based approaches are unable to differentiate between an authorized person and an impostor who fraudulently acquires the token or knowledge of the authorized person [8], they are unsatisfactory means of achieving the security requirements of our electronically interconnected information society.

Biometric identification refers to identifying an individual based on his or her distinguishing physiological and/or behavioral characteristics (biometric identifiers) [5]. It associates/disassociates an individual with a previously determined identity/identities based on how one is or what one does. Because many physiological or behavioral characteristics are distinctive to each person, biometric identifiers are inherently more reliable and more capable than knowledge-based and token-based techniques in differentiating between an authorized person and a fraudulent impostor.

A biometric system is essentially a pattern recognition system that makes a personal identification by establishing the authenticity of a specific physiological or behavioral characteristic possessed by the user. Logically, a biometric system can be divided into the enrollment module and the identification module (see Figure 2). During the enrollment phase, the biometric characteristic of an individual is first scanned by a biometric sensor to acquire a digital representation of the characteristic. In order to facilitate matching and to reduce the storage requirements, the digital representation is further processed by a feature extractor to generate a compact but expressive representation, called a "template." Depending on the application, the template may be stored in the central database of the biometric system or be recorded on a magnetic card or smartcard issued to the individual.

During the recognition phase, the biometric reader captures the characteristic of the individual to be identified and converts it to a digital format, which is further processed by the feature extractor to produce the same representation as the template. The resulting representation is fed to the feature matcher that compares it against the template(s) to establish the identity of the individual.

An ideal biometric should be *universal*, where each person possesses the characteristic; *unique*, where no two persons should share the characteristic; *permanent*, where the characteristic should neither change nor be alterable; and *collectable*, where the characteristic is readily presentable to a sensor and is easily quantifiable.

In practice, however, a characteristic that satisfies all these requirements may not always be feasible for a useful biometric system. The designer of a practical biometric system must also consider a number of other issues, including:

- *Performance*, that is, a system's accuracy, speed, robustness, as well as its resource requirements, and operational or environmental factors that affect its accuracy and speed;
- *Acceptability*, or the extent people are willing to accept for a particular biometric identifier in their daily lives;
- *Circumvention*, as in how easy it is to fool the system through fraudulent methods.

Depending on the application context, a biometric system may either operate in a verification (authentication) mode or in a recognition (identification) mode [5]. A verification system authenticates a person's identity by comparing the captured biometric

Table 1. Biometric applications

Forensic	Civilian	Commercial
Criminal investigation	National ID	ATM
Corpse identification	Driver's license	Credit card
Parenthood determination	Welfare disbursement	Cellular phone
	Border crossing	Access control

characteristic with the person's own biometric template(s) prestored in the database. In this system, an individual who desires to be identified submits a claim to an identity usually via a magnetic-stripe card, login name, or smartcard, and the system either rejects or accepts the submitted claim of identity. In a recognition system, the system establishes a subject's identity (or fails to if the subject is not enrolled in the system database) by searching the entire template database for a match—-without the subject having to claim an identity.

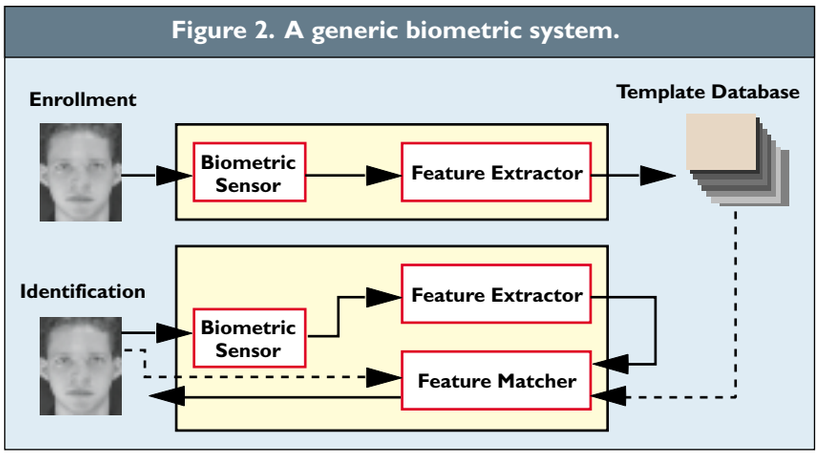


Figure 2. A generic biometric system.

Measuring Performance

Evaluating the performance of a biometric identification system is a challenging research topic [12]. The overall performance of a biometric system is assessed in terms of its accuracy, speed, and storage. Several other factors, like cost and ease-of-use, also affect efficacy.

