An Introduction to Biometric Recognition

Anil K. Jain, *Fellow, IEEE*, Arun Ross, *Member, IEEE*, and Salil Prabhakar, *Member, IEEE*

Invited Paper

***Abstract*—A wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones, and ATMs. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor. Biometric recognition or, simply, biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. By using biometrics, it is possible to confirm or establish an individual's identity based on "who she is," rather than by "what she possesses" (e.g., an ID card) or "what she remembers" (e.g., a password). In this paper, we give a brief overview of the field of biometrics and summarize some of its advantages, disadvantages, strengths, limitations, and related privacy concerns.**

***Index Terms*—Biometrics, identification, multimodal biometrics, recognition, verification.**

I. Introduction

HUMANS have used body characteristics such as face, voice, and gait for thousands of years to recognize each other. Alphonse Bertillon, chief of the criminal identification division of the police department in Paris, developed and then practiced the idea of using a number of body measurements to identify criminals in the mid-19th century. Just as his idea was gaining popularity, it was obscured by a far more significant and practical discovery of the distinctiveness of the human fingerprints in the late 19th century. Soon after this discovery, many major law enforcement departments embraced the idea of first "booking" the fingerprints of criminals and storing it in a database (actually, a card file). Later, the leftover (typically, fragmentary) fingerprints (commonly referred to as *latents*) at the scene of crime could be "lifted" and matched with fingerprints in the database to determine the identity of the criminals. Although biometrics emerged from its extensive use in law enforcement to identify criminals (e.g., illegal aliens, security clearance for employees for sensitive jobs, fatherhood determination, forensics, and positive identification of convicts and prisoners), it is being increasingly used today to establish person recognition in a large number of civilian applications.

What biological measurements qualify to be a biometric? Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

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

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

- *performance*, which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed;
- *acceptability*, which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;
- *circumvention*, which reflects how easily the system can be fooled using fraudulent methods.

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

II. Biometric Systems

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

- In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored in the system database.

Manuscript received January 30, 2003; revised May 13, 2003. This paper was previously published in part in the *IEEE Security Privacy Magazine* and the *Handbook of Fingerprint Recognition*.

A. K. Jain is with the Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824 USA (e-mail: jain@cse.msu.edu).

A. Ross is with the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV 26506 USA (e-mail: ross@csee.wvu.edu).

S. Prabhakar is with the Algorithms Research Group, DigitalPersona Inc., Redwood City, CA 94063 USA (e-mail: salilp@digitalpersona.com).

Digital Object Identifier 10.1109/TCSVT.2003.818349

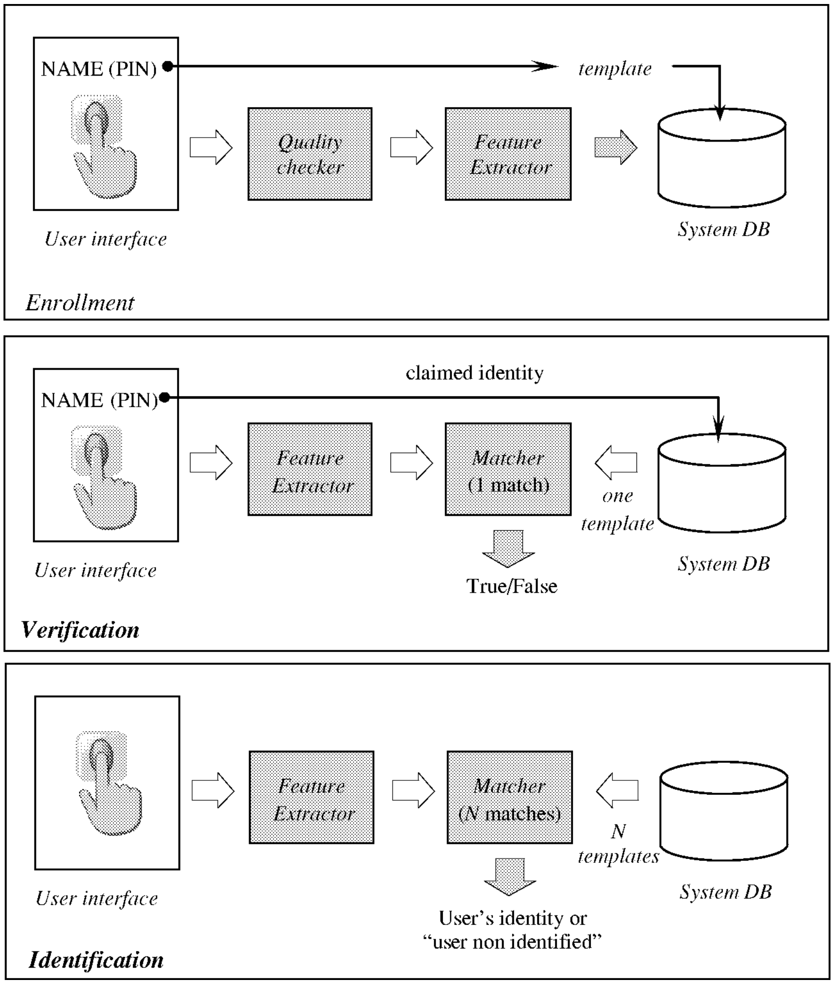

Fig. 1. Block diagrams of enrollment, verification, and identification tasks are shown using the four main modules of a biometric system, i.e., sensor, feature extraction, matcher, and system database.

In such a system, an individual who desires to be recognized claims an identity, usually via a personal identification number (PIN), a user name, or a smart card, and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., "*Does this biometric data belong to Bob?*"). Identity verification is typically used for *positive recognition*, where the aim is to prevent multiple people from using the same identity [26].

- In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., "*Whose biometric data is this?*"). Identification is a critical component in *negative recognition* applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities [26]. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.

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

The verification problem may be formally posed as follows: given an input feature vector X_Q (extracted from the biometric data) and a claimed identity I, determine if (I, X_Q) belongs to class w_1 or w_2, where w_1 indicates that the claim is true (a genuine user) and w_2 indicates that the claim is false (an impostor). Typically, X_Q is matched against X_I, the biometric template corresponding to user I, to determine its category. Thus

$$(I, X_Q) \in \begin{cases} w_1, & \text{if } S(X_Q, X_1) \geq t \\ w_2, & \text{otherwise} \end{cases}$$

where S is the function that measures the similarity between feature vectors X_Q and X_I, and t is a predefined *threshold*. The value $S(X_Q, X_I)$ is termed as a similarity or *matching score* between the biometric measurements of the user and the claimed identity. Therefore, every claimed identity is classified into w_1

or w_2 based on the variables X_Q, I, X_I, and t and the function S. Note that biometric measurements (e.g., fingerprints) of the same individual taken at different times are almost never identical. This is the reason for introducing the threshold t.

The identification problem, on the other hand, may be stated as follows. Given an input feature vector X_Q, determine the identity $I_k, k \in \{1, 2, \ldots, N, N+1\}$. Here $I_1, I_2, \ldots, I_N$ are the identities enrolled in the system and I_{N+1} indicates the reject case where no suitable identity can be determined for the user. Hence

$$X_Q \in \begin{cases} I_k, & \text{if } \max_k\{S(X_Q, X_{Ik})\} \geq t, k = 1, 2, \ldots, N \\ I_{N+1}, & \text{otherwise} \end{cases}$$

where X_{I_k} is the biometric template corresponding to identity I_k, and t is a predefined threshold.

A biometric system is designed using the following four main modules (see Fig. 1).

1) Sensor module, which captures the biometric data of an individual. An example is a fingerprint sensor that images the ridge and valley structure of a user's finger.
2) Feature extraction module, in which the acquired biometric data is processed to extract a set of salient or discriminatory features. For example, the position and orientation of minutiae points (local ridge and valley singularities) in a fingerprint image are extracted in the feature extraction module of a fingerprint-based biometric system.
3) Matcher module, in which the features extracted during recognition are compared against the stored templates to generate matching scores. For example, in the matching module of a fingerprint-based biometric system, the number of matching minutiae between the input and the template fingerprint images is determined and a matching score is reported. The matcher module also encapsulates a decision making module, in which a user's claimed identity is confirmed (verification) or a user's identity is established (identification) based on the matching score.
4) System database module, which is used by the biometric system to store the biometric templates of the enrolled users. The enrollment module is responsible for enrolling individuals into the biometric system database. During the enrollment phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a digital representation of the characteristic. The data capture during the enrollment process may or may not be supervised by a human depending on the application. A quality check is generally performed to ensure that the acquired sample can be reliably processed by successive stages. In order to facilitate matching, the input digital representation is further processed by a feature extractor to generate a compact but expressive representation, 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 *smart card* issued to the individual. Usually, multiple templates of an individual are stored to account for variations observed in the biometric trait and the templates in the database may be updated over time.

III. Biometric System Errors

Two samples of the same biometric characteristic from the same person (e.g., two impressions of a user's right index finger) are not exactly the same due to imperfect imaging conditions (e.g., sensor noise and dry fingers), changes in the user's physiological or behavioral characteristics (e.g., cuts and bruises on the finger), ambient conditions (e.g., temperature and humidity), and user's interaction with the sensor (e.g., finger placement). Therefore, the response of a biometric matching system is the matching score $S(X_Q, X_I)$ (typically a single number) that quantifies the similarity between the input (X_Q) and the template (X_I) representations. The higher the score, the more certain is the system that the two biometric measurements come from the same person. The system decision is regulated by the threshold t: pairs of biometric samples generating scores higher than or equal to t are inferred as *mate pairs* (i.e., belonging to the same person); pairs of biometric samples generating scores lower than t are inferred as *nonmate pairs* (i.e., belonging to different persons). The distribution of scores generated from pairs of samples from the same person is called the *genuine distribution* and from different persons is called the *impostor* distribution [see Fig. 2(a)].

A biometric verification system makes two types of errors: 1) mistaking biometric measurements from two different persons to be from the same person (called *false match*) and 2) mistaking two biometric measurements from the same person to be from two different persons (called *false nonmatch*). These two types of errors are often termed as *false accept* and *false reject*, respectively. There is a tradeoff between false match rate (FMR) and false nonmatch rate (FNMR) in every biometric system. In fact, both FMR and FNMR are functions of the system threshold t; if t is decreased to make the system more tolerant to input variations and noise, then FMR increases. On the other hand, if t is raised to make the system more secure, then FNMR increases accordingly. The system performance at all the operating points (thresholds t) can be depicted in the form of a *receiver operating characteristic* (ROC) curve. A ROC curve is a plot of FMR against (1-FNMR) or FNMR for various threshold values t [see Fig. 2(b)].

