Fingerprint-Based Recognition

Sarat C. DASS

Department of Statistics & Probability
Michigan State University
East Lansing, MI 48824
(*sdass@msu.edu*)

Anil K. JAIN

Department of Computer Science & Engineering
Michigan State University
East Lansing, MI 48824
(*jain@msu.edu*)

Biometric recognition, or biometrics, refers to the authentication of an individual based on her or his biometric traits. Among the various biometric traits (e.g., face, iris, fingerprint, voice), fingerprint-based authentication has the longest history, and it has been successfully adopted in both forensic and civilian applications. Advances in fingerprint capture technology have resulted in new large-scale civilian applications (e.g., US–VISIT program); however, these systems still encounter difficulties due to various noise factors present in operating environments. The purpose of this article is to give an overview of fingerprint-based recognition and discuss research opportunities for making these systems perform more effectively.

KEY WORDS: Classification and indexing; Fingerprint feature extraction; Fingerprint individuality; Fusion.

1. INTRODUCTION

Biometric recognition, or biometrics, refers to the automatic authentication of a person based on his or her physiological or behavioral characteristics (Jain, Bolle, and Pankanti 1999a; Maltoni, Maio, Jain, and Prabhakar 2003). Biometric recognition offers many advantages over traditional personal identification number or password and token-based (e.g., ID cards) approaches; for example, a biometric trait cannot be easily transferred, forgotten, or lost; the rightful owner of the biometric template can be easily identified; and it is difficult to duplicate a biometric trait. Some well-known examples of traits used in biometric recognition are fingerprint, iris, face, signature, voice, hand geometry, retina, and ear (Fig. 1). A number of commercial recognition systems based on these traits have been deployed and are currently in use. Biometric technology has now become a viable and more reliable alternative to traditional authentication systems in many government applications (e.g., US–VISIT program and the proposed e-biometric passport, which is capable of storing biometric information of the owner in a chip inside the passport). With increasing applications involving human–computer interactions, there is a growing need for fast authentication techniques that are reliable and secure. Biometric recognition is well positioned to meet the increasing demand for secure and robust systems.

Several requirements need to be met by a particular biometric trait to be considered for use in an authentication system. These requirements are (a) universality, that each individual should possess the trait; (b) distinctiveness, that the trait for two different persons should be sufficiently different to distinguish between them; (c) permanence, that the trait characteristics should not change, or change minimally, over time; and (d) collectability, that the trait can be measured quantitatively. However, for practical biometric systems, some other considerations are important, namely (a) whether the performance and authentication rates of the system are at acceptable levels, measured in terms of speed, recognition accuracy and robustness, in different operational environments; (b) whether the biometric trait will be widely accepted by the public for use in their daily lives; and (c) whether the system based on the trait can be easily attacked or spoofed. The main requirements of a practical biometric system are that it have acceptable recognition performance rates, recognition speed, and cost. In addition, it should protect the user from privacy intrusions and be robust with respect to various spoofing attacks.

Among all of the biometric traits used for authentication, fingerprint-based recognition has the longest history (almost 100 years) and has been successfully adopted not only in forensic applications, but also in an increasing number of civilian applications (e.g., the US–VISIT program). The reason behind this success is because fingerprints generally meet the requirements of a biometric trait discussed in the previous paragraph. Table 1 compares commonly used biometric traits in terms of these requirements. Due to the wide appeal of fingerprints, fingerprint-based authentication systems continue to dominate the biometrics market, accounting for almost 52% of current authentication systems based on biometric traits (Maltoni et al. 2003). The rapid evolution of mobile commerce (m-commerce) and banking (m-banking) services in recent years has placed new emphasis on user ID technology and created widespread deployment of biometrics in this field. Several mobile manufacturers have incorporated fingerprint, voice, and face biometrics into high-end mobile phones (Fig. 2). New and miniaturized fingerprint sensors capable of being embedded in a mobile phone have been developed to meet the demands of m-commerce and m-banking applications. In contrast to traditional two-dimensional array sensors, these new one-dimensional line scan sensors require that the finger be swiped to acquire a fingerprint impression for recognition.

A biometric system is essentially a pattern recognition system that recognizes an individual by comparing the input biometric trait with a set of traits stored in a database (i.e., templates). The templates are obtained during the enrollment stage, where these traits along with an ID are collected from users and stored in a database. An important issue in designing a biometric system is to ascertain how recognition will be performed. The two modes of recognition are verification and identification. In a verification system, recognition is performed by comparing the input biometric characteristics with the characteristics of a claimed identity (1 to 1 match) stored in the database.

TECHNOMETRICS, AUGUST 2007, VOL. 49, NO. 3
DOI 10.1198/004017007000000272

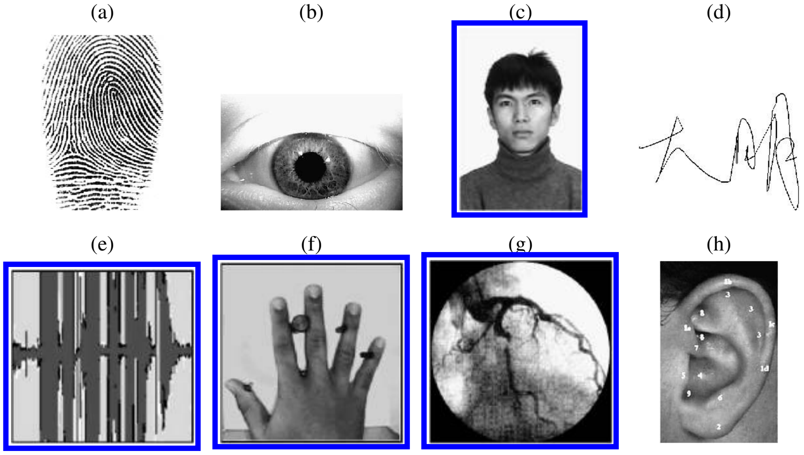

Figure 1. Some examples of biometric traits (Jain et al. 1999a): (a) fingerprint, (b) iris scan, (c) face scan, (d) signature, (e) voice, (f) hand geometry, (g) retina, and (h) ear.

Thus a verification system either accepts or rejects the claimed identity depending on whether or not the biometric characteristics of the input and that of the claimed identity are similar to one another. In the identification mode, however, a claimed identity is not available. The system recognizes an individual by performing an exhaustive search (1 to M matches) in the entire database of M stored templates. Thus in the identification mode, the system establishes an identity without the subject having to provide one. Figure 3 shows the important processing tasks involved in the enrollment, verification, and identification stages of a fingerprint-based authentication system.

For a system operating in the verification mode, we are interested in accepting inputs (i.e., queries) that are "close" or "similar" to the template of the claimed identity and rejecting those that are "far" or "dissimilar." Based on the input Q and a claimed identity I_c, we are interested in testing the hypothesis

$$H_0 : I_t = I_c \qquad \text{versus} \qquad H_1 : I_t \neq I_c, \tag{1}$$

where I_t is the true identity of the user. In (1), H_0 (resp. H_1) is the null (alternative) hypothesis that the user is genuine (impostor). Based on the claimed identity I_c, a template T is retrieved from the database. Subsequently, the testing in (1) is performed by a matcher that computes a similarity measure, $S(Q, T)$, based on Q and T; large (resp. small) values of S indicate that T and Q are close to (far from) each other. A threshold, λ, is specified so that all similarity values lower (resp. greater) than λ lead to the rejection (acceptance) of H_0. Thus decisions of whether to accept or reject H_0 in the verification mode are prone to two types of errors: the false reject rate (FRR), which is the probability of rejecting H_0 when in fact the user is genuine, and the false accept rate (FAR), which is the probability of accepting H_0 when in fact the user is an impostor. The genuine accept rate (GAR), given by $1 - \text{FRR}$, is the probability that the user is accepted given that he or she is genuine. Both the FRR (and hence GAR) and the FAR are functions of the threshold value λ [see Fig. 4(a)]. The receiver operating curve (ROC) is a graph that expresses the relationship between the FAR versus GAR when λ varies, that is,

$$\text{ROC}(\lambda) = (\text{FAR}(\lambda), \text{GAR}(\lambda)), \tag{2}$$

and is commonly used to report the performance of a biometric authentication system [Figs. 4(a) and 4(b)]. Note that the ROC curve is a nondecreasing function of FAR with $\text{ROC} = 0$ when $\text{FAR} = 0$ and $\text{ROC} = 1$ when $\text{FAR} = 1$. Two biometric systems

Table 1. Comparison of selected biometric technologies adapted from Maltoni et al. (2003)

Biometric trait	UVSL	DSTC	PRMN	CLTB	PRFM	ACPT	CRVN
DNA	H	H	H	L	H	L	L
Face	H	L	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
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

NOTE: H, M, and L denote high, medium, and low. UVSL, universality; DSTC, distinctiveness; PRMN, permanence; CLTB, collectability; PRFM, performance; ACPT, acceptability; CRVN, circumvention. As shown, fingerprint has medium universality, high distinctiveness, high permanence, medium collectability, high performance, medium acceptability, and medium circumvention.