Biometric systems are not perfect, and will sometimes mistakenly accept an impostor as a valid individual (a false match) or conversely, reject a valid individual (a false nonmatch). The probability of committing these two types of errors are termed false nonmatch rate (FNR) and false match rate (FMR); the magnitudes of these errors depend upon how liberally or conservatively the biometric system operates. Figure 3 shows the trade-off between a system's FMR and FNR at different operating points; it's called the "Receiver Operating Characteristics (ROC)" and is a comprehensive measure of the system accuracy in a given test environment.

High-security access applications, where concern about break-in is great, operate at a small FMR. Forensic applications, where the desire to catch a criminal outweighs the inconvenience of examining a large number of falsely accused individuals, operate their matcher at a high FMR. Civilian applications attempt to operate their matchers at the operating points with both a low FNR and a low FMR. The error rate of the system at an operating point where FMR equals FNR is called the equal error rate (EER) which may often be used as a terse descriptor of system accuracy. Accuracy performance of a biometrics system is considered acceptable if the risks (benefits) associated with the errors in the decision-making at a given operating point on ROC for the given test environment are acceptable. Similarly, accuracy of a biometrics-based identification is unacceptable/poor if the risks (benefits) associated with errors related to any operating point on the ROC for a given test environment are unacceptable (insufficient).

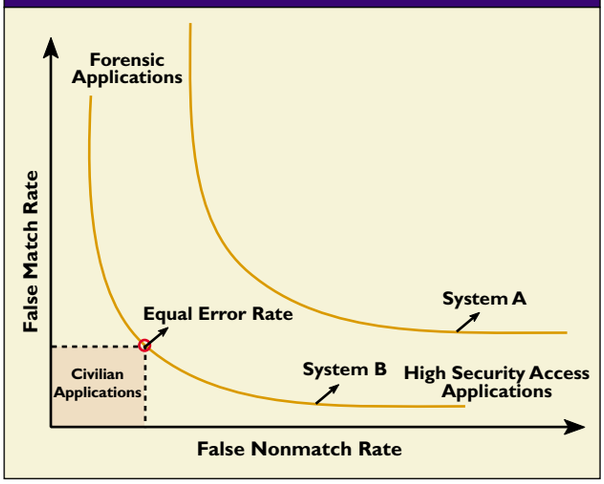
The size of a template, the number of templates stored per individual, and the availability of compression mechanisms determine the storage required per user. When template sizes are large and the templates are stored in a central database, network bandwidth may become a system bottleneck for identification. A typical smartcard may only hold a few kilobytes of information (for instance, 8K) and in systems using smartcards to distribute the template storage, template size becomes an important design issue.

The time required by a biometric system to make an identification decision is critical to many applications. For a typical access-control application, the system needs to make an authentication decision in real-time. In an ATM application, for instance, it is desirable to accomplish the authentication within about one second. For forensic applications, however, the time requirements may not be very stringent.

All other factors remaining identical, the widespread use of biometrics will be stimulated by its adoption in the consumer market. The single most important factor affecting this realization is the cost of the biometrics systems including the sensors and related infrastructure. Some sensors, such as microphones, are already very inexpensive, while others, such as CCD cameras, are now becoming standard peripherals in a personal computing environment. With the recent advances in solid-state technology, fingerprint sensors will become sufficiently inexpensive in the next few years. Storage requirements of the biometric templates and processing requirements for matching are among the two major considerations towards the infrastructure cost.

The human factors issue is also important to the

Figure 3. Receiver Operating Characteristics (ROC) of a system illustrates false nonmatch rate (FNR) and false match rate (FMR) of a matcher at all operating points. Each point on a ROC defines FNR and FMR for a given matcher, operating at a particular matching score threshold. A smaller FNR (that is, a more tolerant system) usually leads to a larger FMR while a smaller FMR (a less tolerant system) usually implies a larger FNR. Note that System A is consistently inferior to System B in accuracy performance.



success of a biometric-based identification. How easy and comfortable is it to acquire a given biometric? For example, biometric measurements that do not involve touching an individual, such as face, voice, or iris, may be perceived as more user-friendly. Additionally, biometric technologies requiring very little cooperation/participation from the users (such as face and thermograms) may be perceived as more convenient to users. A related issue is public acceptance. There may be a prevalent perception that biometrics are a threat to the privacy of an individual. In this regard, the public needs to learn that biometrics could be one of the most effective, and in the long run, more profitable means for protecting individual privacy. For instance, a biometrics-based patient information system can reliably ensure that medical records can only be accessed by medical personnel and the individual concerned. As in any industry, government regulations and directives may either provide a boost or lead to the demise of certain types of biometric technologies. Upcoming U.S. legislation such as the Health Information Portability Act (HIPA), may have a favorable impact on the biometrics industry. A good approach to piloting and gaining gradual acceptance of a biometrics solution could be to introduce it on a voluntary basis with either explicit or implicit incentives for opting biometrics-based solution.