Mathematically, the errors in a verification system can be formulated as follows. If the stored biometric template of the user I is represented by X_I and the acquired input for recognition is represented by X_Q, then the null and alternate hypotheses are:

H_0 input X_Q does not come from the same person as the template X_I;

H_1 input X_Q comes from the same person as the template X_I.

The associated decisions are as follows:

D_0 person is not who she claims to be;

D_1 person is who she claims to be.

The decision rule is as follows. If the matching score $S(X_Q, X_I)$ is less than the system threshold t, then decide D_0, else decide D_1. The above terminology is borrowed from communication theory, where the goal is to detect a message in the presence of noise. H_0 is the hypothesis that the received signal is noise alone, and H_1 is the hypothesis that the received

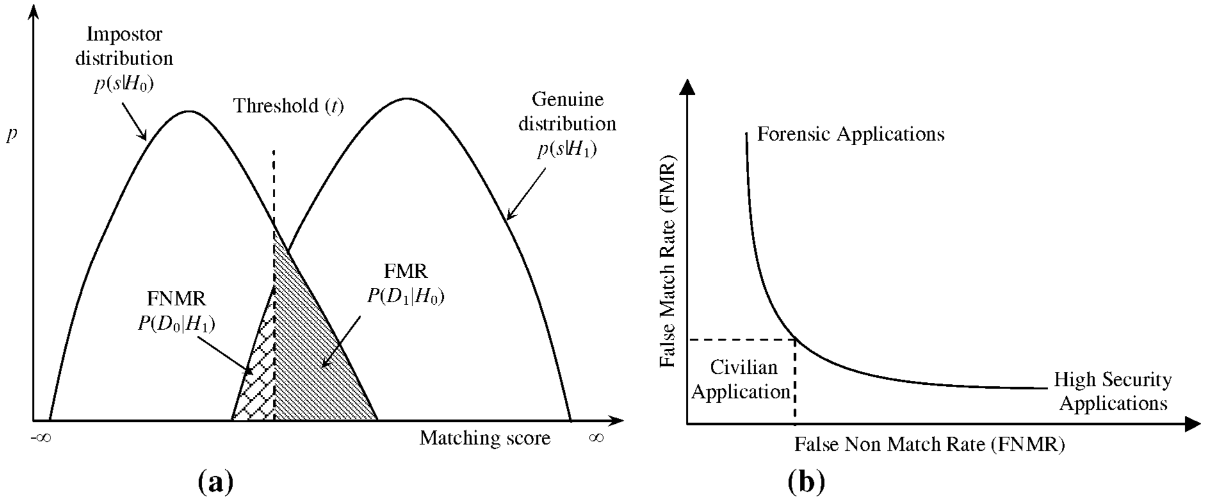

Fig. 2. Biometric system error rates. (a) FMR and FNMR for a given threshold t are displayed over the genuine and impostor score distributions; FMR is the percentage of nonmate pairs whose matching scores are greater than or equal to t, and FNMR is the percentage of mate pairs whose matching scores are less than t. (b) Choosing different operating points results in different FMR and FNMR. The curve relating FMR to FNMR at different thresholds is referred to as receiver operating characteristics (ROC). Typical operating points of different biometric applications are displayed on an ROC curve. Lack of understanding of the error rates is a primary source of confusion in assessing system accuracy in vendor/user communities alike.

signal is message plus the noise. Such a hypothesis testing formulation inherently contains two types of errors.

Type I: false match (D_1 is decided when H_0 is true);

Type II: false nonmatch (D_0 is decided when H_1 is true).

FMR is the probability of type-I error (also called significance level in hypothesis testing) and FNMR is the probability of type-II error as

$$\begin{aligned}\mathrm{FMR} &= P(D_1|H_0)\\ \mathrm{FNMR} &= P(D_0|H_1).\end{aligned}$$

The expression (1-FNMR) is also called the power of the hypothesis test. To evaluate the accuracy of a fingerprint biometric system, one must collect scores generated from multiple images of the same finger (the distribution $p(S(X_Q, X_I)|H_1)$), and scores generated from a number of images from different fingers (the distribution $p(S(X_Q, X_I)|H_0)$). Fig. 2(a) graphically illustrates the computation of FMR and FNMR over genuine and impostor distributions

$$\mathrm{FMR} = \int_t^{\infty} p\left(S(X_Q, X_I)|H_0\right) dS$$

$$\mathrm{FNMR} = \int_{-\infty}^{\mathrm{t}} p\left(S(X_Q, X_I)|H_1\right) dS.$$

Besides the above error rates, the failure to capture (FTC) rate and the failure to enroll (FTE) rate are also used to summarize the accuracy of a biometric system. The FTC rate is only applicable when the biometric device has an automatic capture functionality implemented in it and denotes the percentage of times the biometric device fails to capture a sample when the biometric characteristic is presented to it. This type of error typically occurs when the device is not able to locate a biometric signal of sufficient quality (e.g., an extremely faint fingerprint or an occluded face). The FTE rate, on the other hand, denotes the percentage of times users are not able to enroll in the recognition system. There is a tradeoff between the FTE rate and the perceived system accuracy (FMR and FNMR). FTE errors typically occur when the system rejects poor quality inputs during enrollment. Consequently, the database contains only good quality templates and the perceived system accuracy improves. Because of the interdependence among the failure rates and error rates, all these rates (i.e., FTE, FTC, FNMR, FMR) constitute important specifications in a biometric system, and should be reported during performance evaluation.

The accuracy of a biometric system in the identification mode can be inferred using the system accuracy in the verification mode under simplifying assumptions. Let us denote the identification false nonmatch and false match rates with FNMR_N and FMR_N, respectively, where N represents the number of identities in the system database (for simplicity, we assume that only a single identification attempt is made per subject, a single biometric template is used for each enrolled user, and the impostor scores between different users are uncorrelated). Then, $\mathrm{FNMR}_N \cong \mathrm{FNMR}$ and $\mathrm{FMR}_N = 1 - (1 - \mathrm{FMR})^N \cong N \cdot \mathrm{FMR}$ (the approximations hold good only when $N \cdot \mathrm{FMR} < 0.1$). A detailed discussion on these issues is available in [25] and [27].

If the templates in the database of an identification system have been classified and indexed, then only a portion of the database is searched during identification and this leads to the following formulation of FNMR_N and FMR_N.

- $\mathrm{FNMR}_N = \mathrm{RER} + (1 - \mathrm{RER}) \cdot \mathrm{FNMR}$, where RER (retrieval error rate) is the probability that the database template corresponding to the searched finger is wrongly discarded by the retrieval mechanism. The above expression is obtained using the following argument: in case the template is not correctly retrieved (this happens with probability RER), the system always generates a false-non match, whereas in case the retrieval returns the right template [this happens with probability (1-RER)], false nonmatch rate of the system is FNMR. Also, this expression is

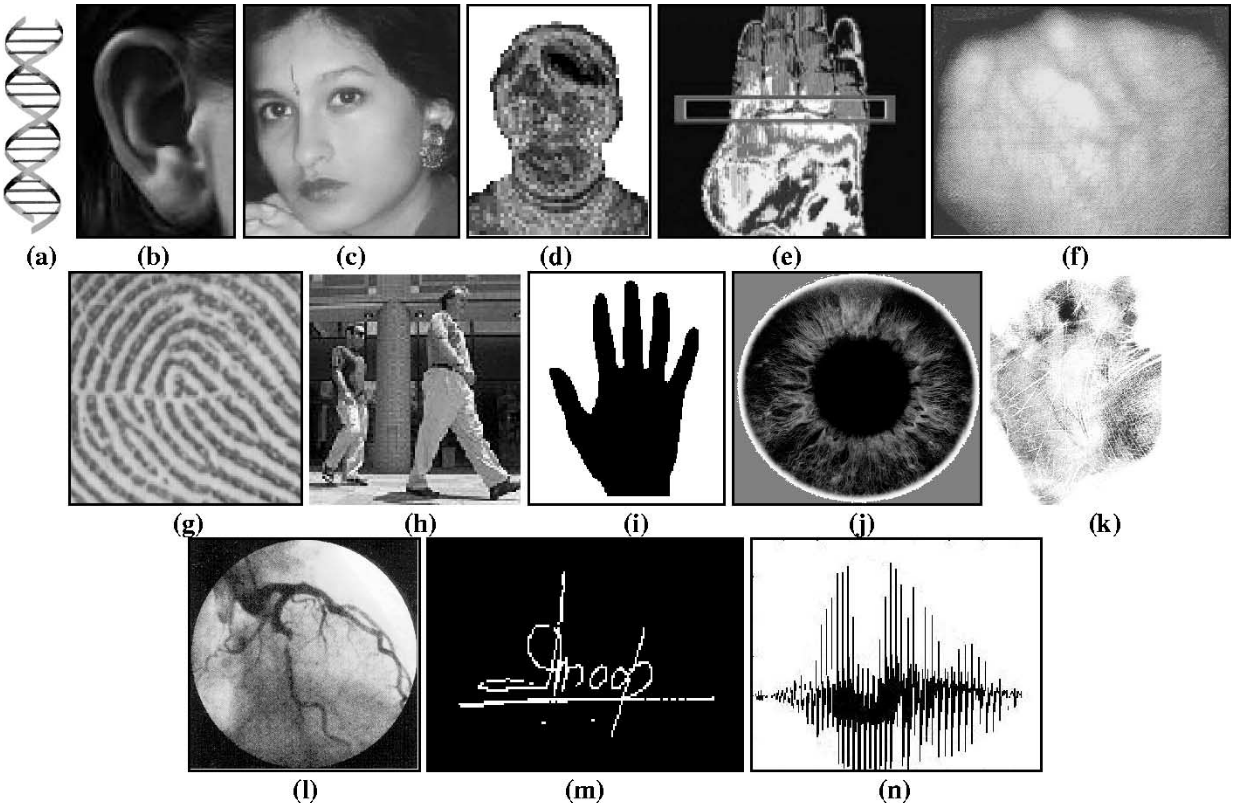

Fig. 3. Examples of biometric characteristics: (a) DNA, (b) ear, (c) face, (d) facial thermogram, (e) hand thermogram, (f) hand vein, (g) fingerprint, (h) gait, (i) hand geometry, (j) iris, (k) palmprint, (l) retina, (m) signature, and (n) voice.

only an approximation since it does not consider the probability of falsely matching an incorrect template before the right one is retrieved [28].

