

Biometrics: A Tool for Information Security

Anil K. Jain, *Fellow, IEEE*, Arun Ross, *Member, IEEE*, and Sharath Pankanti, *Senior Member, IEEE*

Abstract—Establishing identity is becoming critical in our vastly interconnected society. Questions such as “Is she really who she claims to be?,” “Is this person authorized to use this facility?,” or “Is he in the watchlist posted by the government?” are routinely being posed in a variety of scenarios ranging from issuing a driver’s license to gaining entry into a country. The need for reliable user authentication techniques has increased in the wake of heightened concerns about security and rapid advancements in networking, communication, and mobility. Biometrics, described as the science of recognizing an individual based on his or her physical or behavioral traits, is beginning to gain acceptance as a legitimate method for determining an individual’s identity. Biometric systems have now been deployed in various commercial, civilian, and forensic applications as a means of establishing identity. In this paper, we provide an overview of biometrics and discuss some of the salient research issues that need to be addressed for making biometric technology an effective tool for providing information security. The primary contribution of this overview includes: 1) examining applications where biometrics can solve issues pertaining to information security; 2) enumerating the fundamental challenges encountered by biometric systems in real-world applications; and 3) discussing solutions to address the problems of scalability and security in large-scale authentication systems.

Index Terms—Biometrics, cryptosystems, digital rights management, grand challenge, information security, multibiometrics.

I. INTRODUCTION

THE PROBLEM of information security entails the protection of information elements (e.g., multimedia data) thereby ensuring that only authorized users are able to access the contents available in digital media. Content owners, such as authors and authorized distributors, are losing billions of dollars annually in revenue due to the illegal copying and sharing of digital media. In order to address this growing problem, digital rights management (DRM) systems are being deployed to regulate the duplication and dissemination of digital content [68]. The critical component of a DRM system is user authentication which determines whether a certain individual is indeed authorized to access the content available in a particular digital medium. In a generic cryptographic system, the user authentication method is possession based. That is, the possession of the decrypting key is sufficient to establish the authenticity

of the user. Since cryptographic keys are long and random (e.g., 128 bits for the advanced encryption standard (AES) [1], [2]), they are difficult to memorize. As a result, these keys are stored somewhere (for example, on a computer or a smart card) and released based on some alternative authentication mechanism (e.g., password). Most passwords are so simple, that they can be easily guessed (especially based on social engineering methods) or broken by simple dictionary attacks [3]. It is not surprising that the most commonly used password is the word “password.” Thus, multimedia data protected by a cryptographic algorithm are only as secure as the password (weakest link) used to release the correct decrypting key(s) that can be used for establishing user authenticity. Simple passwords are easy to guess and, thus, compromise security; complex passwords are difficult to remember and, thus, are expensive to maintain.¹ Some users tend to “store” complex passwords at easily accessible locations. Furthermore, most people use the same password across different applications; an impostor upon determining a single password can now access multiple applications. Finally, in a multiuser account scenario, passwords are unable to provide nonrepudiation (i.e., when a password is divulged to a friend, it is impossible to determine who the actual user is: this may eliminate the feasibility of countermeasures such as holding conniving legitimate users accountable in a court of law).

Many of these limitations associated with the use of passwords can be ameliorated by the incorporation of better methods for user authentication. Biometric authentication or, simply biometrics [5], [6], [69], refers to establishing identity based on the physical and behavioral characteristics (also known as traits or identifiers) of an individual such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc. Biometric systems offer several advantages over traditional authentication schemes. They are inherently more reliable than password-based authentication as biometric traits cannot be lost or forgotten (passwords can be lost or forgotten); biometric traits are difficult to copy, share, and distribute (passwords can be announced in hacker websites); and they require the person being authenticated to be present at the time and point of authentication (conniving users can deny that they have shared the password). It is difficult to forge biometrics (it requires more time, money, experience, access privileges) and it is unlikely for a user to repudiate having accessed the digital content using biometrics. Thus, a biometrics-based authentication scheme is a powerful alternative to traditional authentication schemes. In some instances, biometrics can be used in conjunction with passwords (or tokens) to enhance the security offered by the authentication system. In the context of a DRM system,

Manuscript received May 1, 2005; revised March 2, 2006. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Pierre Moulin.

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: arun.ross@mail.wvu.edu).

S. Pankanti is with the Exploratory Computer Vision Group, IBM T. J. Watson Research Center, Yorktown Heights, NY 10598 USA (e-mail: sharat@us.ibm.com).

Digital Object Identifier 10.1109/TIFS.2006.873653

¹For example, anywhere between 25% and 50% of helpdesk calls relate to password resets; these calls cost as much as U.S. \$30 per end user, with the helpdesk receiving at least five calls per end user every year [4].

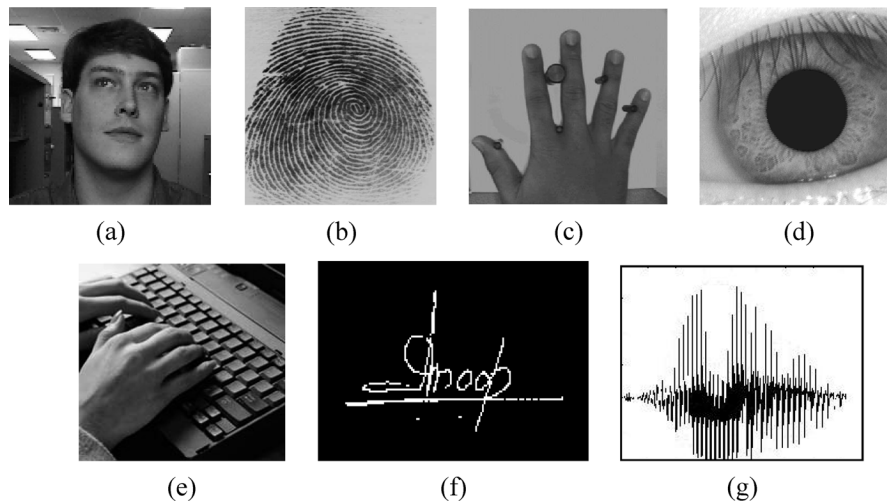


Fig. 1. Examples of biometric characteristics: (a) face, (b) fingerprint, (c) hand geometry, (d) iris, (e) keystroke, (f) signature, and (g) voice.

biometrics can be used 1) to facilitate the entire authentication mechanism, or 2) secure the cryptographic keys that protect a specific multimedia file.

A number of biometric characteristics have been in use for different applications [79]. Each biometric trait has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet all of the requirements (e.g., accuracy, practicality, and cost) of all applications (e.g., DRM, access control, and welfare distribution). In other words, no biometric is “optimal” although a number of them are “admissible.” The suitability of a specific biometric for a particular application is determined depending upon the requirements of the application and the properties of the biometric characteristic. It must be noted that traits, such as voice and keystroke, lend themselves more easily to a challenge-response mechanism that may be necessary in some applications (e.g., telebanking). A brief description of the commonly used biometrics is given below (Fig. 1).

1) *Face*: Face recognition is a nonintrusive method, and facial images are probably the most common biometric characteristic used by humans to make personal recognition. The applications of facial recognition range from a static, controlled “mugshot” authentication to a dynamic, uncontrolled face identification in a cluttered background. The most popular approaches to face recognition [7] 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 authentication performance of the face recognition systems that are commercially available is reasonable [8], they impose a number of restrictions on how the facial images are obtained, often requiring a fixed and simple background or special illumination. These systems also have difficulty in matching face images captured from two drastically different views and under different illumination conditions (i.e., varying temporal contexts). 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 con-

fidence. In order that a facial recognition system works 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; 3) recognize the face from a general viewpoint (i.e., from any pose).

2) *Fingerprint*: Humans have used fingerprints for personal identification for many decades and the matching (i.e., identification) accuracy using fingerprints has been shown to be very high [9]. 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 authentication systems involving a few hundred users. Multiple fingerprints of a person provide additional information to allow for large-scale identification 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 the 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).

3) *Hand 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 [10]. Commercial hand geometry-based authentication 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 authentication 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 such as laptops. There are authentication 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 are still much larger than those used in some other biometrics (e.g., fingerprint, face, and voice).

4) *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 [11], [71], [72]. The accuracy and speed of currently deployed iris-based recognition systems is promising and points to the feasibility of large-scale identification systems based on iris information. Each iris is believed to be distinctive and, like fingerprints, even the irises of identical twins are expected to be different. It is extremely difficult to surgically tamper the texture of the iris. Further, the ability to detect artificial irises (e.g., designer contact lenses) has been demonstrated in the literature. 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. While iris systems have a very low false accept rate (FAR) compared to other biometric traits, the false reject rate (FRR) of these systems can be high [75].

5) *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 is expected to offer sufficient discriminatory information that permits identity verification [12]. 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. However, this biometric permits "continuous verification" of an individual over a period of time.

6) *Signature*: The way a person signs his or her name is known to be a characteristic of that individual [13]. 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 authentication. 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.

7) *Voice*: Voice is a combination of physical 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

TABLE I
EXAMPLES OF COMMONLY USED REPRESENTATION AND MATCHING SCHEMES FOR FIVE DIFFERENT BIOMETRIC TRAITS. ADVANCEMENTS IN STATISTICAL PATTERN RECOGNITION, SIGNAL PROCESSING, AND COMPUTER VISION HAVE RESULTED IN OTHER SOPHISTICATED SCHEMES NOT INDICATED HERE

Modality	Representation Scheme	Matching Algorithm
Fingerprint	Minutiae distribution	String matching
Face	Principal Component Analysis (PCA), Local Feature Analysis (LFA)	Euclidean distance, Bunch graph matching
Iris	Texture analysis, Key-point extraction	Hamming distance
Hand	Length/width of fingers/palm	Euclidean distance
Voice	Mel-Cepstrum	Hidden Markov model, Gaussian mixture model

TABLE II
COMPARISON OF VARIOUS BIOMETRIC TECHNOLOGIES BASED ON THE PERCEPTION OF THE AUTHORS. HIGH, MEDIUM, AND LOW ARE DENOTED BY H, M, AND L, RESPECTIVELY. UNIVERSALITY (DO ALL PEOPLE HAVE IT?), DISTINCTIVENESS (CAN PEOPLE BE DISTINGUISHED BASED ON AN IDENTIFIER?), PERMANENCE (HOW PERMANENT ARE THE IDENTIFIERS?), AND COLLECTABLE (HOW WELL CAN THE IDENTIFIERS BE CAPTURED AND QUANTIFIED?) ARE PROPERTIES OF BIOMETRIC IDENTIFIERS. PERFORMANCE (MATCHING SPEED AND ACCURACY), ACCEPTABILITY (WILLINGNESS OF PEOPLE TO ACCEPT), AND CIRCUMVENTION (FOOLPROOF) ARE ATTRIBUTES OF BIOMETRIC SYSTEMS [18]

Factors →							
Biometric identifier ↓	Universality	Distinctiveness	Permanence	Collectable	Performance	Acceptability	Circumvention
Face	H	H	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

sound [70]. These physical 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 common cold), 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 he or 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 communication channel.

Table I lists some of the commonly used representation and matching schemes for a few biometric traits. Table II compares various biometric traits based on seven different factors.

II. BIOMETRIC VARIANCE

Password-based authentication systems do not involve any complex pattern recognition techniques (passwords have to match exactly) and, hence, they almost always perform accurately as intended by their system designers. On the other



Fig. 2. Variations in a biometric signal: (a) inconsistent presentation: change in facial pose with respect to the camera [76]; (b) irreproducible presentation: temporary change in fingerprint due to the wear and tear of ridges.

hand, biometric signals and their representations (e.g., facial image and eigen-coefficients of facial image) of a person vary dramatically depending on the acquisition method, acquisition environment, user's interaction with the acquisition device, and (in some cases) variation in the traits due to various patho-physiological phenomena. Below, we present some of the common reasons for biometric signal/representation variations.