Applications Flourish

Biometrics is a rapidly evolving technology that has been widely used in forensics, such as criminal identification and prison security. Biometric identification is also under serious consideration for adoption in a broad range of civilian applications. E-commerce and e-banking are two of the most important application areas due to the rapid progress in electronic transactions. These applications include electronic fund transfers, ATM security, check cashing, credit card security, smartcards security, and online transactions. There are currently several large biometric security projects in these areas under development, including credit card security (MasterCard) and smartcard security (IBM and American Express). A variety of biometric technologies are now competing to demonstrate their efficacy in these areas.

The market of physical access control is currently dominated by token-based technology. However, it is predicted that, with the progress in biometric technology, market share will increasingly shift to biometric techniques.

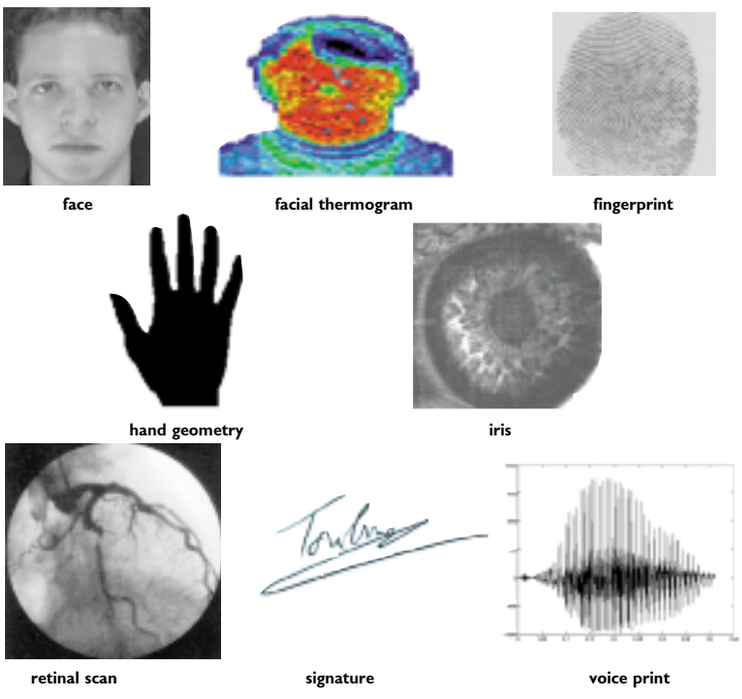
Information system and computer-network security, such as user authentication and access to databases via remote login is another potential application area. It is expected that more and more information systems and computer-networks will be secured with biometrics with the rapid expansion of Internet and intranet. With the introduction of biometrics, government benefits distribution programs such as welfare disbursements will experience substantial savings in deterring multiple claimants. In addition, customs and immigration initiatives such as INS Passenger Accelerated Service System (INSPASS), which permits faster processing of passengers at immigration checkpoints based on hand geometry, will greatly increase the operational efficiency. A biometric-based national identification system provides a unique ID to the citizens and integrates different government services. Biometrics-based voter registration prevents voter fraud; and biometrics-based driver registration enforces issuing only a single driver license to a person; and biometrics-based time/attendance monitoring systems prevent abuses of the current token-based manual systems.

Biometric Technologies

There are a multitude of biometric techniques either widely used or under investigation. These include,

facial imaging (both optical and infrared), hand and finger geometry, eye-based methods (iris and retina), signature, voice, vein geometry, keystroke, and finger- and palm-print imaging. Some of these methods are indicated in Figure 4.

Figure 4. Examples of different biometric characteristics.



THE AUTHORS ARE GRATEFUL TO EYEDENTIFY CORP., IRISCAN INC., AND MIKOS LTD. FOR PROVIDING THE PICTURES OF RETINA, SMARTCARD, IRIS, AND THERMOGRAM, RESPECTIVELY; FROM [5] USED WITH PERMISSION FROM KLUWER ACADEMIC PUBLISHING.