- $\mathrm{FMR}_N = 1 - (1 - \mathrm{FMR})^{N \cdot P}$, where P (also called the *penetration rate*) is the average percentage of database searched during the identification of an input fingerprint.

The accuracy requirements of a biometric system are very much application-dependent. For example, in some forensic applications such as criminal identification, one of the critical design issues is the FNMR rate (and not the FMR), i.e., we do not want to miss identifying a criminal even at the risk of manually examining a large number of potentially incorrect matches generated by the biometric system. On the other extreme, the FMR may be one of the most important factors in a highly secure access control application, where the primary objective is deterring impostors (although we are concerned with the possible inconvenience to the legitimate users due to a high FNMR). There are a number of civilian applications whose performance requirements lie in between these two extremes, where both FMR and FNMR need to be considered. For example, in applications like bank ATM card verification, a false match means a loss of several hundred dollars while a high FNMR may lead to a potential loss of a valued customer. Fig. 2(b) depicts the FMR and FNMR tradeoffs in different types of biometric applications.

IV. Comparison of Various Biometrics

A number of biometric characteristics exist and are in use in various applications (see Fig. 3). Each biometric has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet the requirements of all the applications. In other words, no biometric is "optimal." The match between a specific biometric and an application is determined depending upon the operational mode of the application and the properties of the biometric characteristic. A brief introduction to the commonly used biometrics is given below.

- **DNA**: Deoxyribonucleic acid (DNA) is the one-dimensional (1–D) ultimate unique code for one's individuality—except for the fact that identical twins have identical DNA patterns. It is, however, currently used mostly in the context of forensic applications for person recognition. Three issues limit the utility of this biometrics for other applications: 1) contamination and sensitivity: it is easy to steal a piece of DNA from an unsuspecting subject that can be subsequently abused for an ulterior purpose; 2) automatic real-time recognition issues: the present technology for DNA matching requires cumbersome chemical methods (wet processes) involving an expert's skills and is not geared for on-line noninvasive recognition; and 3) privacy issues: information about susceptibilities of a person to certain diseases could be gained from the DNA pattern and there is a concern that the unintended abuse of genetic code information may result in discrimination, e.g., in hiring practices.
- **Ear**: It has been suggested that the shape of the ear and the structure of the cartilegenous tissue of the pinna are distinctive. The ear recognition approaches are based on

matching the distance of salient points on the pinna from a landmark location on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual.

- **Face**: Face recognition is a nonintrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The applications of facial recognition range from a static, controlled "mug-shot" verification to a dynamic, uncontrolled face identification in a cluttered background (e.g., airport). The most popular approaches to face recognition are based on either: 1) the location and shape of facial attributes such as the eyes, eyebrows, nose, lips and chin, and their spatial relationships, or 2) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. While the verification performance of the face recognition systems that are commercially available is reasonable [34], they impose a number of restrictions on how the facial images are obtained, sometimes requiring a fixed and simple background or special illumination. These systems also have difficulty in recognizing a face from images captured from two drastically different views and under different illumination conditions. 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 [29]. In order for a facial recognition system to work well in practice, it should automatically: 1) detect whether a face is present in the acquired image; 2) locate the face if there is one; and 3) recognize the face from a general viewpoint (i.e., from any pose).
- **Facial, hand, and hand vein infrared thermogram**: The pattern of heat radiated by human body is a characteristic of an individual and can be captured by an infrared camera in an unobtrusive way much like a regular (visible spectrum) photograph. The technology could be used for covert recognition. A thermogram-based system does not require contact and is noninvasive, but image acquisition is challenging in uncontrolled environments, where heat emanating surfaces (e.g., room heaters and vehicle exhaust pipes) are present in the vicinity of the body. A related technology using near infrared imaging is used to scan the back of a clenched fist to determine hand vein structure. Infrared sensors are prohibitively expensive which is a factor inhibiting wide spread use of the thermograms.
- **Fingerprint**: Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high [25]. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person. Today, a fingerprint scanner costs about U.S. $20 when ordered in large quantities and the marginal cost of embedding a fingerprint-based biometric in a system (e.g., laptop computer) has become affordable in a large number of applications. The accuracy of the currently available fingerprint recognition systems is adequate for verification systems and small- to medium-scale identification systems involving a few hundred users. Multiple fingerprints of a person provide additional information to allow for large-scale recognition involving millions of identities. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources, especially when operating in the identification mode. Finally, fingerprints of a small fraction of the population may be unsuitable for automatic identification because of genetic factors, aging, environmental, or occupational reasons (e.g., manual workers may have a large number of cuts and bruises on their fingerprints that keep changing).
- **Gait**: Gait is the peculiar way one walks and is a complex spatio-temporal biometric. Gait is not supposed to be very distinctive, but is sufficiently discriminatory to allow verification in some low-security applications. Gait is a behavioral biometric and may not remain invariant, especially over a long period of time, due to fluctuations in body weight, major injuries involving joints or brain, or due to inebriety. Acquisition of gait is similar to acquiring a facial picture and, hence, may be an acceptable biometric. Since gait-based systems use the video-sequence footage of a walking person to measure several different movements of each articulate joint, it is input intensive and computationally expensive.
- **Hand and finger geometry**: Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers. Commercial hand geometry-based verification systems have been installed in hundreds of locations around the world. The technique is very simple, relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems. The geometry of the hand is not known to be very distinctive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population. Further, hand geometry information may not be invariant during the growth period of children. In addition, an individual's jewelry (e.g., rings) or limitations in dexterity (e.g., from arthritis), may pose further challenges in extracting the correct hand geometry information. The physical size of a hand geometry-based system is large, and it cannot be embedded in certain devices like laptops. There are verification systems available that are based on measurements of only a few fingers (typically, index and middle) instead of the entire hand. These devices are smaller than those used for hand geometry, but still much larger than those used in some other biometrics (e.g., fingerprint, face, voice).
- **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 is formed during fetal development and stabilizes during the first two years of life. The

complex iris texture carries very distinctive information useful for personal recognition. The accuracy and speed of currently deployed iris-based recognition systems is promising and point to the feasibility of large-scale identification systems based on iris information. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different. It is extremely difficult to surgically tamper the texture of the iris. Further, it is rather easy to detect artificial irises (e.g., designer contact lenses). Although, the early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more user-friendly and cost-effective.

- **Keystroke**: It is hypothesized that each person types on a keyboard in a characteristic way. This behavioral biometric is not expected to be unique to each individual but it offers sufficient discriminatory information to permit identity verification. Keystroke dynamics is a behavioral biometric; for some individuals, one may expect to observe large variations in typical typing patterns. Further, the keystrokes of a person using a system could be monitored unobtrusively as that person is keying in information.
- **Odor**: It is known that each object exudes an odor that is characteristic of its chemical composition and this could be used for distinguishing various objects. A whiff of air surrounding an object is blown over an array of chemical sensors, each sensitive to a certain group of (aromatic) compounds. A component of the odor emitted by a human (or any animal) body is distinctive to a particular individual. It is not clear if the invariance in the body odor could be detected despite deodorant smells, and varying chemical composition of the surrounding environment.
- **Palmprint**: The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and, as a result, palmprints are expected to be even more distinctive than the fingerprints. Since palmprint scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper [32]. Finally, when using a high-resolution palmprint scanner, all the features of the palm such as hand geometry, ridge and valley features (e.g., minutiae and singular points such as deltas), principal lines, and wrinkles may be combined to build a highly accurate biometric system.
- **Retinal scan**: The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most secure biometric since it is not easy to change or replicate the retinal vasculature. The image acquisition requires a person to peep into an eye-piece and focus on a specific spot in the visual field so that a predetermined part of the retinal vasculature could be imaged. The image acquisition involves cooperation of the subject, entails contact with the eyepiece, and requires a conscious effort on the part of the user. All these factors adversely affect the public acceptability of retinal biometric. Retinal vasculature can reveal some medical conditions, e.g., hypertension, which is another factor deterring the public acceptance of retinal scan-based biometrics.
- **Signature**: The way a person signs his or her name is known to be a characteristic of that individual. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of verification. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories. Signatures of some people vary substantially: even successive impressions of their signature are significantly different. Further, professional forgers may be able to reproduce signatures that fool the system.
- **Voice**: Voice is a combination of physiological and behavioral biometrics. The features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound. These physiological characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions (such as a common cold), and emotional state, etc. Voice is also not very distinctive and may not be appropriate for large-scale identification. A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase. A text-independent voice recognition system recognizes the speaker independent of what she speaks. A text-independent system is more difficult to design than a text-dependent system but offers more protection against fraud. A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise. Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the microphone and the communication channel.

A brief comparison of the above biometric techniques based on seven factors is provided in Table I. The applicability of a specific biometric technique depends heavily on the requirements of the application domain. No single technique can outperform all the others in all operational environments. In this sense, each biometric technique is admissible and there is no optimal biometric characteristic. For example, it is well known that both the fingerprint-based and iris-based techniques are more accurate than the voice-based technique. However, in a tele-banking application, the voice-based technique may be preferred since it can be integrated seamlessly into the existing telephone system.

V. Applications of Biometric Systems

The applications of biometrics can be divided into the following three main groups.

- **Commercial** applications such as computer network login, electronic data security, e-commerce, Internet

TABLE I
COMPARISON OF VARIOUS BIOMETRIC TECHNOLOGIES BASED ON THE PERCEPTION OF THE AUTHORS. HIGH, MEDIUM, AND LOW ARE DENOTED BY H, M, AND L, RESPECTIVELY

Biometric identifier	**Universality**	**Distinctiveness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Circumvention**
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, and distance learning.