1) *Inconsistent Presentation*: The signal captured by the sensor from a biometric identifier depends upon both the intrinsic biometric identifier characteristic as well as the way the biometric identifier was presented. Thus, an acquired biometric signal is a nondeterministic composition of a physical biometric trait, the user characteristic behavior, and the user interaction facilitated by the acquisition interface. For example, the three-dimensional (3-D) shape of the finger gets mapped onto the two-dimensional (2-D) surface of the sensor surface. As the finger is not a rigid object and since the process of projecting the finger surface onto the sensor surface is not precisely controlled, different impressions of a finger are related to each other by various transformations. Further, each impression of a finger may possibly depict a different portion of its surface. In case of face acquisition, different acquisitions may represent different poses of the face [Fig. 2(a)]. Hand geometry measurements may be based on different projections of hand on a planar surface. Different iris/retina acquisitions may correspond to different nonfrontal projections of iris/retina on to the image planes.

2) *Irreproducible Presentation*: Unlike the synthetic identifiers [e.g., radio-frequency identification (RFID)], biometric identifiers represent measurements of a biological trait or behavior. These identifiers are prone to wear-and-tear, accidental injuries, malfunctions, and pathophysiological development. Manual work, accidents, etc., inflict injuries to the finger, thereby changing the ridge structure of the finger either permanently or semipermanently [Fig. 2(b)]. Wearing different kinds of jewelry (e.g., rings) may affect hand geometry measurements in an irreproducible way. Facial hair growth (e.g., sideburns and mustache), accidents (e.g., broken nose), attachments

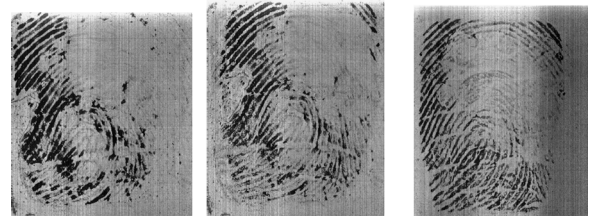


Fig. 3. Imperfect acquisition: three different impressions of a subject's finger exhibiting poor quality ridges possibly due to extreme finger dryness.

(e.g., eyeglasses and jewelry), makeup, swellings, cyst growth, and different hairstyles may all correspond to irreproducible face depictions. Retinal measurements can change in some pathological developments (e.g., diabetic retinopathy). Inebriation results in erratic signatures. The common cold changes a person's voice. All of these phenomena contribute to dramatic variations in the biometric identifier signal captured at different acquisitions.

3) *Imperfect Signal/Representational Acquisition*: The signal acquisition conditions in practical situations are not perfect and cause extraneous variations in the acquired biometric signal. For example, nonuniform contact results in poor quality fingerprint acquisition. That is, the ridge structure of a finger would be completely captured only if ridges belonging to the part of the finger being imaged are in complete physical/optical contact with the image acquisition surface and the valleys do not make any contact with the image acquisition surface. However, the dryness of the skin, shallow/worn-out ridges (due to aging/genetics), skin disease, sweat, dirt, and humidity in the air all confound the situation resulting in a nonideal contact situation (Fig. 3). In the case of inked fingerprints, inappropriate inking of the finger often results in "noisy" low contrast (poor quality) images, which lead to either spurious or missing fingerprint features (i.e., minutiae). Different illuminations cause conspicuous differences in the facial appearance. Backlit illumination may render image acquisition virtually useless in many applications. Depending upon ergonomic conditions, the signature may vary significantly. The channel bandwidth characteristics affect the voice signal.

Further, the feature extraction algorithm is imperfect and introduces measurement errors. Various image processing operations might introduce inconsistent biases to perturb feature localization. A particular biometric identifier of two different people can be very similar because of the inherent lack of distinctive information in it or because of the inadequate representation used for the identifier. As a result of these complex variations in the biometric signal/representations, determining whether two presentations of a biometric identifier are the same typically involves complex pattern recognition and decision making.

III. OPERATION OF A BIOMETRIC SYSTEM

A biometric system may be viewed as a signal detection system with a pattern recognition architecture that senses a raw biometric signal, processes this signal to extract a salient set of features, compares these features against the feature sets residing in the database, and either validates a claimed identity

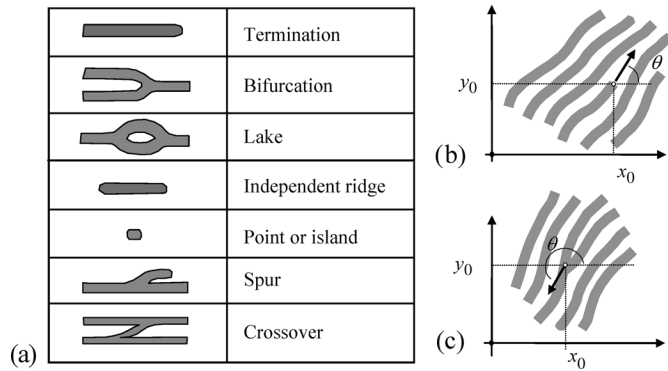


Fig. 4. Fingerprint minutiae: (a) The common fingerprint minutiae types; (b) ridge ending: (x_0, y_0) are the minutia coordinates, θ is the angle that the minutia tangent forms with the horizontal axis; (c) ridge bifurcation.

or determines the identity associated with the signal. Biometric systems attempt to elicit repeatable and distinctive human presentations, and consist (in theory, if not in actual practice) of user-friendly, intuitive interfaces for guiding the user in presenting the necessary traits. In the context of biometric systems, sensing consists of a biometric sensor (e.g., fingerprint sensor or charge-coupled device (CCD) camera), which scans the biometric characteristic of an individual to produce a digital representation of the characteristic. 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 usually further processed by a feature extractor to generate a compact but expressive representation called a feature set which can be stored as a template for future comparison. The feature extraction stage discards the unnecessary and extraneous information from the sensed measurements and gleans useful information necessary for matching.

Let us consider the example of fingerprint matching to illustrate how a biometric matcher operates. The most widely used local features are based on minute details (minutiae) of the fingerprint ridges [Fig. 4(a)]. The pattern of the minutiae of a fingerprint forms a valid representation of the fingerprint. This representation is compact and captures a significant component of information in fingerprints; compared to other representations, minutiae extraction is relatively more robust to various sources of fingerprint degradation. Most types of minutiae in fingerprint images are not stable and cannot be reliably identified by automatic image processing methods. The most widely used features are based on: 1) ridge ending; and 2) ridge bifurcation, which are represented in terms of triplets $[x, y, \theta]$, where $[x, y]$ represents the spatial coordinates in a fixed image-centric coordinate system and θ represents orientation of the ridge at that minutia [Fig. 4(b) and (c)]. Typically, in a live-scan fingerprint image of good quality, there are about 20–70 minutiae.

How are two biometric measurements matched? Typically, a biometric matcher undoes some of the intraclass variations in the biometric measurements to be matched by aligning them with respect to each other. Once the two representations are aligned, an assessment of their similarity is measured. The similarity between the two representations is typically quantified in terms of a matching score; the higher the matching score,

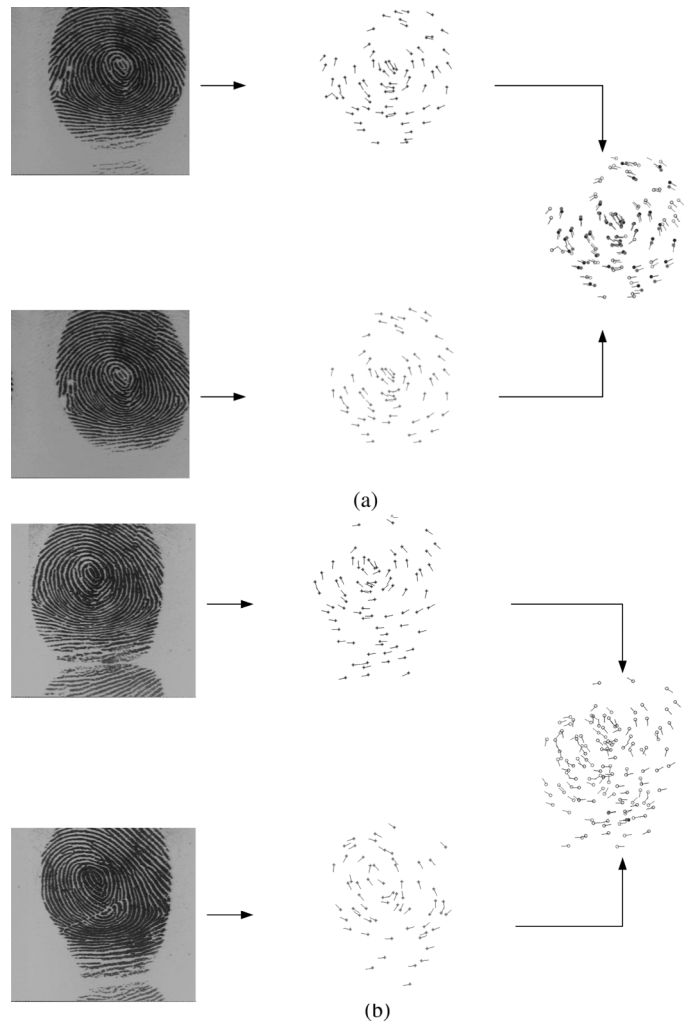


Fig. 5. Fingerprint matching. Here, matching consists of feature (minutiae) extraction followed by alignment and determination of corresponding minutiae (highlighted using filled circles). (a) Matching two impressions of the same fingers; (b) matching impressions from different fingers.

the more similar are the representations. For example, given two (query and template) fingerprint feature representations, the matching module determines whether the prints are impressions of the same finger by a comparison of the query and template features. Only in highly constrained fingerprint systems can one assume that the query and template fingerprints depict the same portion of the finger and are aligned (in terms of displacement from the origin of the imaging coordinate system and of their orientations) with each other. So, in typical situations, one needs to (either implicitly or explicitly) align (or register) the fingerprints (or their representations) before deciding whether the prints are mated pairs. After aligning the fingerprints, the number of matching (or corresponding) features is determined and a fingerprint similarity is defined in terms of the number of corresponding minutiae. Fig. 5 illustrates the matching process. Even in the best practical situations, all minutiae in query and template prints are rarely matched due to spurious minutiae introduced by dirt/leftover smudges, variations in the area of finger being imaged, and displacement of the minutia owing to distortion of the print (Fig. 6) from pressing the finger



Fig. 6. Two (good quality) fingerprint impressions of the same finger exhibiting nonlinear elastic deformation. A fingerprint matching algorithm that assumes a rigid transformation between the two fingerprint representations cannot successfully match the minutiae points present in the two prints.

whose surface is deformable against the flat surface of the acquisition device [55]; the matcher uses a system parameter—the threshold value—to decide whether a given pair of prints belongs to the same finger (mated pair) or not.

IV. FUNCTIONALITIES OF A BIOMETRIC SYSTEM

Biometrics is not only a fascinating pattern recognition research problem but, if carefully used, could also be an enabling technology with the potential to make our society safer, reduce fraud, and lead to user convenience (user friendly man-machine interface) by broadly providing the following three functionalities.

- 1) **Verification (“Is this person truly John Doe?”)**: Biometrics can verify with high certainty the authenticity of a claimed enrollment based on the input biometric sample. For example, a person claims that he or she is known as John Doe within the authentication system and offers his or her fingerprint; the system then either accepts or rejects the claim based on a comparison performed between the offered pattern and the enrolled pattern associated with the claimed identity. Commercial applications, such as computer network logon, electronic data security, ATMs, credit-card purchases, physical access control, cellular phones, personal digital assistants (PDAs), medical records management, and distance learning are sample authentication applications. Authentication applications are typically cost sensitive with a strong incentive for being user friendly.
- 2) **Identification (“Is this person in the database?”)**: Given an input biometric sample, an identification determines if the input biometric sample is associated with any of a large number (e.g., millions) of enrolled identities. Typical identification applications include welfare-disbursement, national ID cards, border control, voter ID cards, driver’s license, criminal investigation, corpse identification, parenthood determination, missing children identification, etc. These identification applications require a large sustainable throughput with as little human supervision as possible.
- 3) **Screening (“Is this a wanted person?”)**: Screening applications determine whether a person belongs to a watchlist of identities. Examples of screening applications could include airport security, security at public events, and other surveillance applications. The

screening watchlist consists of a moderate (e.g., a few hundred) number of identities. By their very nature, the screening applications: 1) do not have a well-defined “user” enrollment phase; 2) can expect only minimal control over their subjects and imaging conditions; 3) require large sustainable throughput with as little human supervision as possible. Screening cannot be accomplished without biometrics (e.g., by using token-based or knowledge-based identification).