Face. Facial images are probably the most common biometric characteristic used by humans to make a personal identification. Identification based on face is one of the most active areas of research, with applications ranging from the static, controlled mug-shot verification to a dynamic, uncontrolled face identification in a cluttered background [2]. Approaches to face recognition are typically based on location and shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin shape and their spatial relationships; the overall (global) analysis of the face image and its break-down into a number of canonical faces, or a combination thereof.

While performance of the systems [1] commercially available is reasonable, it is questionable whether the face itself, without any contextual information, is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence. It is difficult to recognize a face from images captured from two drastically different views. Further, current face recognition systems impose a number of restrictions on how the facial images are obtained, sometimes requiring a simple background or special illumination. In order for the face recognition systems to be widely adopted, they should automatically detect whether a face is present in the acquired image; locate the face if there is one; and recognize the face from a general viewpoint.

Facial Thermogram. The underlying vascular system in the human face produces a unique facial signature when heat passes through the facial tissue and is emitted from the skin [11]. Such facial signatures can be captured using an infrared camera, resulting in an image called a "face thermogram." It is claimed that a face thermogram is unique to each individual and is not vulnerable to disguises. Even plastic surgery, which does not reroute the flow of blood through the veins, is believed to have no effect on the formation of the face thermogram. Face thermogram is a nonintrusive biometric technique which can verify an identity without contact. The claimed superiority of face thermogram-based recognition over visual face recognition using CCD cameras is based on the following observations: An infrared camera can capture the face thermogram in very low ambient light or in the absence of any light at all; the vascular structure may be more rich in information and remains invariant to intentional or unintentional variations in visual facial appearance [11].

Although it may be true that face thermograms are unique to each individual, it has not been proven that face thermograms are sufficiently discriminative. Face thermograms may depend heavily on a number of factors such as the emotional state of the subjects, or body temperature, and like face recognition, face thermogram recognition is view-dependent.

Fingerprints. Humans have used fingerprints for personal identification for centuries and the validity of fingerprint identification has been well-established [6]. A fingerprint is the pattern of ridges and furrows on the surface of a fingertip, the formation of which is determined during the fetal period. They are so distinct that even fingerprints of identical twins are different as are the prints on each finger of the same person.

With the development of solid-state sensors, the marginal cost of incorporating a fingerprint-based

biometric system may soon become affordable in many applications. Consequently, fingerprints are expected to lead the biometric applications in the near future, with multiple fingerprints providing sufficient information to allow for large-scale recognition involving millions of identities. One problem with fingerprint technology is its lack of acceptability by a typical user, because fingerprints have traditionally been associated with criminal investigations and police work. Another problem is that automatic fingerprint identification generally requires a large amount of computational resources. Finally, fingerprints of a small fraction of a population may be unsuitable for automatic identification because of genetic, aging, environmental, or occupational reasons.

Hand geometry. A variety of measurements of the human hand, including its shape, and lengths and widths of the fingers, can be used as biometric char-

A Case Study in Biometrics

Two primary components of a biometric-based identification system are the feature extractor and matcher. Here, we summarize typical steps involved in these two components for fingerprint-based authentication systems.

The unprocessed input gray values of the fingerprint images are not invariant over the time of capture and are susceptible to noise. Therefore, landmark features on a finger, for example, the fingerprint ridge endings and ridge bifurcations (collectively known as "minutiae"), are used in a fingerprint-based authentication system. The feature extraction system detects the minutiae from the input image through a series of image processing steps (see figure). The feature vector typically consists of a list of the locations and other attributes (for example, orientation of the ridge) of the minutiae detected in a fingerprint image.

A fingerprint matcher (see figures d, e, f) takes two feature vectors and determines whether the minutiae in the feature vectors originate from the same finger. The feature vectors cannot be directly compared from their original representations as the sensed fingers may be differently aligned with respect to the imaging system. The feature vectors are typically aligned based on some landmark information in the feature vector.

In figures d, e, f, the properties of the ridge associated with minutiae are used to align the feature vectors. Once the feature vectors are aligned and overlaid, the number of corresponding minutiae, that is, minutiae in close proximity to each other with similar attributes, constitutes a basis for quantifying the likelihood of fingerprint feature vectors originating from the same finger.