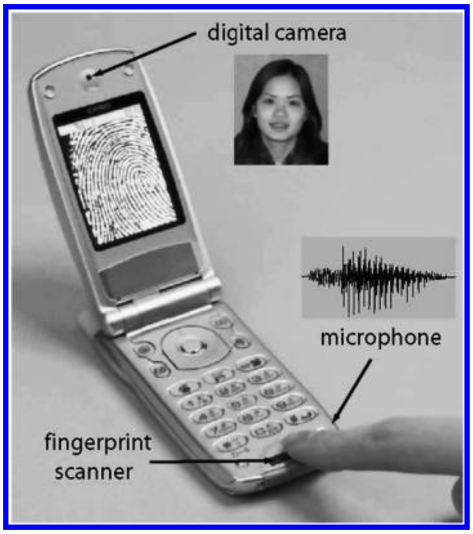

Figure 2. Fingerprint, voice, and face biometric-based recognition in high-end mobile phones.

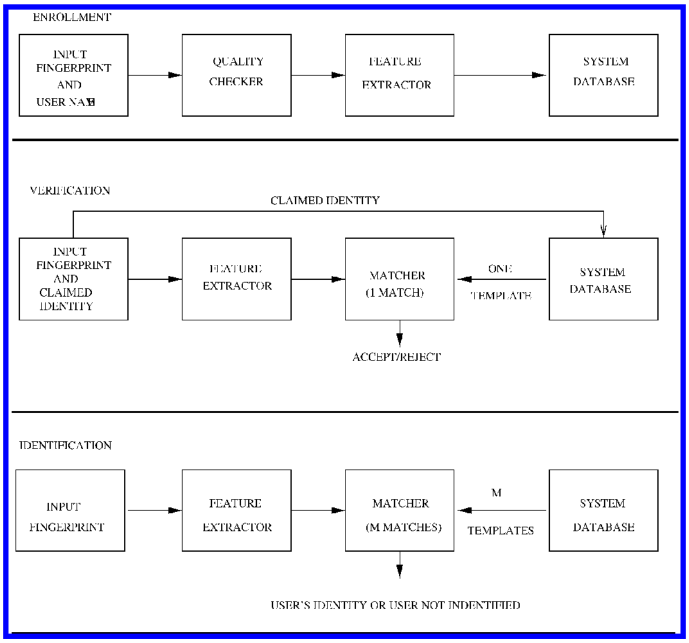

Figure 3. Schematic diagram showing the processing tasks involved in the enrollment, verification, and identification modes of a fingerprint-based authentication system.

can be compared in terms of their ROC curves; system 1 is said to be better than system 2 in the FAR range $[p_0, p_1]$ if their ROCs satisfy

$$\mathrm{ROC}_1(p) \geq \mathrm{ROC}_2(p) \tag{3}$$

for all $p \in [p_0, p_1]$ with strict inequality for at least one such p. Another popular performance measure is the equal error rate (EER), defined as the common value of FAR(λ^*) and FRR(λ^*) for the threshold λ^* that makes FAR(λ^*) equal to FRR(λ^*).

Although it can be argued that fingerprints represent one of the best biometric traits, the performance of fingerprint-based authentication systems in many cases does not meet the desired levels of accuracy. For example, in the fingerprint verification competition FVC 2002, the best-performing algorithm had an EER of .1% (Maio, Maltoni, Cappelli, Wayman, and Jain 2002), whereas 2 years later in FVC 2004 (Maio et al. 2004), the best-performing algorithm had an EER of 2%. The drop in performance rate was caused by the fact that the fingerprint database used in FVC 2004 was more challenging than that used in FVC 2002. The drop in performance also reflects real operating environments, which are affected by large intraclass and small interclass variability, resulting in far from perfect performance of these systems. Large intraclass variability refers to the situation in which fingerprints from the same individual look very different from one another. For example, the variability in placement of a finger on the sensing surface gives rise to finger impressions that are rigid transformations (i.e., rotation and translation) of one another in the two-dimensional plane and causes a large intraclass variability. Other factors include uneven skin elasticity and finger pressure that give rise to nonlinear distortions in the sensed image (Fig. 5). Extraneous factors such as sensor noise, sensing environments, and the condition of the finger itself (e.g., cuts on a finger) constitute sources of variability that effect the quality of the acquired impressions. It is well known that the fingerprint features lose their ability to discriminate when the underling quality of the image is poor. Consequently, these noise sources also have the effect of increasing the intraclass variability among multiple acquisitions of fingerprints for the same individual. Small interclass variability refers to the case when fingerprints from different individuals look very similar to one another; Figure 6 provides an example.

It is important to note that these noisy input images cause fingerprint-based authentication systems to make mistakes, which can have serious consequences for the general public. In the case of Brandon Mayfield (Federal Bureau of Investigation 2004; Thompson and Cole 2005), a wrong fingerprint match based on a latent lifted from the Madrid train bombing scene resulted in his wrongful imprisonment for 19 days. Incidents such as this emphasize the need for research for further improving the performance of these authentication systems.

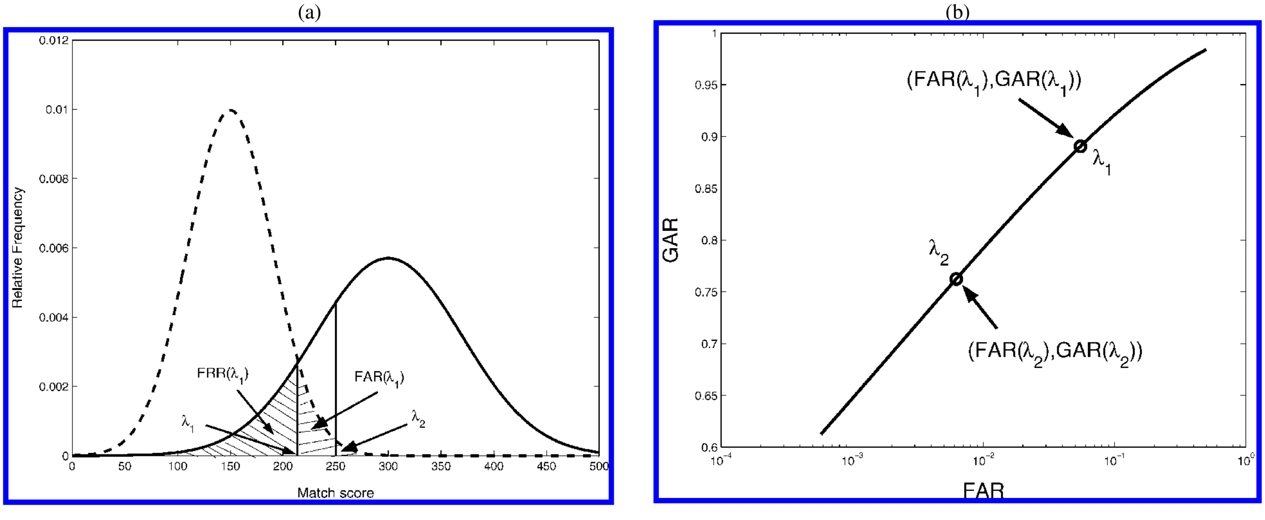

Figure 4. Obtaining the ROC curve by varying the threshold λ on the match scores (Dass, Zhu, and Jain 2006a). (a) The FRR and FAR corresponding to a threshold λ_1. λ_2 is another threshold different than λ_1. (b) The ROC curve obtained when λ varies. The values of (FAR, GAR) on the ROC curve corresponding to the thresholds λ_1 and λ_2 are shown.