Biometric systems are being increasingly deployed in civilian applications that have several thousand enrolled users. The Schiphol Privium scheme at the Amsterdam airport, for example, employs iris scan cards to speed up the passport and visa control procedures.² Passengers enrolled in this scheme insert their card at the gate and look into a camera; the camera acquires the eye image of the traveler, processes it to locate the iris, and computes the IrisCode [11]; 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.

A. Matcher Accuracy and Template Capacity

Unlike password or token-based system, a practical biometric system does not make perfect match decisions and can make two basic types of errors: 1) False Match: the biometric system incorrectly declares a successful match between the input pattern and a nonmatching pattern in the database (in the case of identification/screening) or the pattern associated with an incorrectly claimed identity (in the case of verification). 2) False Nonmatch: the biometric system incorrectly declares failure of match between the input pattern and a matching pattern in the database (identification/screening) or the pattern associated with the correctly claimed identity (verification). Besides the above two error rates, the failure to capture (FTC) rate and the failure to enroll (FTE) rate are also necessary to summarize the accuracy of a biometric system. The FTC rate is only applicable when the biometric device supports automatic capture functionality, 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 of these rates (i.e., FTE, FTC, FNMR, and FMR) constitute important accuracy specifications of a

²“Schiphol backs eye scan security,” (CNN World News, March 27, 2002, Available at <http://www.cnn.com/2002/WORLD/europe/03/27/schiphol.security/>).

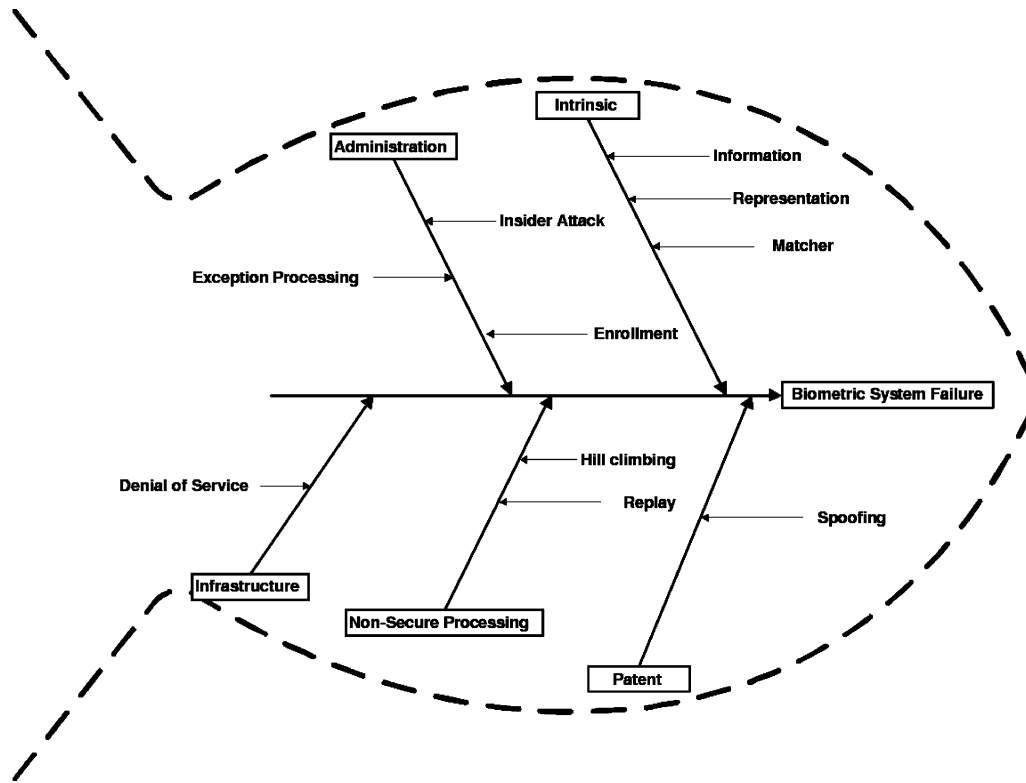


Fig. 7. Fishbone (cause and effect) diagram of biometric failures. The security afforded by a biometric system can be undermined due to a variety of reasons. (a) Administration: The administrative capability of the system can be abused to compromise the integrity of the system. (b) Intrinsic: The inherent limitation in information content, and the representation/matching schemes may result in the erroneous acceptance of an intruder. (c) Infrastructure: A denial-of-service attack can disable system functionality. (d) Nonsecure processing: A hacker could exploit the nature of processing adopted by the system to fraudulently gain access into the system. (e) Patent: Biometrics identifiers are not secrets and, hence, an intruder, though unaware of the intricacies of the system, could create physical or digital artifacts to fool the system.

biometric system and should be reported during performance evaluation.

From an information theory perspective, one is interested in determining the number of unique users that can be represented by the contents of a particular template. Consider a biometric template consisting of n bits. If all bit combinations are possible, then the number of users that can be uniquely represented is 2^n . However, in reality, this is not true because 1) not all bit combinations are valid, and 2) a single user will require more than a single bit-combination. This imposes an upper bound ($\ll 2^n$) on the number of users that can be accommodated by the template. Another formulation of the same problem requires computing the probability that the templates pertaining to two different users demonstrate sufficient similarity. As noted earlier, the notion of similarity in biometrics is defined using a tolerance level (known as a threshold) since it is practically impossible to extract the same feature set from two different instances of a person's biometric. The capacity of a template is an indication of the number of unique users that can be represented by its contents.

V. ATTACKS ON A BIOMETRIC SYSTEM

A biometric system is vulnerable to different types of attacks that can compromise the security afforded by the system, thereby resulting in system failure (Fig. 7). All attacks observed in Fig. 7 can be categorized into two basic types.

- 1) *Zero-effort attacks*: The biometric traits of an opportunistic intruder may be sufficiently similar to a legitimately en-

rolled individual, resulting in a False Match and a breach of system security. This event is related to the probability of observing a degree of similarity between templates originating from different sources by chance.

- 2) *Adversary attacks*: This refers to the possibility that a determined impostor would be able to masquerade as an enrolled user by using a physical or a digital artifact of a legitimately enrolled user. An individual may also deliberately manipulate his or her biometric trait in order to avoid detection by an automated biometric system.

A. Zero-Effort Attacks

What is the probability that the biometric data originating from two different individuals will be sufficiently similar? This question leads to the issue of individuality in biometrics. The individuality of a certain biometric trait is a function of the interclass similarity and the intraclass variability associated with the trait. In order to address this issue, one could model the source that generates the biometric signal or model the parameters constituting the template (i.e., feature set). The individuality problem, in the context of, say, fingerprints, can be formulated in many different ways depending on which one of the following aspects of the problem is under examination: 1) determine the probability that any two (or more) individuals may have sufficiently similar fingerprints in a given target population; 2) given a sample fingerprint, determine the probability of finding a sufficiently similar fingerprint in a target population; 3) given two fingerprints from two different fingers, determine the

probability that they are sufficiently similar. A scientific basis for fingerprint comparison can establish an upper bound on the performance of fingerprint systems.

Given a representation scheme (e.g., minutiae distribution) and a similarity measure (e.g., string matching), there are two approaches for determining the individuality of the fingerprints. In the empirical approach, representative samples of fingerprints are collected and using a typical fingerprint matcher, the accuracy of the matcher on the samples provides an indication of the uniqueness of the fingerprint with respect to the matcher. However, there are known problems (and costs) associated with collection of the representative samples. Additionally, even if a large database of fingerprints, such as the FBI database, which contains about 450 million fingerprints (ten prints of about 45 million people) is used for an empirical evaluation of the fingerprint individuality, it would take approximately 127 years to match all of the fingerprints in the database with each other using a processor with a speed of one million matches per second. In a theoretical approach to individuality estimation, one models all realistic phenomenon affecting interclass and intraclass fingerprint pattern variations. Given the similarity metric, one could then theoretically estimate the probability of a false correspondence. Theoretical approaches are often limited by the extent to which the assumed model conforms to the reality.

The total number of degrees-of-freedom of the pattern space (e.g., minutiae configuration space) does not directly relate to the discriminability of the different patterns (e.g., minutiae from different fingers). The effective estimation of discriminatory information can only be achieved by taking into account intraclass variations. There are several sources of variability in the multiple impressions of a finger: nonuniform contact (with the sensor), irreproducible contact, inconsistent contact, and imaging artifacts. This variability in multiple impressions of a finger manifests itself as: 1) detection of spurious minutiae or missing genuine minutiae; 2) displacement/disorientation (also called deformation) of genuine minutiae; 3) transformation of the type of minutiae (connective ambiguity). However, designing a matcher to accommodate these intraclass variations may result in a significant increase in the probability of false correspondences between minutiae points.

Pankanti *et al.* [14] developed a fingerprint individuality model based on the minutiae configuration of a fingerprint. Given an input fingerprint containing n minutiae, they compute the probability that an arbitrary fingerprint template (in a database of fingerprints) containing m minutiae will have exactly q corresponding minutiae with the input. They assume that minutiae are defined by their location, (x, y) , and by the angle θ , of the ridge on which they reside. If A denotes the area of overlap between the two fingerprints and C denotes the area of tolerance used to decide minutiae correspondences (Fig. 8), then the probability of matching q minutiae in both position and orientation is computed as

$$P(M, m, n, q) = \sum_{\rho=q}^{\min(m, n)} \left(\frac{\binom{m}{\rho} \binom{M-m}{n-\rho}}{\binom{M}{n}} \binom{\rho}{q} l^q (1-l)^{\rho-q} \right)$$

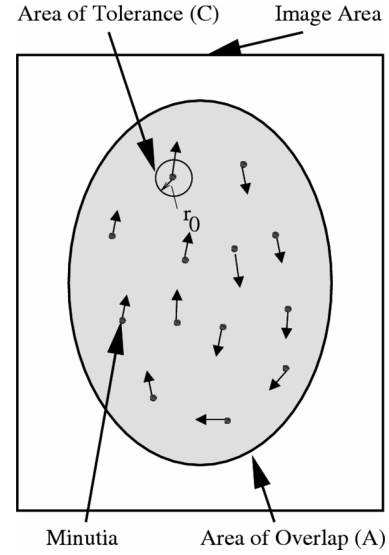


Fig. 8. Illustration of the area of overlap and the area of tolerance when comparing two fingerprints.

TABLE III
FINGERPRINT CORRESPONDENCE PROBABILITIES OBTAINED FROM THE INDIVIDUALITY MODEL PROPOSED BY PANKANTI ET AL. [14] FOR DIFFERENT SIZES OF FINGERPRINT IMAGES CONTAINING 26, 36, OR 46 MINUTIAE. THE ENTRY (70, 12, 12, 12) CORRESPONDS TO THE 12-POINT GUIDELINE. THE VALUE OF M FOR THIS ENTRY WAS COMPUTED BY ESTIMATING TYPICAL PRINT AREA MANIFESTING 12 MINUTIAE IN A 500-dpi OPTICAL FINGERPRINT SCAN

M, m, n, q	$P(\text{Fingerprint Correspondence})$
104, 26, 26, 26	5.27×10^{-40}
104, 26, 26, 12	3.87×10^{-9}
176, 36, 36, 36	5.47×10^{-39}
176, 36, 36, 12	6.10×10^{-8}
248, 46, 46, 46	1.33×10^{-77}
248, 46, 46, 12	5.86×10^{-7}
70, 12, 12, 12	1.22×10^{-20}

where l is the probability of two position-matched minutiae having similar orientation, and $M = A/C$ is assumed to be an integer (since $A \gg C$).