- **Government** applications such as national ID card, correctional facility, driver's license, social security, welfare-disbursement, border control, and passport control.
- **Forensic** applications such as corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children.

Traditionally, commercial applications have used knowledge-based systems (e.g., PINs and passwords), government applications have used token-based systems (e.g., ID cards and badges), and forensic applications have relied on human experts to match biometric features. Biometric systems are being increasingly deployed in large-scale civilian applications (see Fig. 4). The Schiphol Privium scheme at the Amsterdam airport, for example, employs iris scan cards to speed up the passport and visa control procedures [4]. Passengers enrolled in this scheme insert their card at the gate and look into a camera; the camera acquires the image of the traveler's eye and processes it to locate the iris and compute the Iriscode [5]; the computed Iriscode is compared with the data residing in the card to complete user verification. A similar scheme is also being used to verify the identity of Schiphol airport employees working in high-security areas. Thus, biometric systems can be used to enhance user convenience while improving security.

VI. ADVANTAGES AND DISADVANTAGES OF BIOMETRICS

Let us now examine the advantages and disadvantages of biometrics in two groups of applications: the commercial positive recognition applications that may work either in the verification or the identification modes and the government and forensic negative recognition applications that require identification.

A. *Positive Recognition in Commercial Applications*

The traditional technologies available to achieve a positive recognition include knowledge-based methods (e.g., PINs and passwords) and token-based methods (e.g., keys and cards). Most people set their passwords based on words or digits that they can easily remember, such as names and birthdays of family members, favorite movie or music stars, and dictionary words (a survey of 1200 British office workers in year 2001 found that almost half chose their own name, the name of a pet, or that of a family member as a password; others based their passwords on the names such as Darth Vader and Homer Simpson). Such passwords are easy to crack by guessing or by a simple brute force dictionary attack. Although it is possible, and even advisable, to keep different passwords for different applications and change them frequently, most people use the same password across different applications and never change them. If a single password is compromised, it may result in a breach in security in many applications. For example, a hacker may create a bogus web site that entices users with free air miles if they were to register on the website with a login name and password. The hacker may then try to use the same login name and password to attack the users' corporate accounts, and most likely succeed. Longer passwords are more secure but harder to remember which prompts some users to write them down in accessible locations (e.g., on a "Post-it" note) and hide it under the keyboard. Strong passwords are difficult to remember and result in more help desk calls for forgotten or expired passwords. Cryptographic techniques such as encryption can provide very long passwords (encryption keys) that are not required to be remembered but that are in turn protected by simple passwords, thus defeating their purpose. Further, a hacker needs to break only one password among all the employees to gain access to a company's Intranet and thus, a single weak password compromises the overall

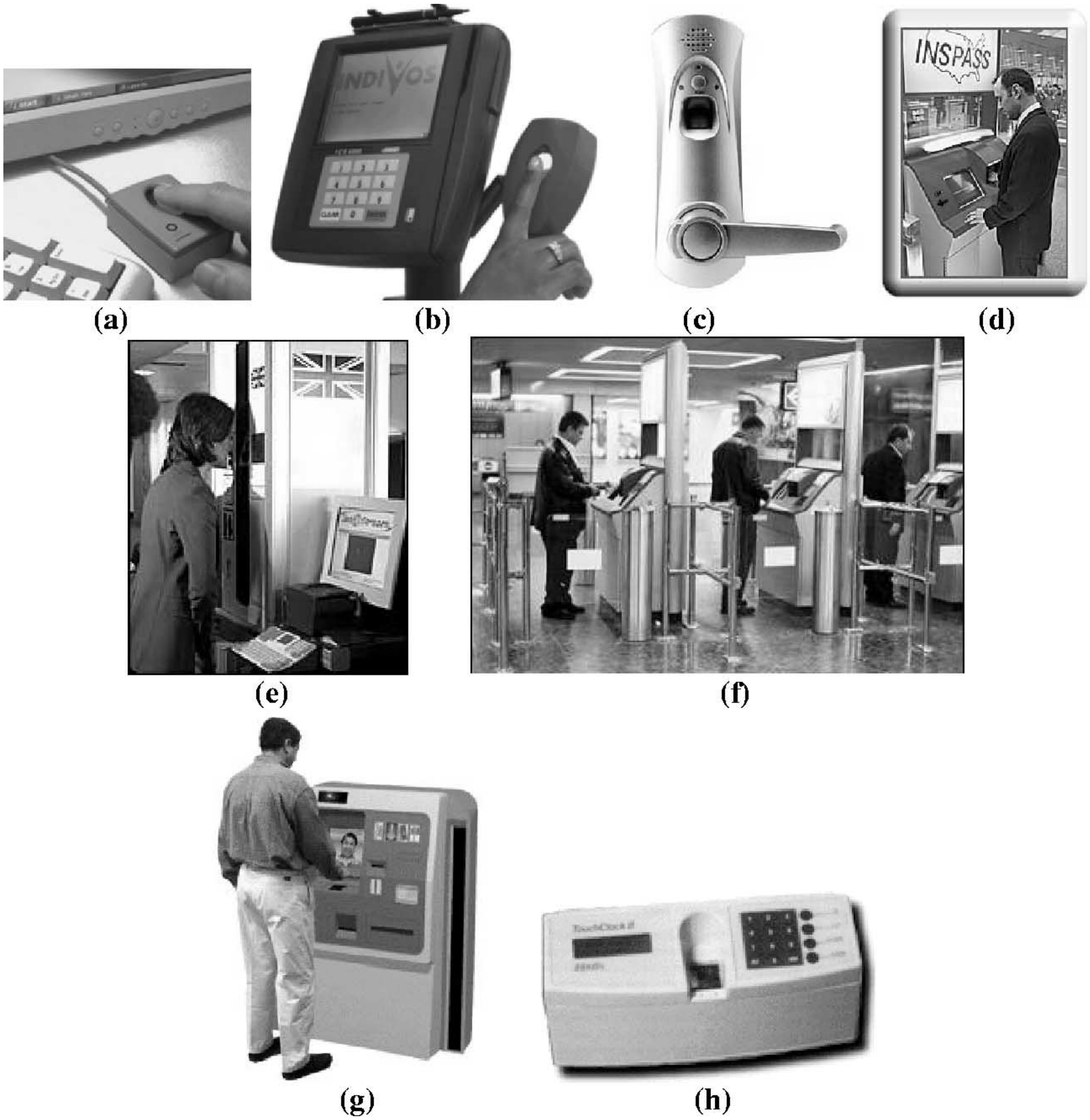

Fig. 4. Examples of biometric application. (a) Fingerprint verification system manufactured by Digital Persona, Inc., is used for computer and network login. (b) Fingerprint-based point of sale (POS) terminal manufactured by Indivos, Inc., that verifies the customers before charging their credit cards and speeds up payment in retail shops, restaurants and cafeterias. (c) Fingerprint-based door lock manufactured by BioThentica Corporation used to restrict access to premises is shown. (d) Immigration and naturalization service accelerated service system (INSPASS), which is installed at major airports in the U.S., is based on hand geometry verification technology developed by Recognition Systems, Inc., and significantly reduces the immigration processing time. (e) Border passage system using iris recognition at London's Heathrow airport. (f) Ben Gurion airport in Tel Aviv (Israel) uses Express Card entry kiosks fitted with hand geometry systems for security and immigration. (g) The FacePass system from Viisage is used in POS verification applications like ATMs, therefore obviating the need for PINs. (h) The Identix TouchClock fingerprint system is used in time and attendance applications.

security of every system that the user has access to. Thus, the security of the entire system is only as good as the weakest password. Finally, when a password is shared with a colleague, there is no way for the system to know who the actual user is. Similarly, there are many problems with possession-based personal recognition. For example, keys and tokens can be shared, duplicated, lost or stolen and an attacker may make a "master" key that may open many locks. It is significantly more difficult to copy, share, and distribute biometrics with as much ease as passwords and tokens. Biometrics cannot be lost or forgotten and online biometrics-based recognition systems require the person to be recognized to be present at the point of recognition. It is difficult to forge biometrics and extremely unlikely for a user to repudiate, for example, having accessed a computer network. Further, all the users of the system have relatively equal security level and one account is no easier to break than any other (e.g., through social engineering methods). Biometrics introduces incredible convenience for the users (as users are no longer required to remember multiple, long and complex frequently changing passwords) while maintaining a sufficiently high degree of security.

Let us now consider a brute force attack on a biometric system operating in a verification mode in a commercial application. The chance of success of a brute force attack depends on the matching accuracy of the biometric verification. Let us assume that a certain commercial biometric verification system wishes to operate at 0.001% FMR. At this setting, several biometric systems (e.g., the state-of-the-art fingerprint and iris recognition systems) can easily deliver less than 1% FNMR [3]. A FMR of 0.001% indicates that, if a hacker launches a brute force attack with a large number of different fingerprints, 1 out of 100 000 attempts will succeed on an average. This may be considered equivalent to the security offered by a randomly chosen five-digit PIN (although a brute force attack against a five-digit PIN is *guaranteed* to succeed in 100 000 attempts and requires only 50 000 attempts, on an average). To attack a biometric-based system, one needs to generate (or acquire) a large number of samples of that biometric (e.g., fingerprints), which is much more difficult than generating a large number of PINs/passwords. Finally, the FMR of a biometric system can be arbitrarily reduced for higher security at the cost of increased inconvenience to the users that results from a higher FNMR. Note that a longer PIN or password also increases the security while causing more inconvenience in remembering and correctly typing them.

Certain commercial applications would like to operate the biometric system in an identification mode instead of the verification mode for the added convenience of not requiring the users to claim an identity. Usually, speed is perceived as the biggest problem in scaling up an identification application. However, the fact is that the identification accuracy scales even worse than the speed. Consider an identification application with 10 000 users. We can certainly find a combination of a fast fingerprint matching algorithm and special purpose hardware capable of making an identification in a few seconds. On the other hand, a matching algorithm with a verification FMR of 0.001% will have an identification FMR_N of 10,000 $\times$ 0.001% $=$ 10%! This implies that an impostor has a good chance of gaining access to the system by simply using all of the ten fingers on her two hands. Therefore, while small- to medium-scale commercial applications (e.g., a few hundred users) may still use single biometric identification, the only obvious solution for building a highly accurate identification system for large scale applications appears to be *multimodal biometric* systems (see Section VIII). For example, a system may combine face and fingerprint of a person or fingerprints from multiple fingers of a person for recognition.