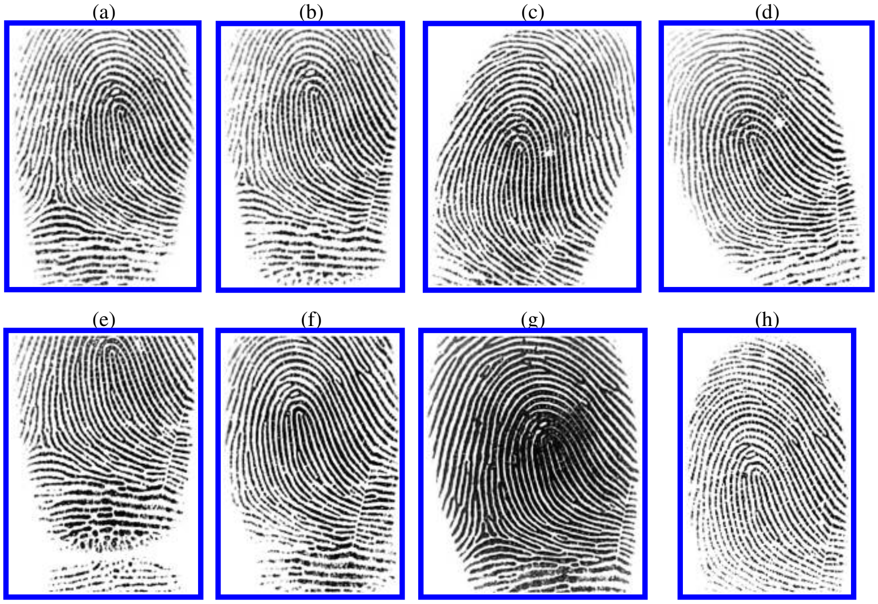

Figure 5. Eight different impressions of the same finger showing the intraclass variability due to finger placement and nonlinear distortions caused by skin elasticity. Source: FVC 2002 DB1 database.

As illustrated in Figure 3, a fingerprint-based authentication system goes through several intermediate processing tasks before deciding the outcome of the matching algorithm. The outcome of each intermediate task and the final decision are affected by one or more sources of noise mentioned above. In this article we give an overview of four major tasks of fingerprint-based authentication systems—feature extraction, indexing, individuality, and fusion—and discuss methods that have been developed to perform these tasks effectively. We point out the current challenges in these four areas and discuss work that has been done to further enhance the performance of fingerprint-based recognition systems.

2. FINGERPRINT FEATURE EXTRACTION

Two fingerprint images from the NIST Special Database 4 (*http://www.nist.gov/srd/nistsd4.htm*) are shown in Figure 7. These images are of size 512×512 (pixels^2), with gray intensities at each pixel ranging from 0 (darkest) to 255 (lightest). Note that alternating dark and light flow lines traverse the entire fingerprint area, termed ridges and valleys. Occasionally, the ridges and valleys either form patterns of very high curvature or meet at a point from three different directions. These points are termed singularities. Figure 7 shows all of the important characteristics, or fingerprint features, typically present in a fingerprint image. These features can be categorized into two main groups, global and local. The global features in a fingerprint image consist of the information on ridge flow and the location and type of singularities. A singularity of type “core” is localized at the innermost point with the highest curvature of a sequence of alternating ridges and valleys, whereas the “delta” is localized at the confluence of three different ridge flow directions. Local or fine fingerprint features arise due to anomalies in the ridge flow. The most common type of anomaly, termed minutiae, consists of breaks (endings) and bifurcations in the ridges. Thus information from a minutiae consists of its spatial location (where the break or bifurcation occurs), type (either bifurcation or ending), and direction (i.e., the direction of ridge flow at that minutiae location). Most fingerprint-based authentication systems use information extracted from minutiae bifurcation and endings, as well as the ridge flow and singularities, to assess the degree of similarity between two fingerprints.

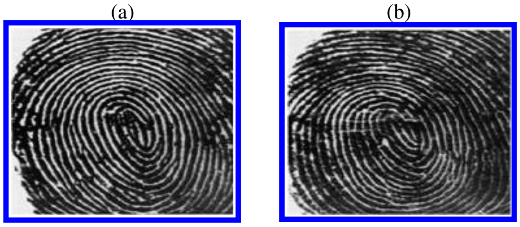

Figure 6. Illustrating small interclass variability: Two fingerprint impressions with similar characteristics from two different fingers.

Information on the ridge flow is obtained through the directional field, that is, the set consisting of the direction of flow of the ridges at each pixel (or a block of pixels) in the fingerprint image. Thus the ridge flow direction at every pixel consists of an angle θ indicating the direction of flow with respect to the x-axis. Because opposite ridge flow directions are equivalent, θ is determined uniquely only in $[0, \pi]$. Obtaining fast and reliable estimates of the directional field has been the focus of many previous research efforts; these include methods based on neural networks (Wilson, Candela, and Watson 1994), filter-based approaches (O’Gorman and Nickerson 1987), and gradient-based approaches (Rao 1990; Hong, Wan, and Jain 1998; Jain, Hong, Pankanti, and Bolle 1997; Ratha, Chen, and Jain 1995; Bazen and Gerez 2002). Extraction of the directional field is prone to various noise factors. For example, cuts and bruises on the fingertip can create disruptions in the ridge flow, whereas low moisture content of the fingertip causes random ridge breaks that distort the extraction process. The detection

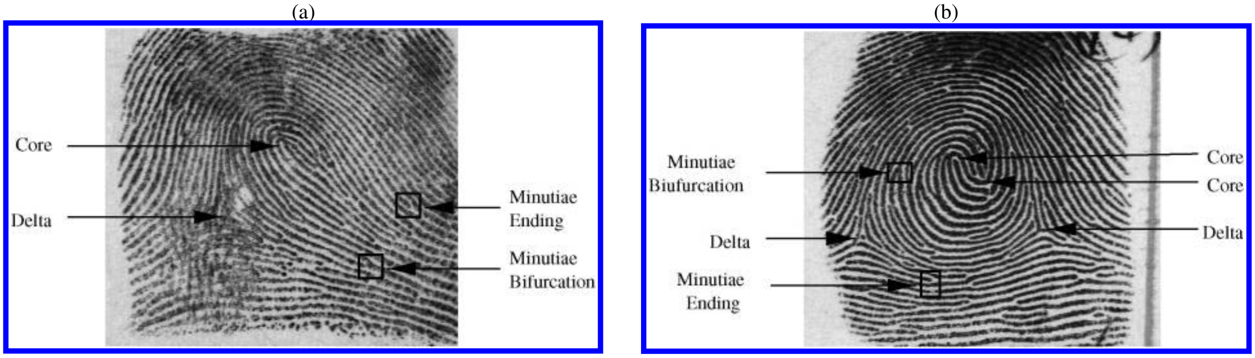

Figure 7. Two examples of fingerprint images showing the salient features used for authentication.

of singularities also has been addressed in many previous studies. Finding regions of high curvature and subsequently classifying a feature vector into core, delta, or a reject class was the approach taken by Nakamura, Goto, and Minami (1982) and Srinivasan and Murthy (1992). Rao and Jain (1992) used a geometric theory of differential equations to derive signal-to-symbol representations in the flow field domain for cores and deltas. Perona (1998) used the local energy of the directional field in a neighborhood of a block of pixels was used to measure how closely it resembles a flow field around singularities. Jain, Prabhakar, Hong, and Pankanti (2000) used a ratio of sines of directional fields in two adjacent regions to detect singularities, whereas Bazen and Gerez (2002) used a scheme for detecting singularities based on the Poincare index. Dass (2004) obtained a more robust directional field and singularity extraction algorithm by eliciting statistical models that account for the natural smoothness of spatial ridge flows. We describe this approach in greater detail later.