The authors in [14] report the value of $P(M, m, n, q)$ for fingerprint images containing 12, 26, 36, and 46 minutiae (Table III). While the individuality of the minutiae-based fingerprint representation based on their model is lower than other estimates in the literature (e.g., [61]), their results indicate that the likelihood of an adversary guessing someone's fingerprint pattern (e.g., requiring matching 20 or more minutia from a total of 36) is significantly lower than a hacker being able to guess a six-character alphanumeric case-sensitive (most probably weak) password by social engineering techniques (most common passwords are based on birthday, spouse's name, etc.) or by brute force (the probability of guessing such a password by brute force is 1.76×10^{-11}). Obviously, more stringent conditions on matching will provide a better cryptographic strength at the risk of increasing the false rejection error rate.

B. Adversary Attacks

Biometrics are not "secrets." Physical traits, such as face and fingerprint, can be surreptitiously obtained from an individual (e.g., covert acquisition of face images or lifting latent prints from an object) for creating digital or physical artifacts that can

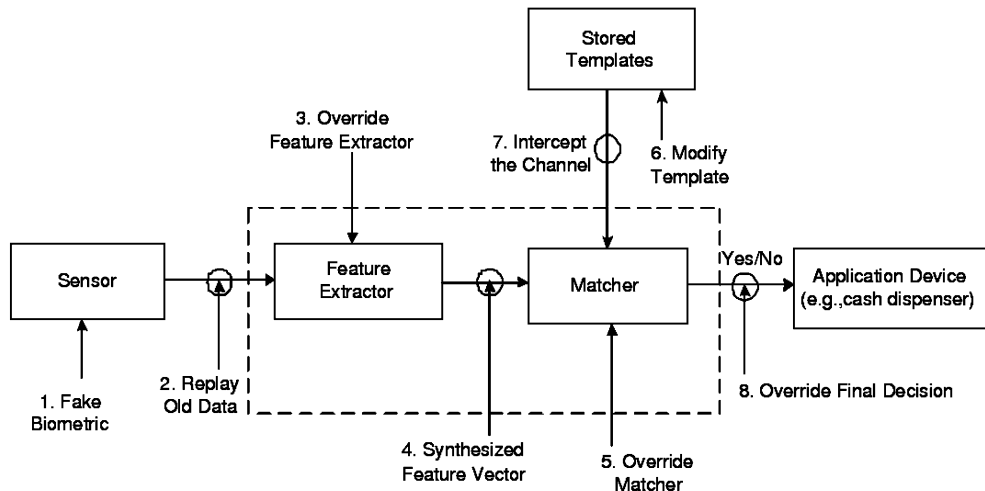


Fig. 9. Vulnerabilities in a biometric system (adapted from [16]).

then be used to spoof the identity of a legitimately enrolled individual. Besides this, there are other attacks that can be launched against an application whose resources are protected using biometrics [15], [73].

- 1) *Circumvention*: An intruder may fraudulently gain access to the system by circumventing the biometric matcher and peruse sensitive data such as medical records pertaining to a legitimately enrolled user. Besides violating the privacy of the enrolled user, the impostor can modify sensitive data including biometric information.
- 2) *Repudiation*: A legitimate user may access the facilities offered by an application and then claim that an intruder had circumvented the system. A bank clerk, for example, may modify the financial records of a customer and then deny responsibility by claiming that an intruder must have spoofed her (i.e., the clerk's) biometric trait and accessed the records.
- 3) *Collusion*: An individual with super-user privileges (such as an administrator) may deliberately modify biometric system parameters to permit incursions by a collaborating intruder.
- 4) *Coercion*: An impostor may force a legitimate user (e.g., at gunpoint) to grant him access to the system.
- 5) *Denial of Service (DoS)*: An attacker may overwhelm the system resources to the point where legitimate users desiring access will be refused service. For example, a server that processes access requests can be bombarded with a large number of bogus requests, thereby overloading its computational resources and preventing valid requests from being processed.

Ratha *et al.* [16] identified several different levels of attacks that can be launched against a biometric system (Fig. 9). These attacks are intended to either circumvent the security afforded by the system or to deter the normal functioning of the system: 1) a fake biometric trait, such as an artificial finger, may be presented at the sensor; 2) illegally intercepted data may be resubmitted to the system; 3) the feature extractor may be replaced by a Trojan horse program that produces predetermined feature sets; 4) legitimate feature sets may be replaced with synthetic feature sets;

5) the matcher may be replaced by a Trojan horse program that always outputs high scores thereby defying the system security; 6) the templates stored in the database may be modified or removed. Alternately, new templates may be introduced in the database; 7) the data in the communication channel between various modules of the system may be altered; 8) the final decision output by the biometric system may be overridden.

Template security is an important consideration in the design of a biometric system. The U.K. Biometric Working Group (UK-BWG) lists several factors that can affect the integrity of the template [17]: 1) accidental template corruption due to a system malfunction such as a hardware failure; 2) deliberate alteration of an enrolled template by an attacker; 3) substitution of a valid template with a bogus template for the purpose of deterring system functionality.

A template represents a set of salient features that summarizes the biometric data (signal) of an individual. Due to its compact nature, it is commonly assumed that the template cannot be used to elicit complete information about the original biometric signal. Furthermore, since the templates are typically stored in an encrypted form, it is substantially difficult to decrypt and determine the contents of the stored template (without knowledge of the correct decrypting keys). Thus, traditionally, template-generating algorithms have been viewed as one-way algorithms. However, in recent literature, there have been techniques presented that contradict these assumptions. Adler [74] demonstrated that a face image can be regenerated from a face template using a "Hill Climbing Attack." An iterative scheme is employed to reconstruct a face image using a face verification system that releases match scores. Uludag and Jain [15] devised a synthetic template generator (STG) that also uses the "Hill Climbing Attack" to determine the contents of a target minutiae template.

Several methods have been suggested in the literature to protect biometric templates from revealing important information. In order to prevent the Hill-Climbing Attack from successfully converging, Soutar [18] has suggested the use of coarsely quantized match scores by the matcher. However, Adler [19] demonstrated that it is still possible to estimate the unknown enrolled

image although the number of iterations required to converge is significantly higher now. The Hill-Climbing attack can be prevented if the biometric system aborts the matching process upon detecting multiple (say, 3) unsuccessful attempts.

Yeung and Pankanti [20] describe an invisible fragile watermarking technique to detect regions in a fingerprint image that have been tampered with by an attacker. In the proposed scheme, a chaotic mixing procedure is employed to transform a visually perceptible watermark to a random-looking textured image in order to make it resilient against attacks. This “mixed” image is then embedded in a fingerprint image. The authors show that the presence of the watermark does not affect the feature extraction process. Furthermore, the original “unmixed” watermark may be recovered by using an inverse mapping. The use of a watermark also imparts copyright capability by identifying the origin of the raw fingerprint image.

Jain and Uludag [21] suggest the use of steganography principles [81] to hide biometric data (e.g., eigencoefficients of a face image) in host images (e.g., fingerprints). This is particularly useful in distributed systems where the raw biometric data may have to be transmitted over a nonsecure communication channel. Embedding biometric data in an innocuous host image prevents an eavesdropper from accessing sensitive template information. Further, the embedded data are not significantly affected when the host image is subjected to a severe tampering method such as cropping. The authors also discuss a novel application wherein the facial features of a user (i.e., eigencoefficients) are embedded in a host fingerprint image (of the user). In this scenario, the watermarked fingerprint image of a person may be stored in a smart card issued to that person. At an access control site, the fingerprint of the person possessing the card will first be compared with the fingerprint present in the smart card. The eigencoefficients hidden in the fingerprint image can then be used to reconstruct the user’s face, thereby serving as a second source of authentication.

Watermarking and steganography techniques should be applied before encrypting the raw biometric data or the template. Note that encryption relies on the use of a difficult-to-compute secret key(s) to protect biometric information. Watermarking and steganography principles, on the other hand, protect the data even if this secret key is compromised and the biometric data are decrypted. Therefore, it is necessary for biometric vendors to use both of these techniques in conjunction in order to enhance the privacy of the stored information.

Since the biometric trait of a person cannot be easily replaced (unlike passwords and PINs), a compromised template would mean the loss of a user’s identity. Ratha *et al.* [22] propose the use of distortion functions to generate biometric data that can be canceled if necessary. They use a noninvertible transformation function that distorts the input biometric signal (e.g., face image) prior to feature extraction or, alternately, modifies the extracted feature set (e.g., minutiae points) itself. When a stored template is compromised, then the current transformation function is replaced with a new function thereby “canceling” the current (compromised) template and generating a new one. This also permits the use of the same biometric trait in several different applications by merely adopting an application-specific transformation function. However, it is not clear how one would

ensure that the biometric discriminability is not impoverished in the transformed domain.

Linnartz and Tuyls [23] proposed the use of shielding functions to protect the biometric templates of a user from being misused by an administrator of the biometric system. The authors accomplish this by using delta-contracting and epsilon-revealing functions to preprocess the biometric data acquired from an individual. These functions make it computationally prohibitive for an administrator to estimate the original data of the user. Although several techniques have been proposed to enhance the security of a user’s template, government regulations will also have to be established in order to address the issue of template privacy. For example, issues related to the sharing of biometric templates across agencies (e.g., health-care providers and law-enforcement agencies) and the inferring of personal information about an enrolled user (e.g., Is this person prone to diabetes?) from biometric data have to be countered by establishing an appropriate legal framework.

VI. BIOMETRIC CRYPTOSYSTEMS: THE FUZZY VAULT SCHEME

Given that the biometric system (like any other security system) is vulnerable to a number of adversary attacks, it is important to address the issue of secure design of the biometric system. Specifically, one would like to know whether there is a secure method of combining biometric authentication and cryptographic techniques. In a simplistic biometrics-based key release method [52], a successful biometric template match releases a cryptographic key [Fig. 10(a)]. This method is vulnerable to attacks on the biometric template database, cryptographic key database, and the biometric matcher. A more monolithic combination would entail generating a combined biometric-cryptographic key that is cryptographically secure (e.g., will not reveal information about a biometric template or about the cryptographic key) from intruders while, for legitimate users, will permit access to the protected resource (e.g., key). The advantage of the second method [Fig. 10(b)], called the biometrics-based key generation method [52], is that since secret and biometric templates are securely stored in the crypto-biometric template, the system is less vulnerable to attacks on the template information database.

The matching of biometric identifiers within a cryptographic framework is a very challenging problem. In traditional (symmetric) cryptography, if the encryption and decryption keys are not identical, the decryption operation will produce useless random data. When biometric identifiers are employed as “keys” in the context of the cryptographic system, demanding such an exactitude is impractical, that is, for the same biometric entity (e.g., the right index finger) that is analyzed during different acquisitions, the extracted biometric data will significantly vary due to acquisition characteristics. The issue dealing with the variability of the biometric data within the context of the cryptographic (biometric key generation) system has not been studied until recent years [52].