Finally, in commercial applications, addition or replacement of existing personal recognition methods with biometrics-based solutions should be based on a cost-benefit analysis. For example, is the installation and maintenance cost of a biometric-based computer login system less than the currently used password system? Note that, according to the Gartner Group, between 20% and 50% of all help desk calls are for password resets. Forrester Research states that the average help desk labor cost for a single password reset is about US $38.

B. Negative Recognition in Government and Forensic Applications

In negative recognition applications such as employee background checking and preventing terrorists from boarding airplanes, the personal recognition is required to be performed in the identification mode. As mentioned earlier, achieving the same accuracy in an identification system as in a verification system is a much harder problem due to the large number of comparisons that are required to be performed. Consider that airport authorities are looking for the FBI's 100 most wanted criminals (database size of 100) and the state-of-the-art fingerprint verification system operates at 1% FNMR and 0.001% FMR, i.e., if this system was deployed as a verification system, the system would fail to match the correct users 1% of the time and erroneously verify wrong users 0.001% of the time. Let us consider the outcome of the same system when deployed as an identification system. While the identification FNMR_N will still be 1%, the identification FMR_N will be $\sim 100 \times 0.001\% = 0.1\%$. This means that, while the system has a 99% chance of catching a criminal, it will produce large number of false alarms (e.g., assuming that 200 000 people may use a major U.S. airport in a day, the system will produce 200 false alarms!). Further, if faces are used instead of fingerprints for the identification (face recognition may be preferred for an airport application because faces can be acquired covertly), the number of misses and false alarms will be considerably higher, given the rather poor accuracy of face identification systems, especially in environments with cluttered background and varying lighting conditions. Although multimodal biometric systems (see Section VIII) can significantly improve the identification accuracy, exclusively relying on automatic biometric systems for negative identification may be unfeasible.

Traditional personal recognition tools such as passwords and PINs are not at all useful for negative recognition applications. While biometric systems may not yet be extremely accurate to support large-scale identification applications, they are the only choice for negative recognition applications. Further, if operated in a semi-automatic mode where a human expert examines all the alarms generated by the system for the final decision, biometric systems can be quite effective. For example, if 100 airport security agents are required to manually match every person at an airport against the FBI's 100 most wanted, only five agents may be required to take a closer look at the 200 alarms generated daily by the biometric system. We need to understand that, in such semi-automatic applications, the biometric system only generates an alarm that calls for a closer (manual) examination of the individual and an alarm does not directly translate into catching a terrorist. In fact, the tradeoff between the FMR and FNMR rates in a biometric system is no different from that in any detection system, including the metal detectors already in use at all the airports

Other negative recognition applications such as background checks and forensic criminal identification are also expected to operate in semi-automatic mode and their use follows a similar cost-benefit analysis. For example, in a latent search, an automatic fingerprint identification system (AFIS) is typically used by law enforcement agencies only to narrow down the number of fingerprint matches to be performed by a human expert from a few million to a few hundred. A forensic expert always makes the final decision. In our opinion, use of biometrics in negative recognition applications does not infringe upon the civil liberties of individuals since, if you are not in the "criminal database" already, the recognition system does not keep a record of you (does not remember you). However, appropriate legislation is required to protect the abuse of such systems.

TABLE II
STATE-OF-THE-ART ERROR RATES ASSOCIATED WITH FINGERPRINT, FACE, AND VOICE BIOMETRIC SYSTEMS [6]. NOTE THAT THE ACCURACY ESTIMATES OF BIOMETRIC SYSTEMS ARE DEPENDENT ON A NUMBER OF TEST CONDITIONS

	Test	Test Parameter	FNMR	FMR
Fingerprint	FVC 2002 [25]	Users mostly in the age group 20-39	0.2%	0.2%
Face	FRVT 2002 [34]	Enrollment and test images were collected in indoor environment and could be on different days	10%	1%
Voice	NIST 2000	Text dependent	10-20%	2-5%

VII. LIMITATIONS OF (UNIMODAL) BIOMETRIC SYSTEMS

The successful installation of biometric systems in various civilian applications does not imply that biometrics is a fully solved problem. Table II presents the state-of-the-art error rates of three popular biometric traits. It is clear that there is plenty of scope for improvement in biometrics. Researchers are not only addressing issues related to reducing error rates, but they are also looking at ways to enhance the usability of biometric systems.

Biometric systems that operate using any single biometric characteristic have the following limitations.

1) *Noise in sensed data*. The sensed data might be noisy or distorted. A fingerprint with a scar or a voice altered by cold are examples of noisy data. Noisy data could also be the result of defective or improperly maintained sensors (e.g., accumulation of dirt on a fingerprint sensor) or unfavorable ambient conditions (e.g., poor illumination of a user's face in a face recognition system). Noisy biometric data may be incorrectly matched with templates in the database (see Fig. 5) resulting in a user being incorrectly rejected.
2) *Intra-class variations*. The biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during enrollment, thereby affecting the matching process. This variation is typically caused by a user who is incorrectly interacting with the sensor (see Fig. 6) or when sensor characteristics are modified (e.g., by changing sensors—the sensor interoperability problem) during the verification phase. As another example, the varying psychological makeup of an individual might result in vastly different behavioral traits at various time instances.
3) *Distinctiveness*. While a biometric trait is expected to vary significantly across individuals, there may be large inter-class similarities in the feature sets used to represent these traits. This limitation restricts the discriminability provided by the biometric trait. Golfarelli *et al.* [29] have shown that the *information content* (number of distinguishable patterns) in two of the most commonly used representations of hand geometry and face are only of the order of 10^5 and 10^3, respectively. Thus, every biometric trait has some theoretical upper bound in terms of its discrimination capability.
4) *Nonuniversality*. While every user is expected to possess the biometric trait being acquired, in reality it is possible for a subset of the users to not possess a particular biometric. A fingerprint biometric system, for example, may be unable to extract features from the fingerprints of certain individuals, due to the poor quality of the ridges (see Fig. 7). Thus, there is a failure to enroll (FTE) rate associated with using a single biometric trait. It has been empirically estimated that as much as 4% of the population may have poor quality fingerprint ridges that are difficult to image with the currently available fingerprint sensors and result in FTE errors. Den Os *et al.* [7] report the FTE problem in a speaker recognition system.
5) *Spoof attacks*. An impostor may attempt to spoof the biometric trait of a legitimate enrolled user in order to circumvent the system. This type of attack is especially relevant when behavioral traits such as signature [9] and voice [8] are used. However, physical traits are also susceptible to spoof attacks. For example, it has been demonstrated that it is possible (although difficult and cumbersome and requires the help of a legitimate user) to construct artificial fingers/fingerprints in a reasonable amount of time to circumvent a fingerprint verification system [11].

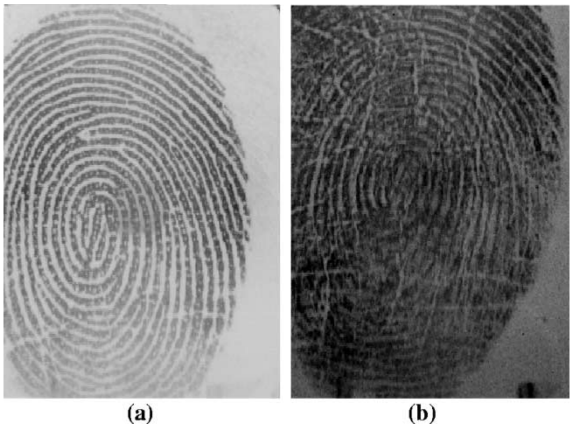

Fig. 5. Effect of noisy images on a biometric system. (a) Fingerprint obtained from a user during enrollment. (b) Fingerprint obtained from the same user during verification after three months. The development of scars or cuts can result in erroneous fingerprint matching results.

VIII. MULTIMODAL BIOMETRIC SYSTEMS

Some of the limitations imposed by unimodal biometric systems can be overcome by using multiple biometric modalities (such as face and fingerprint of a person or multiple fingers of a person). Such systems, known as *multimodal biometric systems* [12], are expected to be more reliable due to the presence

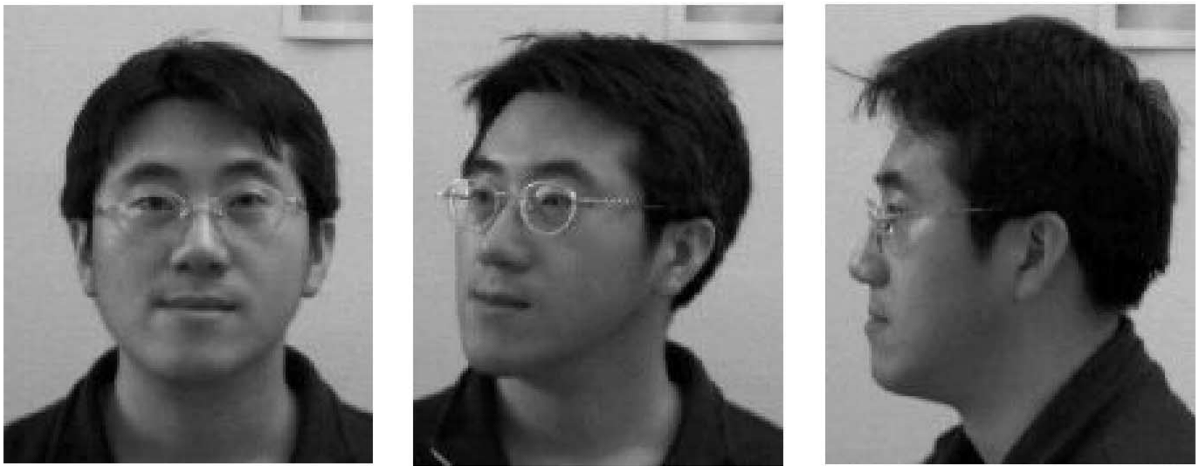

Fig. 6. Intra-class variation associated with an individual's face image. Due to changes in pose, an appearance-based face recognition system will not be able to match these three images successfully, even though they belong to the same individual.