For the gray intensity image $I(x, y)$ over a rectangular domain, we wish to recover its directional field. The fundamental image attributes for this purpose are the sitewise image intensity gradients denoted by $\mu_s = (\frac{\partial I}{\partial x}, \frac{\partial I}{\partial y})^T$ for each site $s = (x, y)$. Also let ν_s denote the normalized version of μ_s, so that $\|\nu_s\| = 1$. It is common in the image processing literature to analyze blocks of sites, instead of individual sites, to remove noise and achieve faster processing speed. For a block B with image intensity gradients μ_s, $s \in B$, our objective is to recover the principal gradient direction of block B, denoted by the unit vector l_B, which represents the dominant direction of the μ_s, $s \in B$. Once l_B is obtained, the directional field for block B, DF_B, is taken to be the unit vector orthogonal to l_B, namely

$$DF_B = l_B^{\perp}. \tag{4}$$

The main challenge here is that gradients μ_s with opposite signs should reinforce, not cancel out each other (see, e.g., Fig. 8). This criteria is satisfied if the distribution of ν_s given l_B (thus the likelihood of l_B) has the form

$$\ell_B(l_B \mid \nu_s, s \in B) = \prod_{s \in B} C(\tau_s) \cdot \exp\{\tau_s d(\nu_s, l_s)\}, \tag{5}$$

where

$$d(\nu, l) = (\nu^T l)^2 \tag{6}$$

measures the degree of similarity between ν and l, τ_s denotes the precision, and $C(\tau_s)$ is the normalizing constant (independent of l_B). For the collection of all blocks, $\mathcal{B}$, the likelihood of $l_B, B \in \mathcal{B}$ is obtained through independence as

$$\begin{aligned}\ell(l_B, B \in \mathcal{B}) &= \prod_{B \in \mathcal{B}} \big(\ell_B(l_B \mid \nu_s, s \in B)\big)^{w_B} \\ &= \prod_{B \in \mathcal{B}} \prod_{s \in B} (C(\tau_s))^{w_B} \cdot \exp\{w_B \tau_s d(\nu_s, l_s)\}, \end{aligned} \tag{7}$$

where w_B is the weight given to block B. Dass (2004) discussed the choices of (a) $\tau_s = \|\mu_s\|^2$ within each block B and (b) w_B = coherence of block B as a measure of influence of block B in $\mathcal{B}$. The implication of (a) is that gradients with larger magnitudes are more influential in the recovery of l_B in block B, whereas (b) gives more weight to blocks with larger coherence (i.e., when all of the μ_s's point in the same direction, up to the ± sign, as opposed to being randomly distributed). Based on (7), the maximum likelihood estimate of l_B, $\hat{l}_B$, can be shown to be the unit eigenvector corresponding to the maximum eigenvalue of

$$A_B = \sum_{s \in B} \tau_s \nu_s \nu_s^T. \tag{8}$$

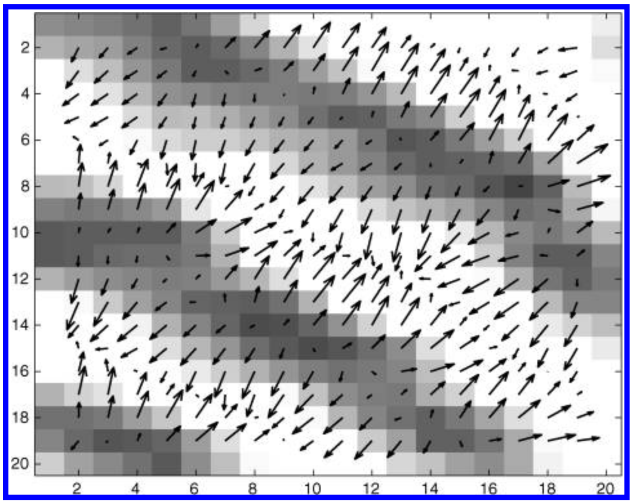

Figure 8. An example of a fingerprint image block with gradient directions and magnitudes indicated by arrowheads and lengths.

Subsequently, the directional field estimate, $\hat{DF}_s = \hat{l}_B^{\perp}$, is precisely the well-known Rao estimate of the directional field reported in the literature (see, e.g., Bazen and Gerez 2002; Rao 1990). Note that the weights w_B do not influence this estimate of the directional field, because we are assuming that the blocks are independent of one another. However, the weights w_B, will be influential when we incorporate spatial dependence between neighboring blocks. We will pursue this later.

One drawback of Rao's estimator is that it is highly susceptible to noise factors, thus requiring several postprocessing stages to satisfactorily smooth out the errors. To alleviate the problem with Rao's estimator, Dass (2004) incorporated spatial smoothness of the principal gradient directions in neighboring blocks to achieve a more robust estimator of the directional field. More specifically, a Markovian prior of the form

$$\pi(l_B, B \in \mathcal{B}) = C(\alpha) \cdot \exp\left\{\lambda \sum_{B \sim B'} w_{BB'} d_\alpha(l_B, l_{B'})\right\} \tag{9}$$

is assumed on the collection $\{l_B, B \in \mathcal{B}\}$, where $d_\alpha(l, m) = |l^T m|^\alpha$ for a positive constant α, the notation $\sum_{B\sim B'}$ represents the sum over all blocks B and B' that are neighbors of one another in a neighborhood structure specified by Dass (2004), $w_{BB'}$ are nonnegative weights measuring the influence of the block pair (B, B') in the overall summation, and λ measures the degree of spatial smoothness, with large (small) values of λ indicating that neighboring l_B values are similar (dissimilar). Subsequently, the posterior distribution of l_B, $B \in \mathcal{B}$, is given by the density

$$\pi(l_B, B \in \mathcal{B} \mid \text{data}) \propto \exp\left\{\sum_{B\in\mathcal{B}} w_B(l_B^T A_B l_B) + \lambda \sum_{B\sim B'} w_{BB'} d_\alpha(l_B, l_{B'})\right\}. \tag{10}$$

The maximum a posteriori (MAP) estimate of $l_B, B \in \mathcal{B}$, is obtained by maximizing the posterior (10) with respect to l_B, $B \in \mathcal{B}$. Details of the iterative procedure developed to find the MAP estimate were reported by Dass (2004), along with an investigation into the properties of the extracted field for different choices of α, block size, and smoothing parameter λ. Once the MAP estimate $l_{B,MAP}$ is found, the estimate of the directional field is taken to be

$$DF_{B,MAP} = l_{B,MAP}^{\perp}. \tag{11}$$

The singularity detection algorithm of Dass (2004) uses reference parametric templates for the core (C) and delta (D) and checks to see whether the extracted directional field around a point is close to one of the templates. For a window of size $w \times w$ centered at $(0, 0)$, the parametric templates are obtained using

$$DF_{(x,y)}(C) = \begin{pmatrix}\cos(\theta_1/2)\\ \sin(\theta_1/2)\end{pmatrix} \quad \text{and} \quad DF_{(x,y)}(D) = \begin{pmatrix}\cos(\theta_2/2)\\ \sin(\theta_2/2)\end{pmatrix}, \tag{12}$$

where (r_1, θ_1) and (r_2, θ_2) are the polar representations of $(y, -x)$ and $(-y, -x)$. Figure 9 shows the reference parametric templates for the core and delta for a window of size 17 × 17. Now consider a singular point of type $S = \{C, D\}$ centered at $u_0 = (x_0, y_0)$ and rotated ξ degrees with respect to the horizontal axis. In this case the parametric directional field vector is given by

$$DF_u(S, \xi) \equiv \begin{pmatrix}\cos(\xi) & -\sin(\xi)\\ \sin(\xi) & \cos(\xi)\end{pmatrix} \cdot DF_{u^*}(S) \tag{13}$$

for each $u = (x, y)$, where $u^* = (x^*, y^*)$ with $x^* = (x - x_0)\cos(\xi) + (y - y_0)\sin(\xi)$ and $y^* = -(x - x_0)\sin(\xi) + (y -$

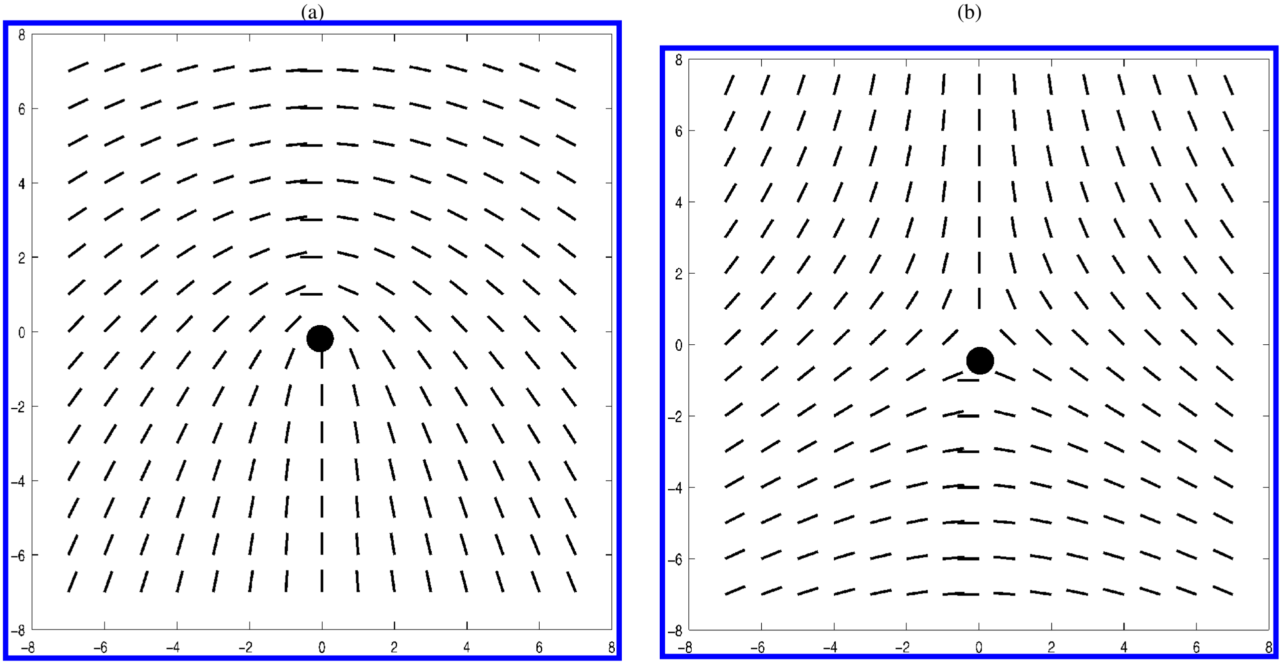

Figure 9. The directional field around singularities based on reference templates for core (a) and delta (b) (Dass 2004). The location of the singularity is indicated by a black dot in the center of each image.