A. Biometric Key Generation Implementation

In this section, we summarize a biometric (fingerprint) key generation system implementation by Uludag *et al.* [63], a cryptographic construct called the fuzzy vault (see Juels and Sudan

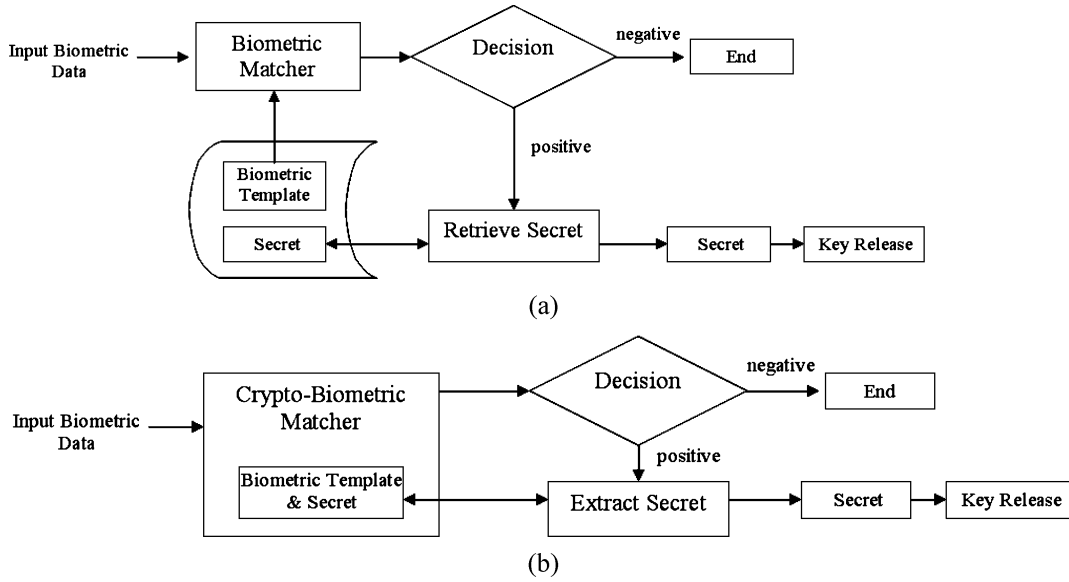


Fig. 10. Two modes of combining biometrics with cryptography: (a) key release and (b) key generation [63].

[62]). The technique suggested by the authors is very preliminary, but the concept is rather powerful.

For simplicity, let us assume that the system uses 8-bit x -coordinates of fingerprint minutiae features but it can be (and has been) extended to include other minutiae information as well. Further assume that x -coordinates have been appropriately coarsely quantized (e.g., to the nearest number divisible by 5). Fig. 11 shows the block diagram of a fingerprint fuzzy vault system.

Encoding: Secret S is any secret data that needs to be protected (e.g., secret encryption key). The fuzzy vault built by Uludag *et al.* [63] begins by concatenating 16-bits CRC data C from the initial secret S (56-bits key) to produce SC (72 bits). This concatenation reduces the chance of a random error being undetected (i.e., failing to identify incorrect decoding). SC is used to find the coefficients of the polynomial P : 72-bits SC can be represented as a polynomial with 8 (72/9) coefficients, with degree $D = 7$, $p(x) = c_7x^7 + c_6x^6 + \dots + c_1x + c_0$, by decomposing SC into nonoverlapping 9-bit segments, and each segment is declared as a specific coefficient c_i , $i = 0, 1, 2, \dots, 7$. Assuming that there are N unique template minutiae, x_1, x_2, \dots, x_N , the authors find a set of ordered pairs $G = \{(x_1, p(x_1)), (x_2, p(x_2)), \dots, (x_N, p(x_N))\}$. A second set of ordered pairs, called the chaff set C , is then generated from M random x -coordinates c_1, c_2, \dots, c_M (distinct from x_1, x_2, \dots, x_N) such that $C = \{(c_1, d_1), (c_2, d_2), \dots, (c_M, d_M)\}$ and $d_i \neq p(c_i), \forall i$. The union of these two sets $G \cup C$ is randomized to produce vault set VS .

Decoding: Here, a user tries to unlock the vault V using the query minutiae features. Given N query minutiae (Q) $x_1^*, x_2^*, \dots, x_N^*$, the points to be used in polynomial reconstruction are found by comparing x_i^* , $i = 1, 2, \dots, N$, with the abscissa values of the vault V , namely v_l , $l = 1, 2, \dots, (M+N)$: if any x_i^* , $i = 1, 2, \dots, N$ is equal to v_l , $l = 1, 2, \dots, (M+N)$, the corresponding vault point (v_l, w_l) is added to the list of points to be used. Assume that this list has K points,

where $K \leq N$. Now, for decoding a degree D polynomial, $(D+1)$ unique projections are necessary. All possible combinations of $(D+1)$ points, among the list with size K are considered, resulting in $\binom{K}{D+1}$ combinations. For each of these combinations, the Lagrange interpolating polynomial is constructed. For a specific combination set given as $L = \{(v_1, w_1), (v_2, w_2), \dots, (v_{D+1}, w_{D+1})\}$, the corresponding polynomial is

$$p^*(x) = \frac{(x - v_2)(x - v_3) \dots (x - v_{D+1})}{(v_1 - v_2)(v_1 - v_3) \dots (v_1 - v_{D+1})} w_1 \\ + \frac{(x - v_1)(x - v_3) \dots (x - v_{D+1})}{(v_2 - v_1)(v_2 - v_3) \dots (v_2 - v_{D+1})} w_2 + \dots \\ + \frac{(x - v_1)(x - v_2) \dots (x - v_D)}{(v_{D+1} - v_1)(v_{D+1} - v_2) \dots (v_{D+1} - v_D)} w_{D+1}$$

yielding $p^*(x) = c_7^*x^7 + c_6^*x^6 + \dots + c_1^*x + c_0^*$. The coefficients are mapped back to the decoded secret SC^* . If the CRC remainder on SC^* is not zero, we are certain that there are errors. If the remainder is zero, with very high probability, there are no errors. For the latter case, SC^* is segmented into two parts: the first 56 bits denote S^* while the remaining 16 bits are CRC data. Finally, the system outputs S^* . If the query minutiae list overlaps with the template minutiae list in at least $(D+1)$ points, for some combinations, the correct secret will be decoded, namely, $S^* = S$ will be obtained. This denotes the desired outcome when the query and template fingerprints are from the same finger.

VII. MULTIBIOMETRIC SYSTEMS

The matching accuracy of a biometric system is impacted by several factors and, therefore, the performances observed in several test conditions suggest that biometric authentication has significant scope for improvement. Table IV presents the “state-of-the-art” error rates of four popular biometric traits. 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. Some of the challenges encountered by

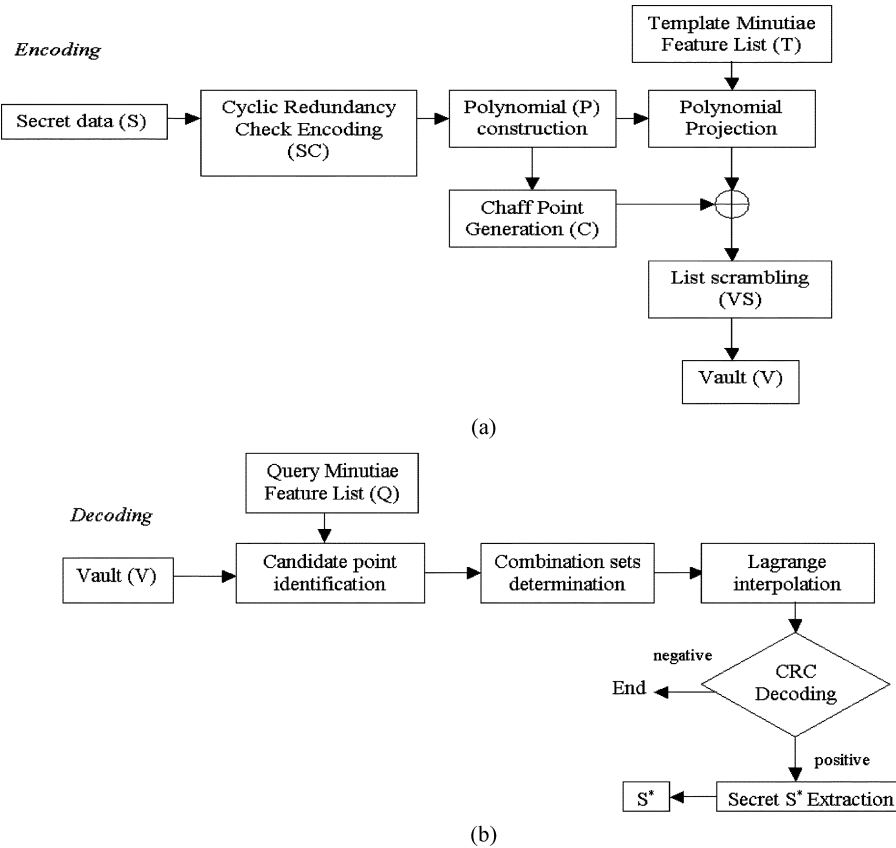


Fig. 11. Flowchart of the fuzzy fingerprint vault: (a) encoding and (b) decoding [63].

TABLE IV

“STATE-OF-THE-ART” ERROR RATES ASSOCIATED WITH FINGERPRINT, FACE, VOICE, AND IRIS BIOMETRIC SYSTEMS. NOTE THAT THE ACCURACY ESTIMATES OF BIOMETRIC SYSTEMS ARE DEPENDENT ON A NUMBER OF TEST CONDITIONS

Modality	Test Label	Test Conditions	FNMR	FMR
Fingerprint	FpVTE 2003 [57]	US Government operational data (>25,000 subjects)	0.1%	1%
Fingerprint	FVC 2004 [56]	Exaggerated skin distortion, rotation (100 subjects)	2%	2%
Face	FRVT [58]	Varied lighting, outdoor/indoor (37,437 subjects)	10%	1%
Voice	NIST [59]	Text independent, multi-lingual	5-10%	2-5%
Iris	ITIRT [75]	Indoor environment (1224 subjects)	0.99%	0.94%

a biometric system in an operational scenario include the following.

- 1) *Noise in sensed data*: The sensed data might be noisy or distorted. Noisy biometric data may be incorrectly matched with templates in the database, resulting in a user being incorrectly rejected.
- 2) *Intraclass 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, or when sensor characteristics are modified (e.g., by changing sensors—the sensor interoperability problem [64]) during the verification phase.

- 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.
- 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 be not able to provide a particular biometric.
- 5) *Spoof attacks*: An impostor may attempt to spoof the biometric trait of a legitimate enrolled user in order to circumvent the system [25]–[27].

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 multibiometric systems, are expected to be more reliable due to the presence of multiple, independent pieces of evidence [28], [82]. These systems are also able to meet the stringent performance requirements imposed by various applications [29]. Multibiometric systems can address the problem of nonuniversality, since multiple traits ensure sufficient population coverage. Further, multibiometric systems could provide antispooing 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-