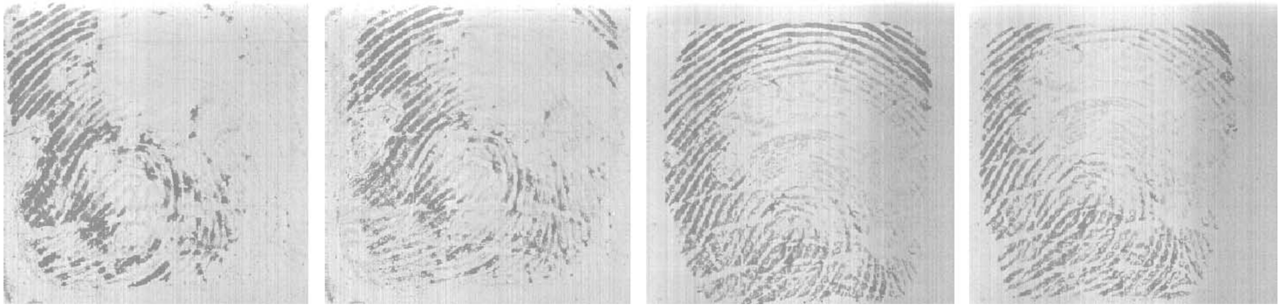

Fig. 7. An example of "failure to enroll" for fingerprints (with respect to a given fingerprint recognition system): four different impressions of a subject's finger exhibiting poor quality ridges due to extreme finger dryness. A given fingerprint system (using a certain sensor and matching algorithm) might not be able to enroll this subject since minutiae and ridge information cannot be reliably extracted.

of multiple, independent pieces of evidence [14]. These systems are also able to meet the stringent performance requirements imposed by various applications [13]. Multimodal biometric systems address the problem of nonuniversality, since multiple traits ensure sufficient population coverage. Further, multimodal biometric systems provide antispoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user. By asking the user to present a random subset of biometric traits (e.g., right index and right middle fingers, in that order), the system ensures that a "live" user is indeed present at the point of data acquisition. Thus, a challenge-response type of authentication can be facilitated using multimodal biometric systems.

A. Modes of Operation

A multimodal biometric system can operate in one of three different modes: serial mode, parallel mode, or hierarchical mode. In the serial mode of operation, the output of one biometric trait is typically used to narrow down the number of possible identities before the next trait is used. This serves as an indexing scheme in an identification system. For example, a multimodal biometric system using face and fingerprints could first employ face information to retrieve the top few matches and then use fingerprint information to converge onto a single identity. This is in contrast to a parallel mode of operation where information from multiple traits is used simultaneously to perform recognition. This difference is crucial. In the serial operational mode, the various biometric characteristics do not have to be acquired simultaneously. Further, a decision could be arrived at without acquiring all the traits. This reduces the overall recognition time. In the hierarchical scheme, individual classifiers are combined in a treelike structure.

B. Levels of Fusion

Multimodal biometric systems integrate information presented by multiple biometric indicators. The information can be consolidated at various levels. Fig. 8 illustrates the three levels of fusion when combining two (or more) biometric systems. These are as follows.

1) *Fusion at the feature extraction level.* The data obtained from each biometric modality is used to compute a feature vector. If the features extracted from one biometric indicator are (somewhat) independent of those extracted from the other, it is reasonable to concatenate the two vectors into a single new vector, provided the features from different biometric indicators are in the same type of measurement scale. The new feature vector has a higher dimensionality and represents a person's identity in a different (and hopefully, more discriminating) feature space. Feature reduction techniques may be employed to extract a small number of salient features from the larger set of features.

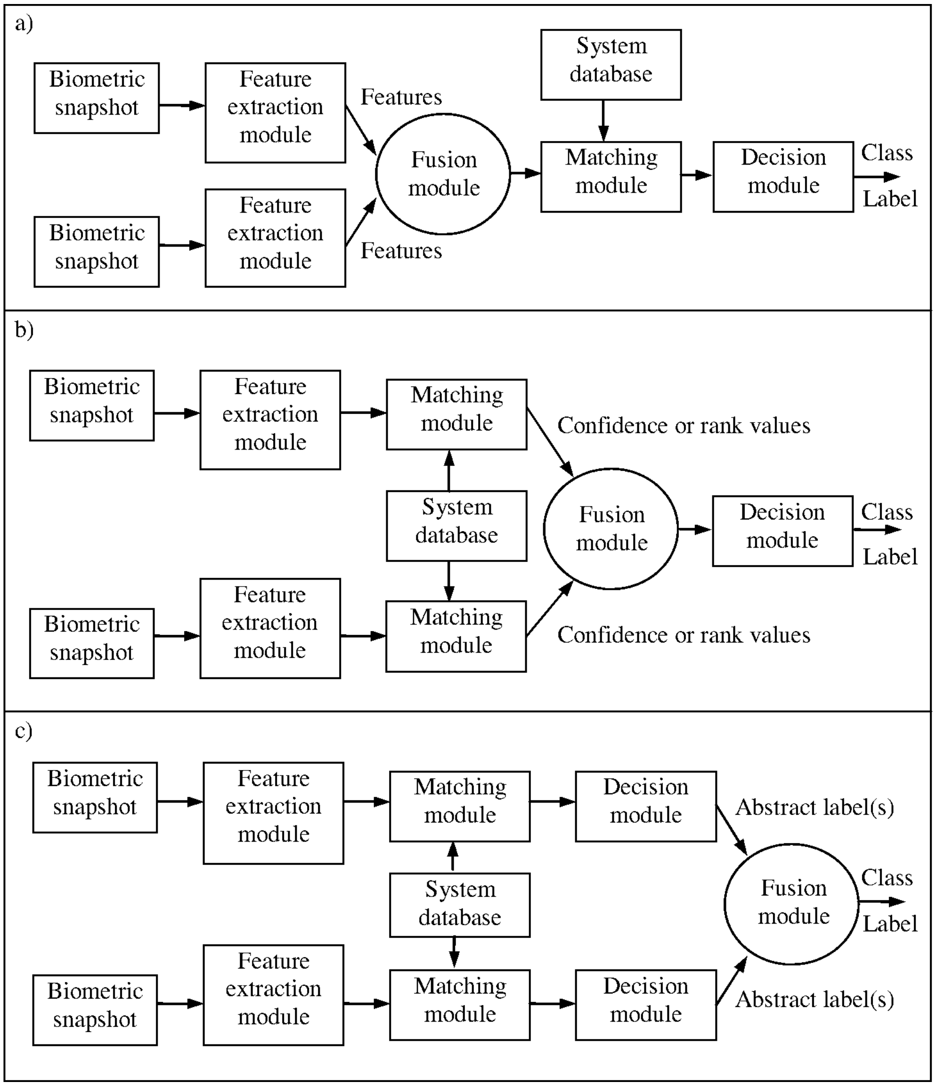

Fig. 8. Different levels of fusion in a parallel fusion mode: (a) fusion at the feature extraction level, and (b) fusion at matching score (confidence or rank) level, and (c) fusion at decision (abstract label) level. In all the three cases, the final class label is "Accept" or "Reject" when the biometric system is operating in the verification mode or the identity of the best matched user when operating in the identification mode. In (c), the intermediate abstract label(s) could be "Accept" or "Reject" in a verification system or a subset of database users in an identification system.

2) *Fusion at the matching score (confidence or rank) level.* Each biometric matcher provides a similarity score indicating the proximity of the input feature vector with the template feature vector. These scores can be combined to assert the veracity of the claimed identity. Techniques such as weighted averaging may be used to combine the matching scores reported by the multiple matchers.
3) *Fusion at the decision (abstract label) level.* Each biometric system makes its own recognition decision based on its own feature vector. A majority vote scheme [15] can be used to make the final recognition decision.

The integration at the feature extraction level assumes a strong interaction among the input measurements and such schemes are referred to as *tightly coupled* integrations [31]. The *loosely coupled* integration, on the other hand, assumes very little or no interaction among the inputs and integration occurs at the output of relatively autonomous agents, each agent independently assessing the input from its own perspective.

It is generally believed that a combination scheme applied as early as possible in the recognition system is more effective. For example, an integration at the feature level typically results in a better improvement than at the matching score level. This is because the feature representation conveys the richest information compared to the matching score of a matcher, while the abstract labels contain the least amount of information about the decision being made. However, it is more difficult to perform a combination at the feature level because the relationship between the feature spaces of different biometric systems may not be known and the feature representations may not be compatible. Further, the multimodal system may not have access to the feature values of individual modalities because of their proprietary nature. In such cases, integrations at the matching score or decision levels are the only options. This is also reflected in the nature of research dedicated to multimodal biometric systems: very few published papers report results on a combination at the feature level. Hong *et al.* [12] theoretically analyzed

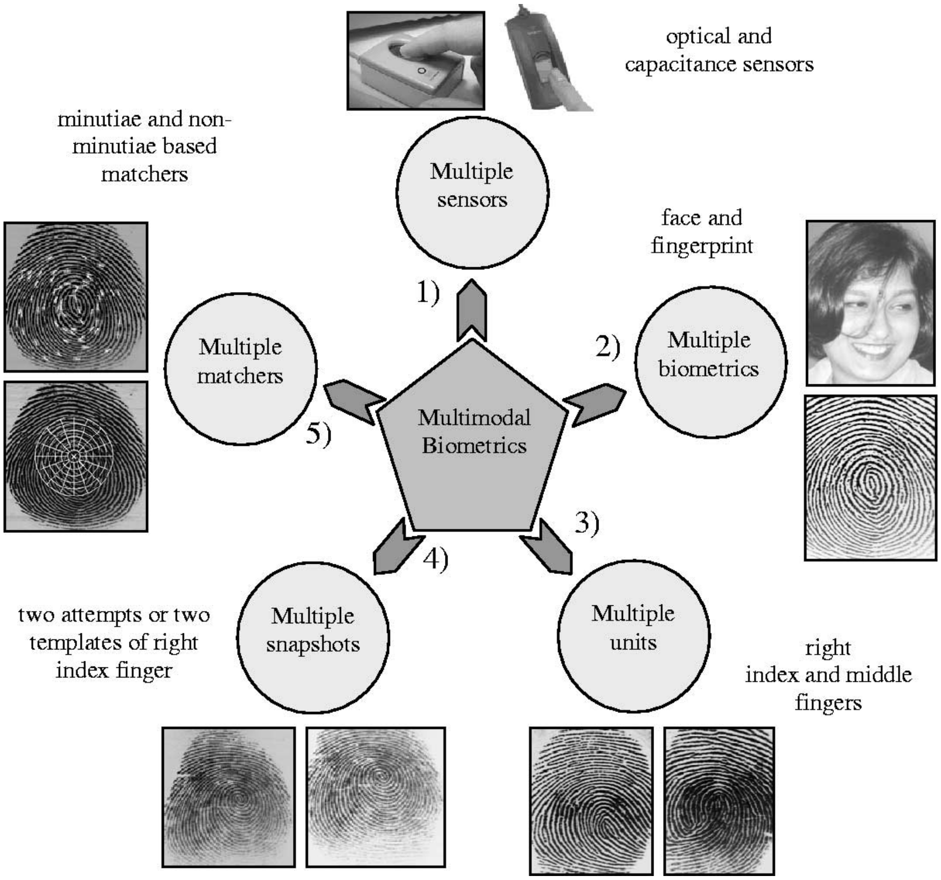

Fig. 9. Various scenarios in a multimodal biometric system.

the improvement in verification accuracy when two biometric characteristics are fused at the matching score level and at the decision level.