$y_0)\cos(\xi)$, and $DF_{u^*}(S)$ is as given in (12). To assess the closeness of the extracted directional field, $DF_{u,MAP}$ [see (11)], to that of $DF_u(S,\xi)$ in a $w \times w$ window $\mathcal{W}_{u_0}$ centered at u_0, the function

$$f(S,\xi;u_0) = \frac{1}{w^2}\sum_{u\in\mathcal{W}_{u_0}} d\big(DF_{u,MAP}, DF_u(S,\xi)\big) \qquad (14)$$

is evaluated with d defined as in (6). Large values of f indicate that the extracted field $DF_{u,MAP}$ around u_0 matches that of $DF_u(S,\xi)$ and suggests the presence of a singularity at u_0. However, the rotation angle ξ is not known in practice and must be estimated. The estimate of ξ is taken to be $\hat{\xi}$, which maximizes $f(S,\xi;u_0)$ for each S-template model, that is,

$$\hat{\xi} = \arg\max_{\xi} f(S,\xi;u_0) \qquad (15)$$

with

$$\hat{f}(S;u_0) = f(S,\hat{\xi};u_0). \qquad (16)$$

The details pertaining to the estimation of ξ have been given by Dass (2004). The value of $\hat{f}(S;u_0)$ represents the best value of similarity of the extracted directional field, with the directional field specified by the S-template model rotated at angle $\hat{\xi}$ with respect to the horizontal axis. The function $\hat{f}(S;u_0)$ is evaluated for all blocks of sites u_0 in a fingerprint image. The maximum of $\hat{f}(C;u_0)$ and $\hat{f}(D;u_0)$ is then determined and compared with a prespecified threshold T_0, where $0 < T_0 < 1$. A singularity is said to be present at u_0 if this maximum is greater than T_0, with singularity type and orientation taken to be those corresponding to the maximum. If the maximum is less than T_0, then no singularity is detected at u_0.

One advantage of the template-based singularity extraction algorithm is that fewer numbers of spurious singularities are detected compared with previous methods. Dass (2004) combined the algorithm to extract the smooth directional field (10) with singularity detection [see (14)–(16)] to obtain an algorithm that extracts both features simultaneously. Another advantage of the dynamic updating of features is that the directional field can be molded based on current singularity information to detect other singularities in the fingerprint impression. Two examples are presented in Figure 10; note that noisy regions do not adversely effect the extracted field with the addition of smoothness constraints on neighboring directional field values.

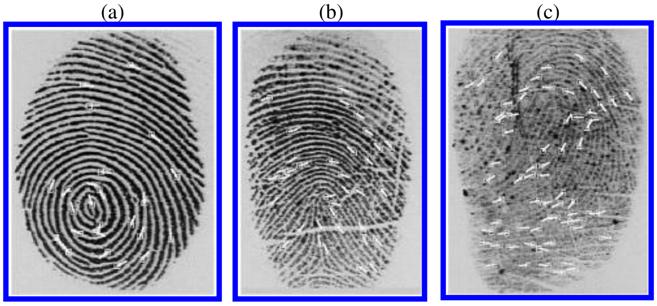

Figure 11. Fingerprint quality (Chen, Dass, and Jain 2005a): (a) good quality, (b) medium quality, (c) poor quality. White boxes and the associated lines indicate locations and directions of detected minutiae. Poor-quality impressions yield higher rates of spurious detection as well as higher rates of missed true minutiae.

Robust detection of ridge ending and bifurcation-type minutiae in a fingerprint is crucial, because most fingerprint-matching algorithms use these two types of minutiae for authentication. Current methods for minutiae detection use some kind of ridge enhancement followed by thinning (i.e., reducing the ridge width to one pixel wide) and detection (Ratha et al. 1995). Nonlinear distortions of the finger caused by uneven fingertip pressure and nonuniform skin elasticity result in spurious minutiae points being detected as well as true minutiae points being missed. Nonlinear distortions also have the effect of changing the type of a minutiae from a bifurcation to an ending or vice versa. Although current authentication systems do some degree of postprocessing of the extracted features, the problems with spurious minutiae, missed true minutiae, and incorrect extraction of minutiae type still exist. With poor-quality images, these problems are further aggravated (Fig. 11). One approach to overcoming the problems associated with incorrect feature extraction is to report confidence measures associated with the extracted minutiae. Current algorithms do not report these values, thus making the contribution of a falsely detected feature in the authentication stage equal to that of a true feature. In addition, errors incurred in the feature-extraction stage propagate to the subsequent matching stage, and thus significantly affect the overall performance of an authentication system.

3. FINGERPRINT CLASSIFICATION AND INDEXING

As mentioned earlier, identification of an individual is a more challenging problem than verification, because no claimed

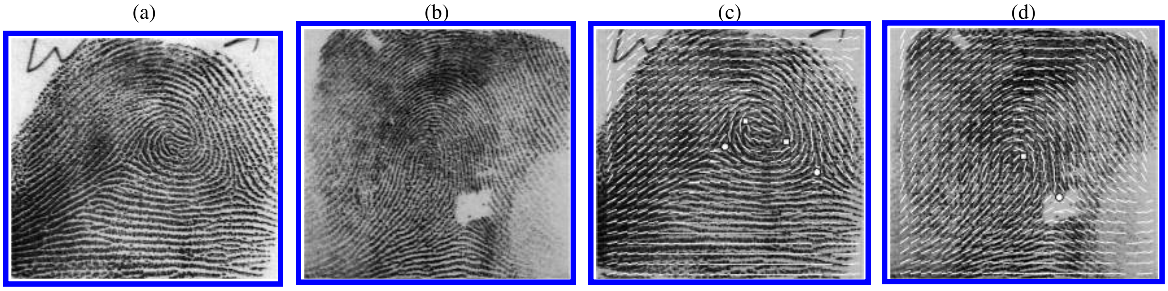

Figure 10. Simultaneous directional field and singularity extraction (Dass 2004): (a) and (b) the original images; (c) and (d) the extracted global features for (a) and (b). Note that the extracted directional field is not affected by the noisy region close to the delta in (b) and (d) due to the imposed smoothness.

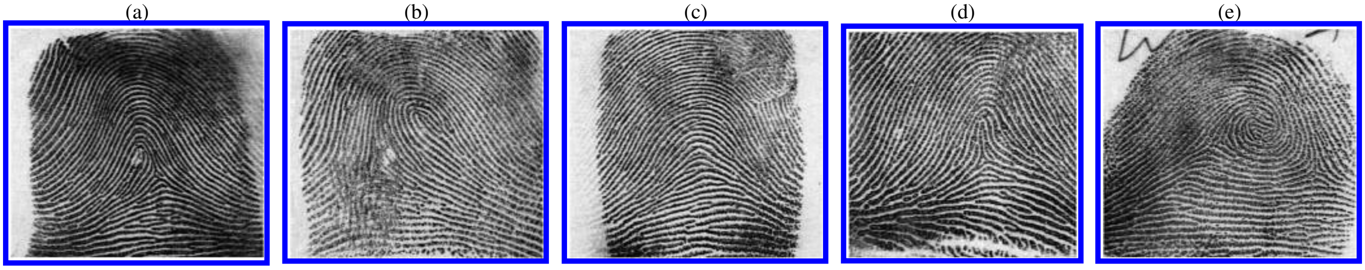

Figure 12. Five major classes of fingerprints in the Henry system of classification: (a) left loop, (b) right loop, (c) arch, (d) tented arch, and (e) whorl. The images are from the NIST database.

identity is provided. Thus the system must perform an exhaustive search on databases to come up with a list of candidate identities (called the top *M* matches). In large-scale government and forensic applications, these databases consist of millions of fingerprints; for example, the FBI database comprises approximately 50 million subjects and 500 million fingerprint images (10 fingers/subject).