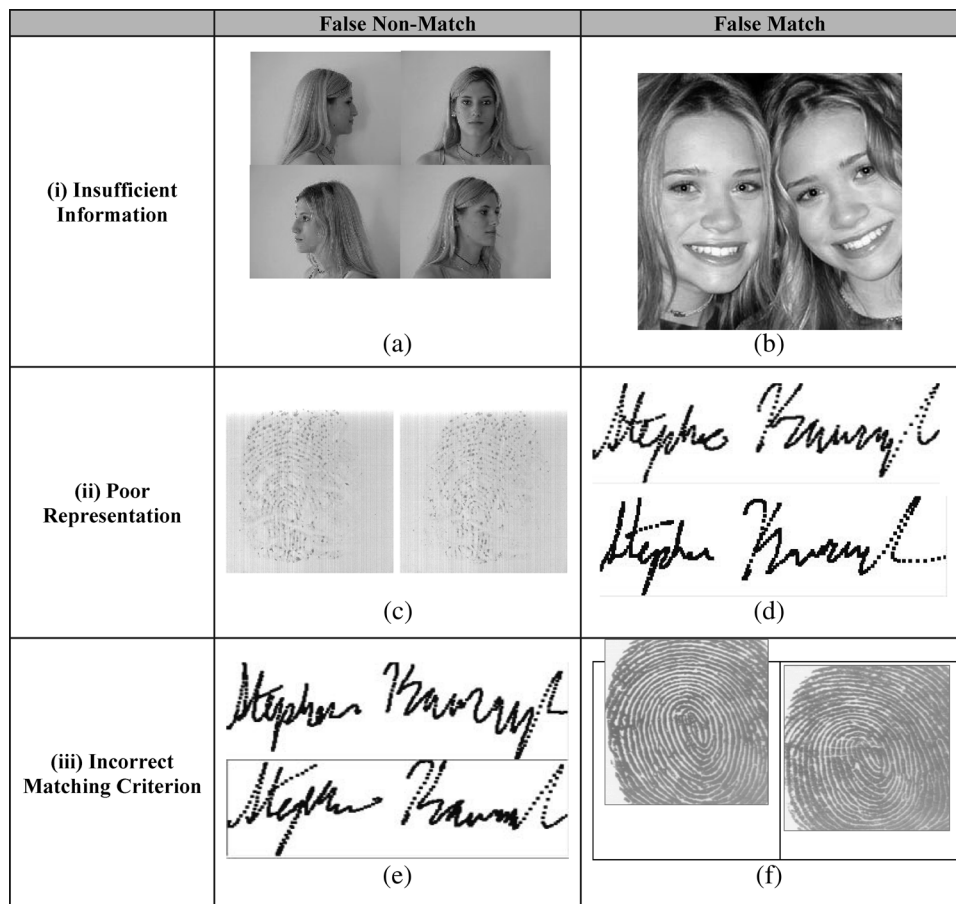


Fig. 12. Generic reasons for poor accuracy performance: (i) information limitation: the invariant and distinctive information content in the pattern samples may be inherently limited [24]. (a) Due to a change in pose, an appearance-based face recognition system will not be able to match these images (taken from <http://www.lrv.fri.uni-lj.si/facedb.html>, see [76]) successfully, even though they belong to the same individual. (b) Identical twins cannot be reliably distinguished using face information alone. (ii) Representation limitation: practical feature extraction systems, typically based on simplistic models of biometric signal, fail to capture all discriminatory information in the biometric signal. (c) “Poor quality” prints from a finger cannot be matched by traditional minutiae-based fingerprint identification systems, although the fingerprint experts claim to routinely use such smudged prints to make a reliable match decision similarly. (d) Forged signatures cannot be distinguished based on the representations derived from shape information alone and temporal (e.g., speed, acceleration of pen) signature information is often useful to distinguish fraudulent impostors. (iii) Matcher limitation: a practical matcher may not be accurate because it does not take into account realistic variations in the biometric signals. (e) Two mated signatures are not correctly matched because the matcher fails to recognize that one is a distorted version of the other. (f) A very simple matching criterion (e.g., gross fingerprint features) may result in an incorrect match decision (i.e., two prints from different fingers can be declared as a match if the matcher uses only the overall appearance similarity (e.g., image correlation) for matching).

response type of authentication can be facilitated using multi-biometric systems.

Mere usage of multiple biometrics does not necessarily imply better system performance; a poorly designed multibiometric system can result in deterioration in performance of the individual modalities, increase the cost of the system, and present increased inconvenience to users/administrators (e.g., complex enrollment procedures).

A. Modes of Operation

A multibiometric 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 multibiometric 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 cascade operational mode, the various biometric characteristics do not have to be acquired simultaneously. Further, a decision could be arrived at without acquiring all of the traits. This reduces the overall recognition time. In the hierarchical scheme, individual classifiers are combined in a treelike structure.

B. Levels of Fusion

Evidence in a multibiometric system can be integrated in several different levels (Fig. 13) as described below.

- 1) *Sensor level*: The raw data acquired from multiple sensors can be processed and integrated to generate new data from which features can be extracted. For example, in the case of face biometrics, both 2-D texture information and 3-D depth (range) information (obtained using two different sensors) may be fused to generate a 3-D texture image of

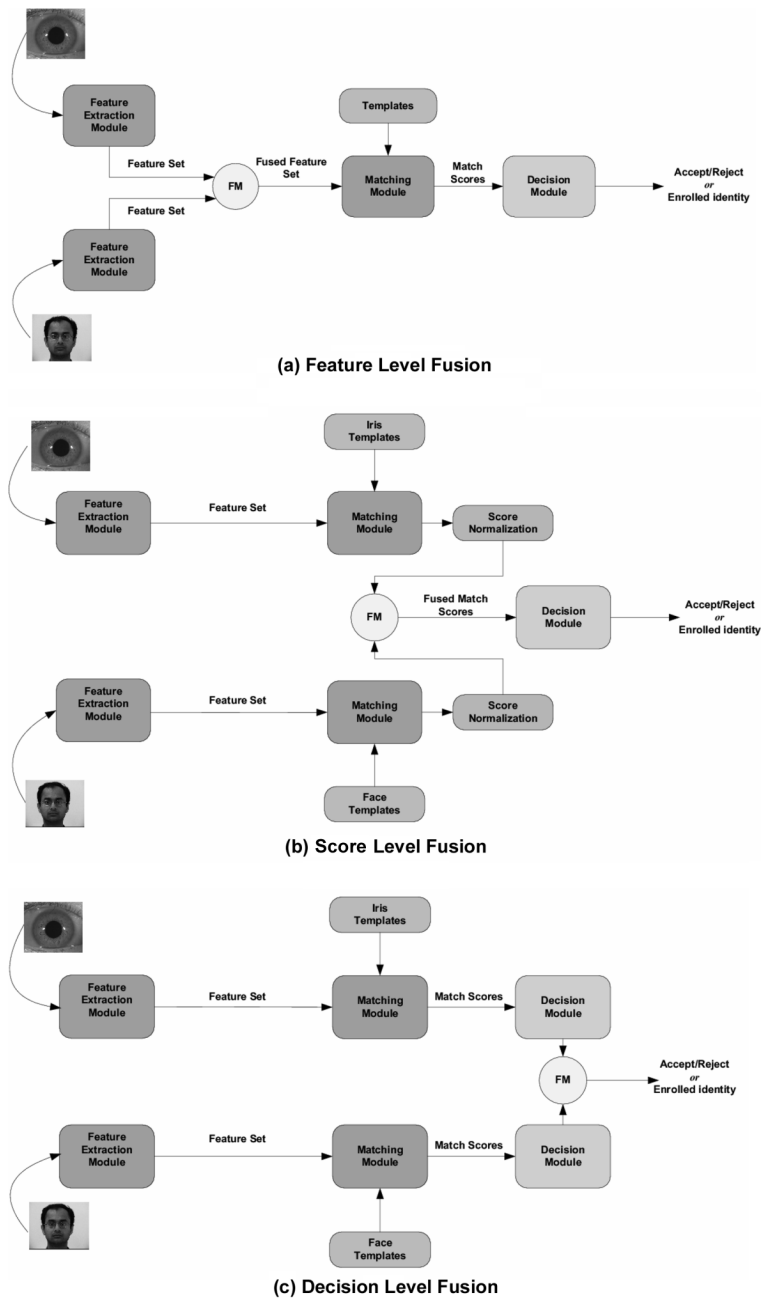


Fig. 13. Examples of fusion in the parallel mode of operation: (a) feature extraction level; (b) match score (confidence or rank) level; (c) decision (abstract label) level.

the face which could then be subjected to feature extraction and matching.

- 2) *Feature level*: The feature sets extracted from multiple data sources can be fused to create a new feature set to represent the individual. The geometric features of the hand, for example, may be augmented with the eigen-coefficients of the face in order to construct a new high-dimension feature vector. A feature selection/transformation procedure may be adopted to elicit a minimal feature set from the high-dimensional feature vector.
- 3) *Match score level*: In this case, multiple classifiers output a set of match scores which are fused to generate a single scalar score. As an example, the match scores generated by

the face and hand modalities of a user may be combined via the simple sum rule in order to obtain a new match score which is then used to make the final decision.

- 4) *Rank level*: This type of fusion is relevant in identification systems where each classifier associates a rank with every enrolled identity (a higher rank indicating a good match). Thus, fusion entails consolidating the multiple ranks associated with an identity and determining a new rank that would aid in establishing the final decision. Techniques such as the Borda count [80] may be used to make the final decision.
- 5) *Decision level*: When each matcher outputs its own class label (i.e., accept or reject in a verification system, or the

identity of a user in an identification system), a single class label can be obtained by employing techniques such as majority voting, behavior knowledge space, etc.

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. 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 assesses 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 is expected to result 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, when the multimodal systems employ proprietary individual modalities developed by different commercial entities, different feature values may not be accessible to the system. In such cases, integration at the matching score, rank, or decision levels are the only options. This is also reflected in the nature of research dedicated to multibiometric systems: very few published papers report results on a combination at the feature level [37].

Multibiometric systems have received much attention in recent literature. Brunelli *et al.* [32] describe a multibiometric 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.* develop a statistical framework based on Bayesian statistics to integrate information presented by the speech (text dependent) and face data of a user [33]. Hong *et al.* combined face and fingerprints for person identification [29]. 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. Kumar *et al.* combined hand geometry and palmprint biometrics in a verification system [36]. A commercial product called BioID [34] uses voice, lip motion, and face features of a user to verify identity. Jain and Ross improved the performance of a multibiometric system by learning user-specific parameters [35]. General strategies for combining multiple classifiers have been suggested in [38] and [39]. All of the approaches presented in [38] (the highest rank method, the Borda count method, and logistic regression) attempt to reduce or re-rank a given set of pattern classes. These techniques are thus relevant to the identification problem in which a large number of classes (identities) are present. Prabhakar and Jain [40] 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. Hong *et al.* [28] theoretically analyzed the improvement in verification accuracy when two biometric characteristics are fused at the matching score level and at the decision level. There is a large amount of literature available on the various combination strategies for fusing multiple biometric modalities using matching scores (see, for example, [41]–[43]).

Recently, Dass *et al.* [65] used copula models to estimate the joint generalized densities of match scores originating from multiple matchers. Copula functions are effective in modeling the joint distribution when the marginal distributions (pertaining to the scores of a single matcher) are non-normal and do not have a parametric form. These functions can represent a variety of dependence structures using a correlation matrix. The authors then employ a copula fusion rule (based on the Neyman–Pearson Lemma) that combines the estimates of the generalized distribution functions of multiple matchers. They demonstrate that the joint generalized densities obtained by using copula fusion rule result in improved matching performance as opposed to product or marginal density estimates (see [40] and [66]). Their approach eliminates the need to perform match score normalization [67] or determine optimal weights [35] for combining matchers.

VIII. RESEARCH CHALLENGES IN BIOMETRIC RECOGNITION

There are several reasons underlying imperfect accuracy performance of a biometric system as summarized in Section II (see, also Fig. 12). A number of challenging research problems in biometric matcher design need to be addressed before the performance hiatus can be effectively closed.

Effective Representation and Matching: The biometric system design challenge is to be able to arrive at a realistic representational/invariance model of the identifier from a few samples acquired under possibly inconsistent conditions, and then, formally estimate the inherent discriminatory information (e.g., individuality) in the signal from the samples. This is especially difficult in a large-scale identification system where the number of classes/identities is huge (e.g., in the millions). Further, the representation/model of a user has to be updated over a period of time (i.e., the template update problem [60]) in order to account for temporal/permanent changes in the user’s biometric trait. The problem of seamlessly integrating multiple biometric cues to provide effective identification across the entire population is also very challenging given the variety of scenarios that are possible.

Performance Modeling (i.e., Biometric Individuality): One of the most fundamental questions one would like to ask about any practical biometric authentication system is: what is the inherent discriminable information available in the input signal? Unfortunately, this question, if at all, has been answered in a very limited setting for most biometrics modalities. The inherent signal capacity issue is of enormous complexity as it involves modeling both the composition of the population as well as the interaction between the behavioral and physiological attributes at

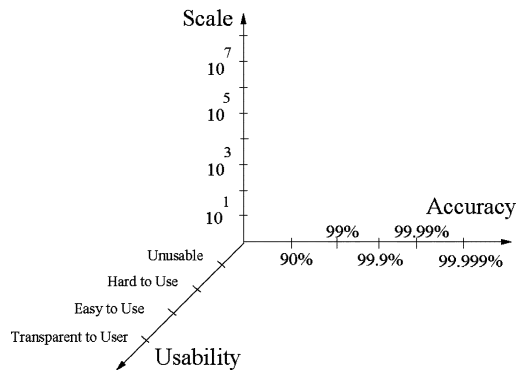


Fig. 14. Biometric system characterization. The accuracy axis represents the intrinsic 1:1 (verification) accuracy of the matcher.

different scales of time and space. Nevertheless, a first-order approximation to the answers to these questions will have a significant bearing on the acceptance of (biometrics-based) personal identification systems into our society as well as determining the upper bounds on scalability of deployments of such systems.