C. What to Integrate?

Multimodal biometric systems can be designed to operate in one of the following five scenarios (see Fig. 9).

1) *Multiple sensors*: the information obtained from different sensors for the same biometric are combined. For example, optical, solid-state, and ultrasound based sensors are available to capture fingerprints.
2) *Multiple biometrics*: multiple biometric characteristics such as fingerprint and face are combined. These systems will necessarily contain more than one sensor with each sensor sensing a different biometric characteristic. In a verification system, the multiple biometrics are typically used to improve system accuracy, while in an identification system the matching speed can also be improved with a proper combination scheme (e.g., face matching which is typically fast but not very accurate can be used for retrieving the top M matches and then fingerprint matching which is slower but more accurate can be used for making the final identification decision).
3) *Multiple units of the same biometric*: fingerprints from two or more fingers of a person may be combined, or one image each of the two irises of a person may be combined.
4) *Multiple snapshots of the same biometric*: more than one instance of the same biometric is used for the enrollment and/or recognition. For example, multiple impressions of the same finger, multiple samples of the voice, or multiple images of the face may be combined.
5) *Multiple representations and matching algorithms for the same biometric*: this involves combining different approaches to feature extraction and matching of the biometric characteristic. This could be used in two cases. First, a verification or an identification system can use such a combination scheme to make a recognition decision. Second, an identification system may use such a combination scheme for indexing.

In scenario 1, multiple sensors are used to sense the same biometric identifier while scenario 2 uses multiple sensors to sense different biometric identifiers. An example of scenario 1 may be the use of multiple cameras mounted to capture different views of a person's face. An example of scenario 2 is the use of a camera for capturing face and an optical sensor to capture a fingerprint. While scenario 1 combines moderately independent information, scenarios 2 and 3 combine independent (or weakly dependent) information and are expected to result in a much larger improvement in recognition accuracy. However, this improvement comes at the cost of inconvenience to the user in providing multiple cues and a longer acquisition time. In scenario 4, only a single input may be acquired during recognition and matched with several stored templates acquired during the one-time enrollment process; alternatively, more data acquisitions may be made at the time of recognition and used to consolidate the matching against a single/multiple template. Scenario 5 combines different representation and matching algorithms to improve the recognition accuracy. In our opinion, scenarios 4 and 5 combine strongly correlated measurements and are expected to result in a smaller improvement in recognition accuracy than scenarios 2 and 3, but they are more cost effective than scenario 2 and more convenient than scenario 3. Scenarios 4 and 5 do require more computational and storage resources than a unimodal biometric system but in principle, different feature extractors and matchers can work in parallel. As a result, the overall response time of the system is limited by the slowest individual feature extractor and/or matcher. Finally, a combination of more than one of these scenarios may also be used.

D. Examples of Multimodal Biometric Systems

Multimodal biometric systems have received much attention in recent literature. Brunelli *et al.* [16] describe a multimodal biometric system that uses the face and voice traits of an individual for identification. Their system combines the matching scores of five different matchers operating on the voice and face features to generate a single matching score that is used for identification. Bigun *et al.* developed a statistical framework based on Bayesian statistics to integrate information presented by the speech (text-dependent) and face data of a user [17]. Hong *et al.* combined face and fingerprints for person identification [13]. Their system consolidates multiple cues by associating different confidence measures with the individual biometric matchers and achieved a significant improvement in retrieval time as well as identification accuracy (see Fig. 10). Kumar *et al.* combined hand geometry and palmprint biometrics in a verification system [33]. A commercial product called BioID [18] uses voice, lip motion, and face features of a user to verify identity. Jain and Ross improved the performance of a multimodal biometric system by learning user-specific parameters [30]. General strategies for combining multiple classifiers have been suggested in [19] and [20]. All the approaches presented in [19] (the highest rank method, the Borda count method and logistic regression) attempt to reduce or re-rank a given set of classes. These techniques are thus relevant to the identification problem in which a large number of classes (identities) are present. Prabhakar and Jain [21] showed, in the context of a fingerprint verification system, that combining multiple matchers, multiple enrollment templates, and multiple fingers of a user can significantly improve the accuracy of a fingerprint verification system. They also argue that selecting matchers based on some "goodness" statistic may be necessary to avoid performance degradation when combining multiple biometric modalities. There is a large amount of literature available on the various combination strategies for fusing multiple biometric modalities using the matching scores (see, for example, [22]–[24]).

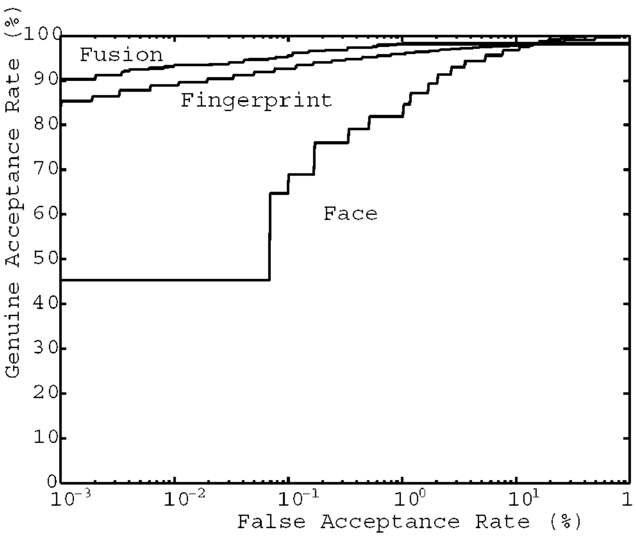

Fig. 10. An improvement in matching accuracy is obtained when face recognition and fingerprint recognition systems are combined in an identification system developed by Hong and Jain [13].

It is well known that independence of modalities plays a very important role in the amount of improvement when combining multiple biometric modalities. A carefully designed combination scheme, that has been trained and tested on a large amount of data, is expected to perform better than the best of the individual ingredient modalities. A combination of uncorrelated modalities (e.g., fingerprint and face or two fingers of a person) is expected to result in a better improvement in performance than a combination of correlated modalities (e.g., different impressions of the same finger or different fingerprint matchers). Further, a combination of uncorrelated modalities can significantly reduce the failure to enroll rate as well as provide more security against "spoofing." On the other hand, such a combination requires the users to provide multiple identity cues, which may cause inconvenience. Additionally, the cost of the system increases because of the use of multiple sensors (e.g., when combining fingerprints and face). The convenience and cost factors remain the biggest barriers in the use of such multimodal biometrics systems in civilian applications. We anticipate that high security applications, large-scale identification systems, and negative identification applications will increasingly use multimodal biometric systems, while small-scale low-cost commercial applications will probably continue striving to improve unimodal biometric systems.

IX. Social Acceptance and Privacy Issues

Human factors dictate the success of a biometric-based identification system to a large extent. The ease and comfort in interaction with a biometric system contribute to its acceptance. For example, if a biometric system is able to measure the characteristic of an individual without contact, such as those using face, voice, or iris, it may be perceived to be more user-friendly and hygienic. Additionally, biometric technologies requiring very little cooperation or participation from the users (e.g., face and face thermograms) may be perceived as being more convenient to users. On the other hand, biometric characteristics that do not require user participation can be captured without the knowledge of the user, and this is perceived as a threat to privacy by many individuals.

The very process of recognition leaves behind trails of private information. For example, if a person is identified each time she makes a purchase, information about where this person shops and what she buys can be simply collected and used by telemarketers to invade her privacy. The issue of privacy becomes more serious with biometric-based recognition systems because biometric characteristics may provide additional information about the background of an individual. For example, retinal patterns may provide medical information about diabetes or high blood pressure in an individual. A health insurance company may use this information in an unethical way for economic gains by denying benefits to a person determined to be of high risk. More importantly, people fear that biometric identifiers could be used for linking personal information across different systems or databases.

On the positive side, biometrics can be used as one of the most effective means for protecting individual privacy. In fact, biometrics ensures privacy by safeguarding identity and integrity. For example, if a person loses a credit card and an adversary finds it, then the credit history of this person is compromised. But, if the credit card could be used only when the user supplies her biometric characteristics (such as in a smartcard containing the user' biometric data), then the user is protected. Biometrics can also be used to limit access to personal information. For instance, a biometric-based patient information system can reliably ensure that access to medical records is available only to the patient and authorized medical personnel. Nevertheless, many people are uneasy about the use of their personal biological characteristics in corporate or government recognition systems. To alleviate these fears, companies and agencies that operate biometric systems have to assure the users of these systems that their biometric information remains private and is used only for the expressed purpose for which it was collected. Legislation is necessary to ensure that such information remains private and that its misuse is appropriately punished.

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

X. Summary

Reliable personal recognition is critical to many business processes. Biometrics refers to automatic recognition of an individual based on her behavioral and/or physiological characteristics. The conventional knowledge-based and token-based methods do not really provide positive personal recognition because they rely on surrogate representations of the person's identity (e.g., exclusive knowledge or possession). It is thus obvious that any system assuring reliable personal recognition must necessarily involve a biometric component. This is not, however, to state that biometrics alone can deliver reliable personal recognition component. In fact, a sound system design will often entail incorporation of many biometric and nonbiometric components (building blocks) to provide reliable personal recognition.