Indexing of a fingerprint database refers to the partitioning of the database by means of assigning a label to each fingerprint and grouping fingerprints with identical labels to form a class. Effective indexing procedures reduce search time (and the resulting matching accuracy) during the identification process, because only an appropriate subset of the entire database is searched. There are two main types of indexing approaches: (a) discrete classification, where fingerprints are partitioned into predefined classes according to their macro features, and (b) continuous classification, where each fingerprint is represented by a similarity metric that measures its proximity to some preselected class prototype. The Henry system (Henry 1900) is a well-known example of discrete classification used in many forensic applications. Whereas the Henry classification system has many classes (∼17), almost 99% of the fingerprints belong to five major types: right loop, left loop, whorl, arch, and tented arch. Figure 12 presents typical fingerprint images in the five major classes of the Henry system. The four-class Henry system is derived from the five classes by combining the arch and tented arch fingerprints into a single class, because these two classes are rather difficult to discriminate. There is a significant body of work on automatic classification of fingerprints into the Henry system (see, e.g., Cappelli, Lumini, Maio, and Maltoni 1999; Chang and Fan 2002; Chong, Ngee, Jun, and Gay 1997; Karu and Jain 1996). These approaches can be grouped into five main categories: (a) approaches based on singular points (Karu and Jain 1996), (b) structure-based (Cappelli et al. 1999; Chang and Fan 2002; Chong et al. 1997), (c) frequency-based (Jain et al. 2000), (d) syntactic or grammar-based (Moayer and Fu 1975, 1976a,b), and (e) approaches based on mathematical models (Dass and Jain 2004). Hybrid methods combine at least two approaches in (a)–(e) to arrive at a fingerprint classification algorithm (see, e.g., Chang and Fan 2002; Chong et al. 1997; Dass and Jain 2004). Table 2 compares the classification accuracies obtained by several fingerprint classification methods reported in the literature.

Classifying fingerprints into the Henry system is extremely difficult; the best reported accuracy is only 94.8% (at 5.1% reject rate) for the five-class problem (see Chang and Fan 2002). The difficulty in classifying fingerprints into the Henry system is inherent in the class definitions themselves; sometimes, even human experts assign more than one class label to the same fingerprint because of the ambiguity among the classes (Fig. 13). Another drawback of the Henry system is that fingerprints are unevenly distributed among the five classes: 31.7% for right loop, 33.8% for left loop, 27.9% for whorl, 3.7% for arch, and 2.9% for tented arch. This makes them very inefficient for indexing, because most searches will be conducted in the first three classes.

In a continuous fingerprint classification scheme, there are no fixed classes as in the discrete case. The main idea of a continuous classification scheme is to compute the similarity of an input image to a set of prototypes. Then a search is performed on those fingerprints that have similarity values (as determined by a threshold) close to the computed values. This procedure significantly reduces the number of fingerprints that must be searched, because only the subset of the fingerprints with similarity measures close to the computed values is considered. There are several advantages of continuous classification over discrete schemes. First, the reduction in search time is significant, because only a subset of relevant fingerprints is searched (i.e., images with similarity values close to the input fingerprint). Second, the continuous classification scheme overcomes the difficulties associated with the ambiguity between

Table 2. A comparison of classification accuracies (in %) of several fingerprint classification methods in the literature (Dass and Jain 2004)

Method	No. of fingerprints	Four-class problem	Five-class problem	Reject rate
Cappelli et al.	1,204		87.1[a]	0
Chang and Fan	2,000		94.8	5.1
Chong et al.	89		96.6[b]	0
Hong and Jain	4,000	92.3	87.5	0
Jain et al.	4,000	94.8	90.0	0
Karu and Jain	4,000	91.4	85.4	0
Wilson et al.	4,000		94.0[c]	10.0
Dass and Jain	4,000	94.4		0

NOTE: Reject rates are given in percentages.

[a] Using the natural distribution (based on the following percentages for the five classes: 31.7% for right loop, 33.8% for left loop, 27.9% for whorl, 3.7% for arch, and 2.9% for tented arch) of fingerprints.

[b] Based on the five classes: double loop, whorl, left loop, right loop, and arch.

[c] Using the natural distribution of fingerprints; equal distribution of each class yields accuracies of 84–88%.

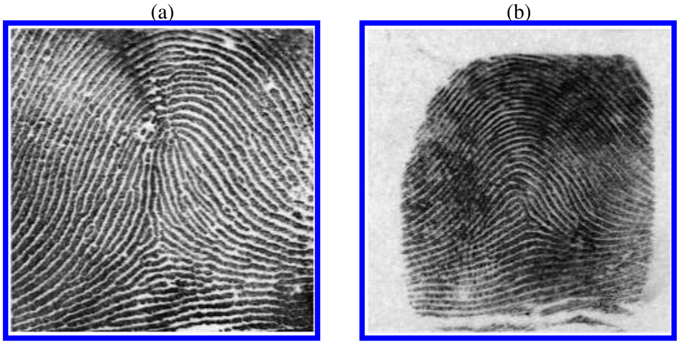

Figure 13. Ambiguous assignment of class in the Henry system. (a) Either right-loop or tented arch. (b) Either left-loop or tented arch. Source: NIST database.

classes in the Henry system. A number of continuous classification schemes have been developed. Cappelli et al. (1999) developed a continuous classification scheme based on partitioning the directional field into several homogeneous regions with respect to the image ridge flow. However, the class prototypes that they chose relate strongly to the basic classes of the Henry system. Other indexing approaches not based on ridge flows were reported by Bhanu and Tan (2003) and Germain, Califano, and Colville (1997). In these approaches, minutiae triplets were generated for an input image, and the features extracted based on the triplets were used for indexing. The performance of an indexing scheme is measured in term of the retrieval accuracy—the probability that the top M matches include the person who provided the input. Bhanu and Tan (2003) achieved an overall retrieval accuracy of 86.5% was achieved for the top ($M = 1$) match. An important point to remember is that retrieval accuracies degrade drastically as a function of image quality, because extraction of features as well as the computation of the similarity measures are affected by noise.

4. THE INDIVIDUALITY OF FINGERPRINTS

Expert testimony based on forensic evidence (e.g., handwriting, fingerprint, hair, bite marks) is delivered in a courtroom by comparing salient features of a latent print lifted from a crime scene with those taken from the defendant. A reasonably high degree of matching between the salient features lead the experts to testify irrefutably that the owner of the latent print and the defendant are one and the same person. For decades, testimony provided by forensic individualization experts was almost never excluded from these cases, and the foundations and basis of this testimony were rarely questioned on cross-examination. Central to establishing an identity based on forensic evidence is the assumption of discernible uniqueness; salient features of different individuals are observably different, and thus when two prints share many common features, the experts conclude that the owner of the two different prints is one and the same person. The assumption of discernible uniqueness (Saks and Koehler 2005), although lacking sound theoretical and empirical foundations, allows forensic experts to offer unquestionable proof of the defendant's guilt, and, to make matters worse, these experts are never questioned on the uncertainty associated with their testimonials (i.e., how frequently would an observable match between a pair of prints lead to errors in the identification of individuals). Thus discernible uniqueness precludes the opportunity to establish error rates that would be known from collecting population samples, analyzing the inherent feature variability, and reporting the corresponding probability of two different persons sharing a set of common features.

A significant break from this trend occurred in the case of Daubert vs. Merrell Dow Pharmaceuticals (1993), where the U.S. Supreme Court ruled that for expert forensic testimony to be allowed in a court case, it had to be subject to three main criteria of scientific validation: whether the particular tool or methodology in question (a) has been tested, (b) has been subject to peer review, and (c) has known error rates. Following Daubert, fingerprint identification was first challenged in the case of U.S. v. Byron Mitchell (1999) under the fundamental premise that the uniqueness of fingerprints had not been objectively tested and thus matching error rates were unknown. Based on the outcome of U.S. v. Byron Mitchell (1999), fingerprint-based identification has been challenged in more than 20 court cases in the United States (e.g., U.S. v. Llera Plaza 2002a,b; U.S. v. Crisp 2003); Cole (2006) has given additional court cases. As recently as December 2005, the Massachusetts Supreme Judicial Court barred key fingerprint evidence obtained from several latent prints in the case of Terry L. Patterson (Saltzman 2005a,b).