Steps in fingerprint-based identification: (a) input fingerprint image; (b) orientation estimation for input image; (c) thinned ridges for input image; (d) input minutiae set overlaid on the input image; (e) template minutiae set overlaid on the template fingerprint image; and (f) matching result where template minutiae and their correspondences are connected by red lines. Matching score for this pair of input and template fingerprints was 630. The maximum matching score is 1,000 and the minimum threshold score for a pair to be considered as a valid match for a typical application using this matcher is 150.

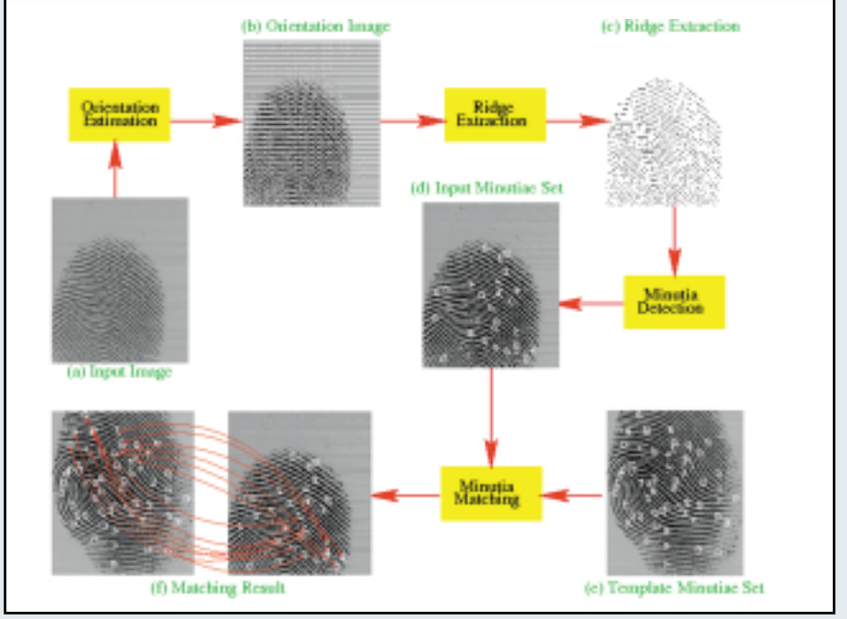


Table 2. Comparison of biometric technologies based on perceptions of three biometrics experts [5].

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	high	low	medium	high	low	high	low
Fingerprint	medium	high	high	medium	high	medium	high
Hand Geometry	medium	medium	medium	high	medium	medium	medium
Iris	high	high	high	medium	high	low	high
Retinal Scan	high	high	medium	low	high	low	high
Signature	low	low	low	high	low	high	low
Voice Print	medium	low	low	medium	low	high	low
F.Thermogram	high	high	low	high	medium	high	high

acteristics [9]. Hand geometry-based biometric systems have been installed at hundreds of locations around the world. The technique is very simple, relatively easy to use, and inexpensive. Operational environmental factors such as dry weather, or individual anomalies such as dry skin, generally have no negative effects on identification accuracy. A main disadvantage of this technique is its low discriminative capability. Hand geometry information may not be invariant over the lifespan of an individual, especially during childhood. In addition, an individual's jewelry or limitations in dexterity (for example, from arthritis), may pose further challenges in extracting the correct hand geometry information. Lastly, because the physical size of a hand geometry-based system is large, it cannot be used in certain applications such as laptop computers.

Retinal Pattern. The pattern formed by veins beneath the retinal surface in an eye is stable and unique [10] and is, therefore, an accurate and feasible characteristic for recognition. Digital images of retinal patterns can be acquired by projecting a low-intensity beam of visual or infrared light into the eye and capturing an image of the retina using optics similar to a retinascope. In order to acquire a fixed portion of the retinal vasculature needed for identification, the subject is required to closely gaze into an eye-piece and focus on a predetermined spot in the visual field. In many applications, the degree of user cooperation required in imaging a retina may not be acceptable to the subjects undergoing identification. Another disadvantage of this biometrics is that retinal scanners are expensive. A number of retinal scan-based biometric systems have been installed in several highly secure environments such as prisons.

Iris. The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual texture of the iris stabilizes during the first two years of life and its complex structure carries very distinctive information useful for identification of individuals. Initial available results on accuracy and speed of iris-based identification are promising and point to the feasibility of a large-scale recognition using iris information. Each iris is unique and even irises of identical twins are different. Furthermore, the iris is more readily imaged than retina; it is extremely difficult to surgically tamper iris texture information and it is easy to detect artificial irises (for example, designer contact lenses) [3]. Although the early iris-based identification systems required considerable user participation and were expensive, efforts are underway to build more user-friendly and cost-effective versions. It remains to be seen how this relatively recently discovered biometric matures and gains public acceptance.