Characterizing Signal Quality and Enhancement: For a particular biometric to be effective, it should be universal: every individual in the target population should possess the biometric and every acquisition of the biometric from an individual should provide useful information for personal identity recognition. In practice, adverse signal acquisition conditions and inconsistent presentations of the signal often result in unusable or nearly unusable biometric signals (biometric samples). This is confounded by the problem that the underlying individual biometric signal can vary over time due to (for example) aging. Hence, poor quality of a biometric sample constitutes the single most cause of inferior matching accuracy in biometric systems. Therefore, it is important to quantify the quality of the signal for either seeking a better representation of the signal or for subjecting the poor signal to alternative methods of processing. In situations involving noncooperative individuals, where it may not be feasible to acquire a good quality biometric signal, it is critical that the procured signal be suitably enhanced in order to permit accurate processing of the data. Indeed, biometric signal enhancement is an important research problem that has to be pursued in a systematic manner.

Empirical Performance Measurement: Performance assessment plays a crucial role in determining whether the given biometric system is acceptable or needs further improvement. Obtaining reliable performance estimation is very challenging [77], [78]. This is especially true when the system is already operational or when the system is being tested against adversarial attacks. How does one reliably predict the performance (accuracy, speed, and vulnerability) of a large-scale biometric system that has several million identities enrolled in it?

Besides the problems enumerated above, issues related to privacy, security, integrity and liveness detection will also have to be addressed [49], [50].

IX. SUMMARY AND CONCLUSION

Biometrics presents important technical, policy, and system challenges that must be solved because there is no substitute

TABLE V
FEW EXAMPLES OF NOVEL BIOMETRIC-ENABLED APPLICATIONS

Application	Description	Precaution
Wallet-less vending	Biometrics allows for convenient account access with sufficient fraud resistance	Privacy safeguards against cross-system linkages; security assurance against vulnerabilities; compliance with "proportionality" principles ⁶
High risk transactions	Biometrics allows for undertaking high-risk high-value transactions without incurring the cost of additional verification	
Recovery from loss/theft	Loss of wallet is no longer a serious problem. Replacement of lost or stolen credit cards is easy	
Disaster relief	Rapid identification of deceased/injured victims and reunification of displaced surviving members (e.g., Tsunami)	
Quick emergency medical services	It is easier to provide assistance in unexpected personal emergencies (e.g., medical relief on airplane)	
Security check-in	It allows for convenient and cost-effective public infrastructure access without compromising security	
Fine grained loyalty schemes	Different persons on an account can be reliably distinguished	

for this technology for addressing many critical information security problems. Considering the recent government mandates for national and international use of biometrics in delivering crucial societal functions, there is urgency to further develop basic biometric capabilities, and to integrate them into practical applications. Because biometrics cannot be easily shared, misplaced, or forged, the resultant security is more reliable than current password systems and does not encumber the end user with remembering long cryptographically strong passwords. Biometric-based system administrator access to sensitive user information affords effective accountability.

While biometric technology appears to be well suited to provide a user-convenient component of secure person-identity linkage, there may be cultural, societal, and religious resistance toward acceptance of this technology [44]. On the other hand, the hyperbole underlying biometric technology has created the expectation that biometric is the panacea for all of our security and identity theft problems and not merely one of the several complementary technologies (e.g., RFID, conventional security, process engineering) that need to be integrated in a way that remains to be well defined. For example, one of the fundamental sources of identity theft problem is the critical reliance on the linkages to and information in legacy identity management systems. While biometric technology can mitigate some of the enrollment problems (e.g., multiple identities), it cannot solve the problem of having to rely on imperfect legacy identity management systems. One may have to rely on process engineering (e.g., ensuring enrollment at birth as is currently done in local birth registers and the U.S. Social Security System) for several generations before we could ensure perfect enrollment. Meanwhile, we may have to rely on a delicate balance of deterrence and detection of identity fraud guided by sound public policy. A poorly implemented biometric system can be the cause of complacency, disaster, and a further basis for resistance. On the other hand, a well-implemented biometrics system with sufficient privacy safeguards may be a clear requirement in the quick response to natural or man-made disasters. Much remains to be accomplished in terms of general education of the end users, system administrators, integrators, and most important, public policy makers.

The limitations of the current state of the biometric technology should not be construed to imply that it is not currently useful in many applications. In fact, there are a large number of biometric solutions that have been successfully deployed to provide useful value in practical applications. For example, the hand geometry system has served as a good access control solution in many deployments such as university dorms, building entrance, and time and attendance applications. AFIS systems³ have been providing terrific value to society (since their inception in the U.S. in the late 1960s), integrating automatic and manual processes. Disney World uses the finger geometry information of individuals to ensure that a season pass is not shared among multiple individuals.⁴ Further iterative cycles of technology development, application to new domains, realistic performance evaluation [46], and standardization efforts⁵ will facilitate the cycle of build-test-share for transforming the technology into business solutions.

The complexity of designing a biometric system [51] based on three main factors (accuracy, scale or size of the database, and usability) is illustrated in Fig. 14. Many application domains require a biometric system to operate on the extreme of only one of the three axes in Fig. 14 and such systems have been successfully deployed. The grand challenge is to design a system that would operate on the extremes of all of these three axes simultaneously. This will entail overcoming the fundamental barriers that have been cleverly avoided in designing the currently successful niche biometric solutions. Addressing these core research problems in the opinion of the authors will significantly advance the state of the art and make biometric systems more secure, robust, and cost-effective. This, we believe, will promote adoption of biometric systems, resulting in potentially broad economic and social impact.

As biometric technology matures, there will be increasing interaction among the market, the technologies, and the applications. This interaction will be influenced by the additional value of the technology, user acceptance, and the credibility of the service provider. It is too early to predict exactly where and how biometric technology will evolve and into which particular applications it will become embedded (see Table V for a list of potential applications). But it is certain that biometric-based recognition will have a profound influence on the way we conduct our daily business because of the inherent potential for effectively linking people to records, thereby ensuring information security.

ACKNOWLEDGMENT

The authors would like to thank U. Uludag, K. Nandakumar, Y. Chen, S. Prabhakar, and S. Dass for their assistance in preparing this manuscript. The authors are grateful to J. L. Wayman, T. Tan, P. Moulin, and the anonymous reviewers for their feedback and useful suggestions.

³<http://www.fbi.gov/hq/cjis/iafis.htm>

⁴http://www.biometricgroup.com/in_the_news/cbs_market_watch.html

⁵The INCITS website http://www.ncits.org/tc_home/m1.htm.

⁶Proportionality principle mandates that system actions cannot go beyond what is strictly necessary to achieve the expressed objectives of the system.

REFERENCES

- [1] Advanced encryption standard (AES), Federal Information Processing Standards Publication 197 National Institute of Standards and Technology, 2001 [Online]. Available: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- [2] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 3rd ed. Upper Saddle River, NJ: Prentice-Hall, 2003, Guest Editorial, S. Pankanti, R. Bolle, A. K. Jain (Guest Editors) Special Issue of IEEE Computer on Biometrics, Feb. 2000.
- [3] D. V. Klein, "Foiling the cracker: a survey of, and improvements to, password security," in *Proc. 2nd USENIX Workshop Security*, 1990, pp. 5–14.
- [4] I. Armstrong, Passwords Exposed: Users are the Weakest Link SCMag [Online]. Available: <http://www.scmagazine.com/>, June 2003
- [5] A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*. Norwell, MA: Kluwer, 1999.
- [6] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technology, Special Issue Image- and Video-Based Biomet.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.
- [7] S. Z. Li and A. K. Jain, Eds., *Handbook of Face Recognition*. New York: Springer Verlag, 2004.
- [8] P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone, FRVT 2002: Evaluation Report March 2003 [Online]. Available: <http://www.frv.org/FRVT2002/documents.htm>
- [9] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York: Springer Verlag, Jun. 2003.
- [10] R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzales-Marcos, "Biometric identification through hand geometry measurements," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 10, pp. 1168–1171, Oct. 2000.
- [11] J. Daugman, "The importance of being random: statistical principles of iris recognition," *Pattern Recognit.*, vol. 36, no. 2, pp. 279–291, 2003.
- [12] F. Monroe and A. Rubin, "Authentication via keystroke dynamics," in *Proc. 4th ACM Conf. Computer and Communications Security*, Apr. 1997, pp. 48–56.
- [13] V. S. Nalwa, "Automatic on-line signature verification," *Proc. IEEE*, vol. 85, no. 2, pp. 213–239, Feb. 1997.
- [14] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the individuality of fingerprints," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 8, pp. 1010–1025, Aug. 2002.
- [15] U. Uludag and A. K. Jain, "Attacks on biometric systems: a case study in fingerprints," in *Proc. SPIE-EI Security, Steganography and Watermarking of Multimedia Contents VI*, San Jose, CA, Jan. 2004, pp. 622–633.
- [16] N. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proc. Int. Conf. Audio and Video-based Biometric Person Authentication*, Halmstad, Sweden, Jun. 2001, pp. 223–228.
- [17] U.K. Biometric Working Group, Biometric Security Concerns CESG, Sep. 2003 [Online]. Available: <http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricSecurityConcerns.pdf>, Tech. Rep.
- [18] C. Soutar, Biometric System Security White Paper, Bioscrypt [Online]. Available: <http://www.bioscrypt.com>
- [19] A. Adler, "Images can be regenerated from quantized biometric match score data," in *Proc. Can. Conf. Electrical Computer Eng.*, Niagara Falls, ON, Canada, May 2004, pp. 469–472.
- [20] M. Yeung and S. Pankanti, "Verification watermarks on fingerprint recognition and retrieval," *Proc. SPIE Conf. Security and Watermarking of Multimedia Contents*, vol. 3657, pp. 66–78, Jan. 1999.
- [21] A. K. Jain and U. Uludag, "Hiding biometric data," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 11, pp. 1493–1498, Nov. 2003.
- [22] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.
- [23] J.-P. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in *Proc. Audio- and Video-based Person Authentication*, Guildford, U.K., Jun. 2003, pp. 393–402.
- [24] M. Golfarelli, D. Maio, and D. Maltoni, "On the error-reject tradeoff in biometric verification systems," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 19, no. 7, pp. 786–796, Jul. 1997.
- [25] D. A. Black, "Forgery above a genuine signature," *J. Criminal Law, Criminol. Police Sci.*, vol. 50, pp. 585–590, 1962.