The aforementioned court rulings demonstrate both the awareness and the need to develop measures that reflect the confidence in a match when fingerprint evidence is presented. Fingerprint individuality deals with the problem of quantifying the extent of uniqueness of a fingerprint. How similar should two fingerprints be before we can conclude with high confidence that they are from the same finger? What are the measures of fingerprint individuality that reflect the extent of uncertainty in the observed match?

The main challenge in studying fingerprint individuality is to develop models that adequately describe the variability of fingerprint features in a target population. These models can, in turn, be used to derive the probability of a random match between two different fingerprints picked arbitrarily from the target population. Eliciting candidate models for representing the variability of fingerprint features is not an easy task due to the complex nature of this variability. Candidate models should satisfy two important requirements: they are flexible (i.e., they can represent a wide range of distributional characteristics of fingerprint features in the population) and associated confidence measures can be easily obtained from them.

Some studies (although not many compared with other topics in fingerprints) have been reported on fingerprint individuality. Pankanti, Prabhakar, and Jain (2002) assumed a uniform distribution as the model on minutiae locations and directions; Figure 14 illustrates how the location and direction of a minutiae are determined. The uniform distribution was used to derive the probability of a random correspondence (PRC) between a pair of fingerprints. The PRC measures the likelihood of observing a certain degree of match or similarity between a pair of arbitrary fingerprints. More specifically, if Q and T denote a pair of fingerprints with m and n minutiae, then the PRC is given by

$$PRC(w) = P(\text{Exactly } w \text{ minutiae matches} \mid m, n), \qquad (17)$$

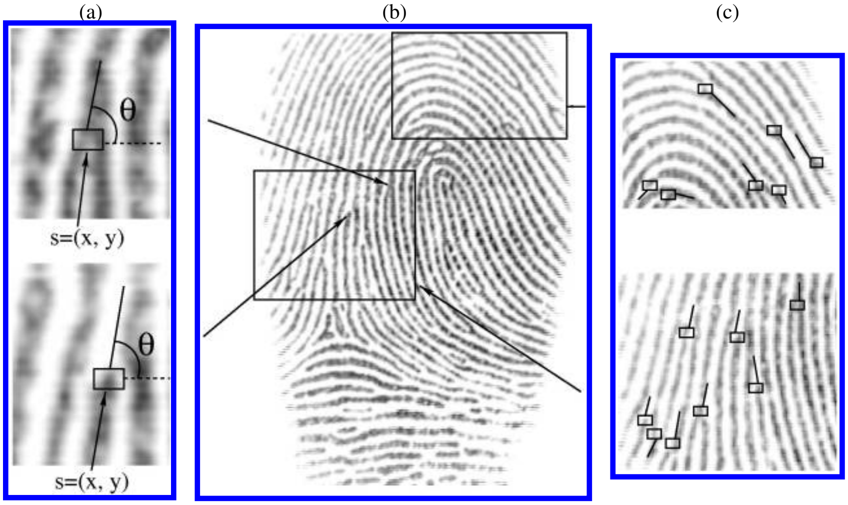

Figure 14. Minutiae features consisting of the location, s, and direction, θ, for a typical fingerprint image (b). (a) s and θ for a ridge bifurcation and ending. (c) Two subregions of (b) in which orientations that are spatially close tend to be very similar. The minutiae location is indicated by a square, and the direction is indicated by a line emanating from the square.

where the probability in (17) is computed assuming that the m (resp. n) minutiae in Q (resp. T) are distributed uniformly and independently of one another.

The uniform model on fingerprint minutiae has several drawbacks. It is well known that fingerprint minutiae form clusters (see, e.g., Stoney and Thornton 1986). Further, minutiae locations in different regions of the fingerprint domain are observed to be associated with different region-specific minutiae directions. Also, minutiae that are spatially close tend to have similar direction values to each other. Figure 14 illustrates these facts. Empirical observations such as these need to be taken into account when eliciting reliable statistical models on fingerprint features. For the reasons mentioned earlier, Pankanti's model underestimates the true probability of a fingerprint match. To alleviate the problem with the uniform distribution, a family of finite mixture models was developed by Dass et al. (2006b) to represent minutiae clusters. The mixture model on minutiae location, s, and direction, θ, has the form

$$f(s,\theta|\Theta_G) = \sum_{g=1}^{G} \tau_g f_g^L(s|\mu_g, \Sigma_g) \cdot f_g^D(\theta|\nu_g, \kappa_g, p_g), \qquad (18)$$

where G is the total number of components; for the gth component, $f_g^L(s \mid \mu_g, \Sigma_g)$ is the distribution of minutiae locations, with μ_g and Σ_g representing the measures of center and dispersion, for f_g^L. The density $f_g^D(\theta|\nu_g, \kappa_g, p_g)$ represents the distribution of minutiae directions with center ν_g, precision κ_g, and mixing probabilities p_g. Whereas any density function on R^2 is a potential model for f_g^L, eliciting a candidate for f_g^D requires more thought. Minutiae directions tend to have either similar or opposite directions to the local ridge orientation flow (see Fig. 14), and we require that our model satisfy this condition. One possible choice for f_g^D is

$$f_g^D(\theta|\nu_g, \kappa_g, p_g) = p_g f_g^O(\theta \mid \nu_g, \kappa_g) + (1-p_g) f_g^O(\theta - \pi \mid \nu_g, \kappa_g), \qquad (19)$$

where f_g^O is the density for the ridge flow orientation for the gth cluster. The density f_g^D in (19) can be interpreted as follows: For the ridge flow ω distributed as f_g^O, minutiae directions that are either ω or $\omega + \pi$ have probabilities p_g and $1 - p_g$. (Dass et al. (2006b) took the density f_g^L to be a bivariate Gaussian density with mean μ_g and covariance matrix Σ_g and took f_g^O to be the Von Mises density (see Mardia 1972),

$$f_g^O(\theta \mid \nu_g, \kappa_g) = \frac{2}{I_0(\kappa_g)} \exp\{\kappa_g \cos 2(\theta - \nu_g)\}, \qquad (20)$$

with $I_0(\kappa_g)$ defined as

$$I_0(\kappa_g) = \int_0^{2\pi} \exp\{\kappa_g \cos(\theta - \nu_g)\}\, d\theta. \qquad (21)$$

In (20), ν_g and κ_g represent the mean angle and the precision (inverse of the variance) of the Von Mises distribution.

Parameter estimation is carried out using the EM algorithm for mixtures (Dempster, Laird, and Rubin 1977); for fixed G, the missing component for the jth minutiae location and direction pair (X_j, D_j) is its class label, $c_j \in \{1, 2, \ldots, G\}$, for $j = 1, 2, \ldots, N$. The transformation

$$\omega_j = \begin{cases} D_j & \text{if } D_j \in [0, \pi) \\ D_j - \pi & \text{if } D_j \in [\pi, 2\pi) \end{cases} \qquad (22)$$

converts the minutiae directions into orientations that take values in $[0, \pi)$. The corresponding distribution for each (X_j, ω_j) then becomes

$$\sum_{g=1}^{G} \tau_g f_g^L(X_j \mid \mu_g, \Sigma_g) \cdot f_g^O(\omega_j \mid \nu_g, \kappa_g), \qquad (23)$$

where $f_g^O(\omega_j \mid \nu_g, \kappa_g)$ is as given in (20). Note that the expression in (23) is now in the standard form for mixture models (see, e.g., McLachlan and Krishnan 1997, sec. 2.7) and can be solved using general formulas for the E and M steps. To find the optimal number of clusters, G^*, we first estimate the model parameters for different values of G using the EM algorithm described earlier, and then select G^* using the Bayes information criterion (BIC). The approach outlined here extends the methodology of Fraley and Raftery (2002) by including angular variables in the mixture modeling. The BIC is defined as

$$BIC(G) = 2 * \sum_{j=1}^{N} \log f(X_j, D_j \mid \Theta_G) - |\Theta_G| \log(N), \qquad (24)$$

where $\Theta_G = \{(\mu_g, \Sigma_g, \nu_g, \kappa_g, p_g, \tau_g), g = 1, 2, \ldots, G\}$ denotes the set of all unknown parameters and $|\Theta_G|$ is the cardinality of Θ_G. The value of G^* is selected as the value of G that maximizes $BIC(G)$.