Biometric-based systems also have some limitations that may have adverse implications for the security of a system. While some of the limitations of biometrics can be overcome with the evolution of biometric technology and a careful system design, it is important to understand that *foolproof* personal recognition systems simply do not exist and perhaps, never will. Security is a risk management strategy that identifies, controls, eliminates, or minimizes uncertain events that may adversely affect system resources and information assets. The security level of a system depends on the requirements (threat model) of an application and the cost-benefit analysis. In our opinion, properly implemented biometric systems are effective deterrents to perpetrators.

There are a number of privacy concerns raised about the use of biometrics. A sound trade-off between security and privacy may be necessary; collective accountability/acceptability standards can only be enforced through common legislation. Biometrics provides tools to enforce accountable logs of system transactions and to protect an individual's right to privacy.

As biometric technology matures, there will be an increasing interaction among the market, technology, and the applications. This interaction will be influenced by the added value of the technology, user acceptance, and the credibility of the service provider. It is too early to predict where and how biometric technology would evolve and get embedded in which applications. But it is certain that biometric-based recognition will have a profound influence on the way we conduct our daily business.

References

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy Mag.*, vol. 1, no. 2, pp. 33–42, 2003.

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York: Springer-Verlag, 2003.

[3] A. K. Jain, R. Bolle, and S. Pankanti, Eds., *Biometrics: Personal Identification in Networked Society*. Norwell, MA: Kluwer, 1999.

[4] (2002) Schiphol Backs Eye Scan Security. CNN World News. [Online]. Available: http://www.cnn.com/2002/WORLD/europe/03/27/schiphol.security/

[5] J. Daugman, "Recognizing persons by their Iris patterns," in *Biometrics: Personal Identification in a Networked Society*, A. K. Jain, R. Bolle, and S. Pankanti, Eds. Norwell, MA: Kluwer, 1999, pp. 103–121.

[6] L. O'Gorman, "Seven issues with human authentication technologies," in *Proc. Workshop Automatic Identification Advanced Technologies (AutoID)*, Tarrytown, NY, Mar. 2002, pp. 185–186.

[7] E. d. Os, H. Jongebloed, A. Stijsiger, and L. Boves, "Speaker verification as a user-friendly access for the visually impaired," in *Proc. Eur. Conf. Speech Technology*, Budapest, Hungary, 1999, pp. 1263–1266.

[8] A. Eriksson and P. Wretling, "How flexible is the human voice? A case study of mimicry," in *Proc. Eur. Conf. Speech Technology*, Rhodes, 1997, pp. 1043–1046.

[9] W. R. Harrison, *Suspect Documents, Their Scientific Examination*. Chicago, IL: Nelson-Hall, 1981.

[10] D. A. Black, "Forgery above a genuine signature," *J. Criminal Law, Criminol. Police Sci.*, vol. 50, pp. 585–590, 1962.

[11] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," *Proc. SPIE*, vol. 4677, pp. 275–289, Feb. 2002.

[12] L. Hong, A. K. Jain, and S. Pankanti, "Can multibiometrics improve performance ?," in *Proc. AutoID'99*, Summit, NJ, Oct. 1999, pp. 59–64.

[13] L. Hong and A. K. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 20, pp. 1295–1307, Dec. 1998.

[14] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, and R. P. W. Duin, "Is independence good for combining classifiers?," in *Proc. Int. Conf. Pattern Recognition (ICPR)*, vol. 2, Barcelona, Spain, 2001, pp. 168–171.

[15] Y. A. Zuev and S. Ivanon, "The voting as a way to increase the decision reliability," in *Proc. Foundations of Information/Decision Fusion with Applications to Engineering Problems*, Washington, DC, Aug. 1996, pp. 206–210.

[16] R. Brunelli and D. Falavigna, "Person identification using multiple cues," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 12, pp. 955–966, Oct. 1995.

[17] E. S. Bigun, J. Bigun, B. Duc, and S. Fischer, "Expert conciliation for multimodal person authentication systems using bayesian statistics," in *Proc. Int. Conf. Audio and Video-Based Biometric Person Authentication (AVBPA)*, Crans-Montana, Switzerland, Mar. 1997, pp. 291–300.

[18] R. W. Frischholz and U. Dieckmann, "Bioid: A multimodal biometric identification system," *IEEE Comput.*, vol. 33, pp. 64–68, 2000.

[19] T. K. Ho, J. J. Hull, and S. N. Srihari, "Decision combination in multiple classifier systems," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 16, pp. 66–75, Jan. 1994.

[20] J. Kittler, M. Hatef, R. P. W. Duin, and J. Matas, "On combining classifiers," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 20, pp. 226–239, Mar. 1998.

[21] S. Prabhakar and A. K. Jain, "Decision-level fusion in fingerprint verification," *Pattern Recognit.*, vol. 35, no. 4, pp. 861–874, 2002.

[22] U. Dieckmann, P. Plankensteiner, and T. Wagner, "Sesam: A biometric person identification system using sensor fusion," *Pattern Recognit. Lett.*, vol. 18, no. 9, pp. 827–833, 1997.

[23] P. Verlinde and G. Cholet, "Comparing decision fusion paradigms using k-NN based classifiers, decision trees and logistic regression in a multi-modal identity verification application," in *Proc. Int. Conf. Audio and Video-Based Biometric Person Authentication (AVBPA)*, Washington, DC, Mar. 1999, pp. 188–193.

[24] S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, "Fusion of Face and Speech Data for Person Identity Verification," IDIAP, Martigny, Switzerland, Res. Paper IDIAP-RR 99–03, 1999.

[25] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Fingerprint verification competition," in *Proc. Int. Conf. Pattern Recognition (ICPR)*, Quebec City, QC, Canada, Aug. 2002, pp. 744–747.

[26] J. L. Wayman, "Fundamentals of biometric authentication technologies," *Int. J. Image Graphics*, vol. 1, no. 1, pp. 93–113, 2001.

[27] (2002) Best Practices in Testing and Reporting Performance of Biometric Devices, Version 2.01. U. K. Biometric Work Group (UKBWG). [Online]. Available: http://www.cesg.gov.uk/technology/biometrics/

[28] R. Cappelli, D. Maio, and D. Maltoni, "Indexing fingerprint databases for efficient 1:N matching," in *Proc. 6th Int. Conf. Control Automation Robotics and Vision*, 2000.

[29] M. Golfarelli, D. Maio, and D. Maltoni, "On the error-reject tradeoff in biometric verification systems," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 19, pp. 786–796, July 1997.

[30] A. K. Jain and A. Ross, "Learning user-specific parameters in a multibiometric system," in *Proc. Int. Conf. Image Processing (ICIP)*, Rochester, NY, Sept. 2002, pp. 57–60.

[31] J. Clark and A. Yuille, *Data Fusion for Sensory Information Processing Systems*. Boston, MA: Kluwer, 1990.

[32] D. Zhang and W. Shu, "Two novel characteristic in palmprint verification: Datum point invariance and line feature matching," *Pattern Recognit.*, vol. 32, no. 4, pp. 691–702, 1999.

[33] A. Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, "Personal verification using palmprint and hand geometry biometric," presented at the 4th Int. Conf. Audio- and Video-based Biometric Person Authentication, Guildford, U.K., June 9–11, 2003.

[34] P. J. Philips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone. FRVT 2002: Overview and Summary. [Online]. Available: http://www.frvt.org/FRVT2002/documents.htm

Anil K. Jain (S'70–M'72–SM'86–F'91) received the B.Tech. degree from the Indian Institute of Technology, Kanpur, in 1969 and the M.S. and Ph.D. degrees in electrical engineering from Ohio State University, Columbus, in 1970 and 1973, respectively.

He is a University Distinguished Professor with the Department of Computer Science and Engineering, Michigan State University, East Lansing. He was the Department Chair between 1995 and 1999. His research interests include statistical pattern recognition, exploratory pattern analysis, Markov random fields, texture analysis, three-dimensional object recognition, medical image analysis, document image analysis, and biometric authentication. Several of his papers have been reprinted in edited volumes on image processing and pattern recognition.

Prof. Jain received Best Paper Awards in 1987 and 1991 and received certificates for outstanding contributions in 1976, 1979, 1992, 1997, and 1998 from the Pattern Recognition Society. He also received the 1996 IEEE TRANSACTIONS ON NEURAL NETWORKS Outstanding Paper Award. He is a Fellow of the International Association of Pattern Recognition (IAPR). He has received the Fulbright Research Award, the Guggenheim Fellowship, and the Alexander von Humboldt Research Award. He delivered the 2002 Pierre Devijver lecture sponsored by the International Association of Pattern Recognition (IAPR).

Arun Ross (M'03) received the B.E. (Hons.) degree in computer science from the Birla Institute of Technology and Science, Pilani, India, in 1996 and the M.S. and Ph.D. degrees in computer science and engineering from Michigan State University, East Lansing, in 1999 and 2003, respectively.

Between July 1996 and December 1997, he was with the Design and Development group of Tata Elxsi Ltd., Bangalore, India. He also spent three summers (2000–2002) with the Imaging and Visualization group at Siemens Corporate Research, Inc., Princeton, NJ. He is currently an Assistant Professor with the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown. His research interests include statistical pattern recognition, machine learning, data mining, and biometric authentication.

Dr. Ross is a Member of the IEEE Computer Society.

Salil Prabhakar (M'01) received the B.Tech. degree from the Institute of Technology, Banaras Hindu University, Varanasi, India, in 1996 and the Ph.D. degree from Michigan State University, East Lansing, in 2001, both in computer science and engineering.

During 1996–1997, he worked with IBM India as a Software Engineer. He currently leads the Algorithms Research Group at DigitalPersona Inc., Redwood City, CA, where he works on fingerprint-based biometric solutions. His research interests include pattern recognition, image processing, computer vision, machine learning, biometrics, data mining, and multimedia applications. He is coauthor of more than 25 technical publications and has two patents pending.

Dr. Prabhakar is a Member of the IEEE Computer Society.