- [26] A. Eriksson and P. Wretling, "How flexible is the human voice? A case study of mimicry," in *Proc. Eur. Conf. Speech Technology*, Rhodes, Greece, 1997, pp. 1043–1046.
- [27] T. Matsumoto, H. Hoshino, K. Yamada, and S. , "Impact of artificial gummy fingers on fingerprint systems," *Proc. SPIE*, vol. 4677, pp. 275–289, Feb. 2002.
- [28] L. Hong, A. K. Jain, and S. Pankanti, "Can multibiometrics improve performance?," in *Proc. AutoID*, Summit, NJ, Oct. 1999, pp. 59–64.
- [29] L. Hong and A. K. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, no. 12, pp. 1295–1307, Dec. 1998.
- [30] 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*, Barcelona, Spain, 2001, vol. 2, pp. 168–171.
- [31] Y. A. Zuev and S. Ivanon, "The voting as a way to increase the decision reliability. foundations of information/decision fusion with applications to engineering problems," in *Proc. Foundations of Information/Decision Fusion With Applications to Engineering Problems*, Washington D.C., Aug. 1996, pp. 206–210.
- [32] R. Brunelli and D. Falavigna, "Person identification using multiple cues," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 12, no. 10, pp. 955–966, Oct. 1995.
- [33] 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*, Crans-Montana, Switzerland, Mar. 1997, pp. 291–300.
- [34] R. W. Frischholz and U. Dieckmann, "Bioid: a multimodal biometric identification system," *IEEE Comput.*, vol. 33, no. 2, pp. 64–68, Feb. 2000.
- [35] A. K. Jain and A. Ross, "Learning user-specific parameters in a multibiometric system," in *Proc. IEEE Int. Conf. Image Processing*, Rochester, NY, Sep. 2002, pp. 57–60.
- [36] A. Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, "Personal verification using palmprint and hand geometry biometric," in *Proc. 4th Int. Conf. Audio- and Video-based Biometric Person Authentication*, Guildford, U.K., Jun. 9–11, 2003.
- [37] A. Ross and R. Govindarajan, "Feature level fusion using hand and face biometrics," in *Proc. SPIE Conf. Biometric Technology for Human Identification II*, Mar. 2005, pp. 196–204.
- [38] T. K. Ho, J. J. Hull, and S. N. Srihari, "Decision combination in multiple classifier systems," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 16, no. 1, pp. 66–75, Jan. 1994.
- [39] J. Kittler, M. Hatef, R. P. W. Duin, and J. Matas, "On combining classifiers," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, no. 3, pp. 226–239, Mar. 1998.
- [40] S. Prabhakar and A. K. Jain, "Decision-level fusion in fingerprint verification," *Pattern Recognit.*, vol. 35, no. 4, pp. 861–874, 2002.
- [41] U. Dieckmann, P. Plankenstein, and T. Wagner, "Sesam: a biometric person identification system using sensor fusion," *Pattern Recognit. Lett.*, vol. 18, no. 9, pp. 827–833, 1997.
- [42] 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*, Washington D.C., Mar. 1999, pp. 188–193.
- [43] S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, "Fusion of face and speech data for person identity verification," Martigny, Switzerland, Jan. 1999, Res. Paper IDIAP-RR 99-03, IDIAP.
- [44] A. K. Jain, L. Hong, and S. Pankanti, "Biometrics: promising frontiers for emerging identification market," *Comm. ACM*, pp. 91–98, Feb. 2000.
- [45] H. Petroski, *To Engineer Is Human: The Role of Failure in Successful Design*. New York: Vintage Books, 1992.
- [46] J. L. Wayman, "Technical testing and evaluation of biometric identification devices," in *Biometric: Personal Identification in Networked Society*, Jain, Bolle, and Pankanti, Eds. Norwell, MA: Kluwer, 1999, ch. 17.
- [47] S. Berinato and L. Cosgove, "The state of IT security," *CIO Mag.*, Oct., 15, 2003.
- [48] J. Beatty, S. Brodsky, M. Nally, and R. Patel, Next-Generation Data Programming: Service Data Objects White Paper Nov. 2003 [Online]. Available: <http://www.ibm.com/developerworks/library/j-commonj-sdomt/>
- [49] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: security & privacy concerns," *IEEE Sec. Privacy Mag.*, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.
- [50] D. Brin, *Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*. Reading, MA: Addison-Wesley, Apr. 1998.
- [51] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross, and J. L. Wayman, "Biometrics: a grand challenge," in *Proc. Int. Conf. Pattern Recognition*, Cambridge, U.K., Aug. 2004.
- [52] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proc. IEEE (Special Issue on Multimedia Security for Digital Rights Management)*, vol. 92, no. 6, pp. 948–960, Jun. 2004.
- [53] A. K. Jain, L. Hong, and S. Pankanti, "Biometrics: promising frontiers for emerging identification market," *Comm. ACM*, pp. 91–98, Feb. 2000.
- [54] J. L. Wayman, *National Biometric Test Center Collected Works*. San Jose, CA: National Biometric Test Center, 1999, vol. 1 and 2.
- [55] A. Ross, S. Dass, and A. K. Jain, "A deformable model for fingerprint matching," *Pattern Recognit.*, vol. 38, no. 1, pp. 95–103, Jan. 2005.
- [56] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance evaluation of fingerprint verification systems," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 1, pp. 3–18, Jan. 2006.
- [57] C. Wilson, A. R. Hicklin, H. Korves, B. Ulery, M. Zoepfl, M. Bone, P. Grother, R. J. Micheals, S. Otto, and C. Watson, Fingerprint vendor technology evaluation 2003: summary of results and analysis report NIST Internal Rep. 7123, Jun. 2004 [Online]. Available: http://fpvte.nist.gov/report/ir_7123_summary.pdf
- [58] P. J. Philips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone, FRVT2002: overview and summary [Online]. Available: <http://www.frvt.org/FRVT2002/documents.htm>.
- [59] D. A. Reynolds, W. Campbell, T. Gleason, C. Quillen, D. Sturim, P. Torres-Carrasquillo, and A. Adami, "The 2004 MIT Lincoln laboratory speaker recognition system," in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing*, Philadelphia, PA, Mar. 2005.
- [60] U. Uludag, A. Ross, and A. K. Jain, "Biometric template selection and update: a case study in fingerprints," *Pattern Recognit.*, vol. 37, no. 7, pp. 1533–1542, Jul. 2004.
- [61] D. A. Stoney, "A quantitative assessment of fingerprint individuality," Ph.D. dissertation, Univ. California, Davis, 1985.
- [62] A. Juels and M. Sudan, "A fuzzy vault scheme," One-page abstract appeared in, A. Lapidot and E. Teletar, Eds., *Proc. IEEE Int. Symp. Inform. Theory* p. 408 Lausanne, Switzerland, 2002.
- [63] U. Uludag, S. Pankanti, and A. Jain, "Fuzzy vault for fingerprints," in *Proc. Audio- and Video-based Biometric Person Authentication*, Rye Brook, NY, Jul. 2005, pp. 310–319, 310–319.
- [64] A. Ross and A. K. Jain, "Biometric sensor interoperability: A case study in fingerprints," *Proc. Int. ECCV Workshop Biometric Authentication (BioAW)*, vol. 3087, Lecture Notes Comput. Sci., pp. 134–145, May 2004.
- [65] S. C. Dass, K. Nandakumar, and A. K. Jain, "A principled approach to score level fusion in multimodal biometric systems," in *Proc. 5th Int. Conf. Audio- and Video-Based Biometric Person Authentication*, Rye Brook, NY, Jul. 20–22, 2005, pp. 1049–1058.
- [66] P. Griffin, Optimal Biometric Fusion for Identity Verification Identix Corporate Res. Ctr. Preprint RDNJ-03-0064, 2004.
- [67] A. K. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern Recognit.*, vol. 38, no. 12, pp. 2270–2285, Dec. 2005.
- [68] G. Oestreicher-Singer and A. Sundararajan, "Are digital rights valuable? Theory and evidence from the eBook industry," in *Proc. 25th Int. Conf. Information Systems*, Washington, D.C., Sep. 2004, pp. 533–545.
- [69] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, *Guide to Biometrics*. New York: Springer, 2004.
- [70] J. P. Campbell, "Speaker recognition: a tutorial," *Proc. IEEE*, vol. 85, no. 9, pp. 1437–1462, Sep. 1997.
- [71] L. Ma, T. Tan, D. Zhang, and Y. Wang, "Personal identification based on iris texture analysis," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 12, pp. 1519–1533, Dec. 2003.
- [72] R. Wildes, "Iris recognition: an emerging biometric technology," *Proc. IEEE*, vol. 85, no. 9, pp. 1348–1363, Sep. 1997.
- [73] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proc. IEEE*, vol. 91, no. 12, pp. 2019–2040, Dec. 2003.
- [74] A. Adler, "Can images be regenerated from biometric templates?," presented at the Proc. Biometrics Consortium Conf., Washington, D.C., Sep. 22–24, 2003.
- [75] International Biometric Group, "Independent Testing of Iris Recognition Technology May 2005 [Online]. Available: http://www.biometric-group.com/reports/public/reports/ITIRT_report.htm.

- [76] F. Solina, P. Peer, B. Batagelj, S. Juvan, and J. Kovac, "Color-based face detection in the '15 seconds of fame' art installation," in *Proc. Mirage, Conf. Computer Vision/Computer Graphics Collaboration for Model-Based Imaging, Rendering, Image Analysis and Graphical Special Effects*, Rocquencourt, France, Mar. 10–11, 2003, pp. 38–47, INRIA.
- [77] A. J. Mansfield and J. L. Wayman, Best Practices in Testing and Reporting Performance of Biometric Devices ver. 2.1, National Physics Laboratory Tech. Rep., U.K., Aug. 2002.
- [78] J. Phillips, A. Martin, C. Wilson, and M. Przybocki, "An introduction to evaluating biometric systems," *IEEE Comput.*, vol. 33, no. 2, pp. 56–63, Feb. 2000.
- [79] J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Eds., *Biometric Systems: Technology, Design and Performance Evaluation*. New York: Springer Verlag, 2005.
- [80] D. Black, *The Theory of Committees and Elections*, 2nd ed. London, U.K.: Cambridge Univ. Press, 1963.
- [81] S. Katzenbeisser and F. A. P. Petitcolas, Eds., *Information Hiding Techniques for Steganography and Digital Watermarking*. Boston, MA: Artech House, 2000.
- [82] A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*. New York: Springer, 2006.



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

He is a University Distinguished Professor in the Departments of Computer Science and Engineering at Michigan State University, East Lansing. He was the Department Chair during 1995–1999. His research interests include statistical pattern recognition, data clustering, texture analysis, document image understanding, and biometric authentication. He is the author of a number of books: *Biometric Systems, Technology, Design, and Performance Evaluation* (Springer, 2005), *Handbook of Face Recognition* (Springer, 2005), *Handbook of Fingerprint Recognition* (Springer, 2003) (received the PSP award from the Association of American Publishers), *BIOMETRICS: Personal Identification in Networked Society* (Kluwer 1999), *3D Object Recognition Systems* (Elsevier, 1993), *Markov Random Fields: Theory and Applications* (Academic Press, 1993), *Neural Networks and Statistical Pattern Recognition* (North-Holland, 1991), *Analysis and Interpretation of Range Images* (Springer-Verlag, 1990), *Algorithms For Clustering Data* (Prentice-Hall, 1988), and *Real-Time Object Measurement and Classification* (Springer-Verlag, 1988).

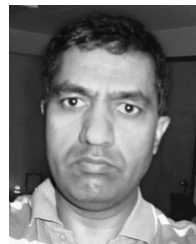
Dr. Jain received awards for best papers in 1987 and 1991, and for outstanding contributions in 1976, 1979, 1992, 1997, and 1998 from the Pattern Recognition Society. He also received the 1996 IEEE TRANSACTIONS ON NEURAL NETWORKS Outstanding Paper Award. He was the Editor-in-Chief of

the IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE from 1991 to 1994. He is a Fellow of the ACM, AAAS, SPIE, and the International Association of Pattern Recognition (IAPR). He received a Fulbright Research Award, a 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) and received the 2003 IEEE Computer Society Technical Achievement Award. He holds six patents in the area of fingerprint matching. He is an associate editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and is currently a member of the study team on Whither Biometrics being conducted by the National Academies (CSTB).



Arun Ross (M'04) 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.

Currently, he is an Assistant Professor in the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown. From 1996 to 1997, he was with the Design and Development Group of Tata Elxsi (India) Ltd., Bangalore, India. He also spent three summers (2000–2002) with the Imaging and Visualization Group at Siemens Corporate Research, Inc., Princeton, NJ, working on fingerprint recognition algorithms. His research interests include pattern recognition, classifier combination, machine learning, and computer vision.



Sharath Pankanti (SM'98) received the Ph.D. degree from the Department of Computer Science, Michigan State University, East Lansing, in 1995.

He joined IBM T. J. Watson Research Center in 1995. He worked on the IBM Advanced Identification Project until 1999. During 2000–2001, he worked on "footprints"—a system for tracking people based on their infrared emission. From 2001 to 2003, he worked on PeopleVision, a system for detecting and tracking individuals in indoor and outdoor environments. From 2003 to 2004, he worked on large-scale biometric indexing systems and since 2005, has been working on human interface designs for effective security and convenience. He has co-edited a comprehensive book on biometrics *Biometrics: Personal Identification* (Kluwer, 1999) and coauthored *A Guide to Biometrics* (Springer, 2004).