Signature. Each person has a unique style of handwriting. However, no two signatures of a person are exactly identical; the variations from a typical signature also depend upon the physical and emotional state of a person. The identification accuracy of systems based on this highly behavioral biometric is reasonable but does not appear to be sufficiently high to lead to large-scale recognition. There are two approaches to identification based on signature [7]: static and dynamic. Static signature identification uses only the geometric (shape) features of a signature, whereas dynamic (online) signature identification uses both the geometric (shape) features and the dynamic features such as acceleration, velocity, pressure, and trajectory profiles of the signature. An inherent advantage of a signature-based biometric system is that the signature has been established as an acceptable form of personal identification method and can be incorporated transparently into the existing business processes requiring signatures such as credit card transactions.

Speech. Speech is a predominantly behavioral biometrics. The invariance in the individual characteristics of human speech is primarily due to relatively invariant shape/size of the appendages (vocal tracts, mouth, nasal cavities, lips) synthesizing the sound [4]. Speech of a person is distinctive but may not contain sufficient invariant information to offer large-scale recognition. Speech-based verification could be based on either a text-dependent or a text-independent speech input. A text-dependent verification authenticates the identity of an individual based on the utterance of a fixed predetermined phrase. A text-independent verification verifies the identity of a speaker independent of the phrase, which is more difficult than a text-dependent verification but offers more protection against fraud. Generally, people are willing to accept a speech-based biometric system. However, speech-based features are sensitive to a number of factors such as background noise as well as the emotional and physical state of the speaker. Speech-based authentication is currently restricted to low-security applications because of high variability in an individual's voice and poor accuracy performance of a typical speech-based authentication system.

Conclusions

Biometrics refers to automatic identification of a person based on his or her physiological or behavioral characteristics. It provides a better solution for the increased security requirements of our information society than traditional identification methods such as passwords and PINs. As biometric sensors become less expensive and miniaturized, and as the public realizes that biometrics is actually an effective strategy for protection of privacy and from fraud, this technology is likely to be used in almost every transaction needing authentication of personal identity. C

References

1. Biometrics Consortium homepage; www.biometrics.org.
2. Chellappa, R., Wilson, C., and Sirohey, A. Human and machine recognition of faces: A survey. In *Proceedings of the IEEE 83,* 5 (1995) 705–740.
3. Daugman, J.G. High confidence visual recognition of persons by a test of statistical independence. *IEEE Trans. Pattern Anal. and Machine Intell. 15,* 11 (1993)1148–1161.
4. Furui, S. Recent advances in speaker recognition. *Pattern Recognition Letters 18* (1997) 859–872.
5. Jain, A.K. Bolle, R. and Pankanti S. (eds.). *Biometrics: Personal Identification in Networked Society.* Kluwer, New York, 1999.
6. Jain, A.K., Hong, L., Pankanti, S., and Bolle, R. An identity-authentication system using fingerprints. In *Proceedings of the IEEE 85,* 9 (1997), 1365–1388.
7. Nalwa, V. Automatic on-line signature verification. In *Proceedings of the IEEE 85,* 2 (1997), 213–239.
8. Miller, B. Vital signs of identity. *IEEE Spectrum 31*, 2 (1994), 22–30.
9. Sidlauskas, D.R. 3D hand profile identification apparatus. U.S. Patent No. 4736203, 1988.
10. Hill, R.B. Apparatus and method for identifying individuals through their retinal vasculature patterns. US Patent No. 4109237, 1978.
11. Prokoski, F.K. Disguise detection and identification using infrared imagery. In the *Proceedings of SPIE, Optics, and Images in Law Enforcement II*. A.S. Hecht, Ed. (Arlington, VA, May, 1982), 27–31.
12. Wayman, J.L. Error Rate Equations for the General Biometric System. I*EEE Robotics & Automation 6,* 9 (Jan. 1999), 35–48.

Anil Jain (Jain@cse.msu.edu) is a University Distinguished Professor at the Department of Computer Science and Engineering at Michigan State University.
Lin Hong (lin@faceit.com) is a research staff member at Visionics Corp., Jersey City, NJ.
Sharath Pankanti (sharat@us.ibm.com) is a research staff member at IBM T. J. Watson Research Center, Hawthorne, NY.