Along with the mixture models developed to represent (a) the minutiae variability in different fingers, Dass et al. (2006b) also developed stochastic models for two other sources of minutiae variability, namely (b) the variability due to local perturbations arising from nonlinear distortion effects in multiple impressions of a finger and (c) the variability due to the size of partial prints (or the area of finger region captured) in multiple acquisitions of a finger. For a fingerprint database with F fingers, the compound stochastic model is fit to each finger $f, f = 1, 2, \ldots, F$. For each finger f, the stochastic models are then used to generate H synthetic sets of query (resp. template) minutiae with m (resp. n) minutiae. We denote the simulated query (resp. template) minutiae sets by $\mathcal{F}^Q(f, h)$, $h = 1, 2, \ldots, H$ [resp. $\mathcal{F}^T(f, h)$, $h = 1, 2, \ldots, H$]. The matcher, M, of Ross, Dass, and Jain (2005) is used to determine the number of minutiae matches for each impostor pair of query and template minutiae sets [i.e., between $\mathcal{F}^Q(f, h)$ and $\mathcal{F}^T(f', h')$, where $f \neq f'$ and $h, h' = 1, 2, \ldots, H$]. The value of the PRC in (17) is estimated using

$$p(w) = \frac{\sum_{h=1}^{H} \sum_{h'=1}^{H} \sum_{f=1}^{F} \sum_{f'=1, f' \neq f}^{F} I_w\{(f, h), (f', h')\}}{F(F-1)H^2} \qquad (25)$$

for integers $w \leq w_0$, where $I_w\{(f, h), (f', h')\}$ is 1 if $M(\mathcal{F}^Q(f, h), \mathcal{F}^T(f', h'))$ equals w and 0 otherwise. For values of $w > w_0$, an extrapolation scheme based on $p(w)$ for $w \leq w_0$ is developed; Dass et al. (2006b) have provided further details on these estimation and extrapolation procedures.

The PRC corresponding to the FBI's "12-point match" criteria (i.e., declare that the two prints come from one and the same person if the number of minutiae matches is 12 or more) can be obtained by summing (17) over w values greater than or equal to 12. Table 3 gives the fingerprint individuality estimates derived from the mixture as well as Pankanti's models for the "12-point match criteria" based on FVC 2002 DB1 database (see Dass et al. 2006b for more details). Note that the estimates based on the mixture models are orders of magnitude higher compared with those of Pankanti et al. (2002) due to common clustering tendencies of minutiae in different fingerprints.

Table 3. A comparison between fingerprint individuality estimates (Dass et al. 2006b)

(m_Q, m_T, w)	Mixture model	Pankanti's model
(26, 26, 12)	6.8×10^{-10}	2.4×10^{-15}
(36, 36, 12)	6.5×10^{-7}	1.0×10^{-10}
(46, 46, 12)	2.0×10^{-5}	3.9×10^{-8}

Basic questions related to fingerprint individuality remain unanswered. For example, we have assumed that all of the detected minutiae in a fingerprint are true. Of course, this is not a valid assumption for medium- to poor-quality images. One topic of investigation would be to see how the PRCs deteriorate as a function of the quality of the underlying input image. More specifically, given an input with a certain image quality, what is the best estimate of PRC (corresponding to the lowest uncertainty in the observed match) that can be reported? Research in these areas will enhance the scientific basis of presenting fingerprint evidence in courts.

5. MULTIBIOMETRIC FUSION

The best performing fingerprint authentication algorithm (among the 41 algorithms evaluated) in the FVC 2004 (Maio et al. 2004) fingerprint verification competition had an EER of 2%. In general, biometric systems based on fingerprint evidence alone (unimodal systems) suffer from limitations such as the lack of uniqueness, nonuniversality, and noisy data (Jain and Ross 2004) resulting in suboptimal performance. In contrast, multimodal biometric systems combine information from its component modalities (e.g., multiple fingers or fingerprint and face) to arrive at a decision (Ross and Jain 2003). Several studies (Bigun, Bigun, Duc, and Fischer 1997; Kittler, Hatef, Duin, and Matas 1998; Lam and Suen 1995; Wang, Tan, and Jain 2003) have demonstrated that by consolidating information from multiple sources, better recognition performance can be achieved compared with the unimodal systems. In a multimodal biometric system, integration can be done at the feature level, matching-score level, or decision level. However, to achieve the best results, devising methods for optimally combining information from these multiple sources is necessary.

Compared with fusion at the feature and decision levels, consolidation of information at the matching-score level is the most useful and feasible for biometric systems. Biometric feature spaces are often high-dimensional and not compatible with each other for combination [e.g., fingerprint minutiae and PCA for face (Moon and Phillips 2001)], whereas decision-level fusion has very limited information available for useful consolidation. There are several challenges involved in fusing matching scores as well. Scores from different matchers may not be compatible; for example, the two face matchers in the NIST–BSSR1 database generate scores in the intervals $[-1, 1]$ and $[0, 100]$. Further, the scores of different matchers can be either dissimilarity or similarity measures, and they may follow different probability distributions. Another issue is that the accuracy of the matchers may be quite different, and the matching scores may be correlated.

A popular approach to fusion at the matching-score level is based on score normalization (Ross and Jain 2003; Jain, Nandakumar, and Ross 2005). In a score normalization scheme, matching scores from the different sources are transformed to a common domain by changing the location and scale parameters of the individual score distributions. In a good normalization scheme, the estimates of the location and scale parameters are required to be robust as well as efficient; robustness refers to the property where the estimator of interest is not affected by outliers, whereas efficiency relates to the closeness of the estimator to the true value (see, e.g., Huber 1981). Once robust and efficient estimators are determined, score normalization then fuses the (normalized) scores using various combination rules. Although many score normalization techniques are available, the challenge is to find a procedure that is both robust and efficient. Typical transformations involved in score normalization are of the form:

$$s' = \frac{s-\mu}{\sigma}, \tag{26}$$

where μ and σ are the location and scale parameters, and s and s' are the original and transformed scores. Different normalization rules arise by making different choices for μ and σ; the min–max rule is derived by taking μ to be the minimum score and σ to be the range, the z score results from taking μ to be the mean and σ to be the standard deviation, and a robust version of the z score is derived by taking μ to be the median and σ to be the mean absolute deviation. The $\tan h$ estimators based on work of Hample, Rousseeuw, Ronchetti, and Stahel (1986) are robust and highly efficient. This normalization rule is given by

$$s' = \frac{1}{2}\left\{\tan h\left(.01\left(\frac{s-\mu_{GH}}{\sigma_{GH}}\right)\right)+1\right\}, \tag{27}$$

where μ_{GH} and σ_{GH} are the mean and standard deviation estimators corresponding to the genuine score distribution given by the Hampel estimators. The Hampel estimators are based on an influence function that reduces the influence of points at the tails of the matching score distributions (see Jain et al. 2005) for details. Other score normalization techniques use the double-sigmoid function (see Cappelli, Maio, and Maltoni 2000 for details).

Subsequently, fusion of the normalized scores is based on several different rules: simple and weighted sum of scores and the maximum, minimum, and product rules (Kittler et al. 1998; Jain et al. 2005). Snelick, Indovina, Yen, and Mink (2003) studied the different score normalization techniques and concluded that the max–min rule followed by the sum fusion rule performed the best based on the experimental results on their database. Jain et al. (2005) conducted a more systematic study of the different normalization techniques to ascertain their performance based on a multimodal database comprising the fingerprint, face, and hand-geometry modalities. It was found that the weighted sum rule performed the best among all combination rules. An important component of the analysis presented by Jain et al. (2005) is the use of a nonparametric technique for estimating the density of the matching score distributions. This has the added advantage that it is not necessary to assume that each matching score distribution has a Gaussian distribution.

The disadvantage of a score normalization scheme is that the selection of optimal weights for the score combination is carried out on a case-by-case basis. This can be very challenging. Another approach that has been investigated is to fuse information automatically at the matching-score level based on likelihood functions (Dass, Nandakumar, and Jain 2005). One challenge with the likelihood function framework, as in score normalization, is that it is not easy to specify complete parametric distributions for matching scores. Matching-score distributions tend to be highly non-Gaussian and to consist of discrete components. The method of fusion outlined by Dass et al. (2005) uses copula functions (Nelsen 1999; Cherubini, Luciano, and Vecchiato 2004) and has several desirable properties. First, no parametric form is assumed for distributions on matching scores. Thus this approach is applicable in a variety of contexts. Second, the correlation between different biometric matchers is accounted for by the copula. Previous studies assumed that different matchers are independent of each other (see Griffin 2004) and, consequently, could not be applied to highly correlated data (e.g., matching scores from two different fingerprint matchers applied on the same fingerprint database). Finally, the copula approach automatically assigns optimal weights to different matchers during fusion and, thus bypasses the need to determine fusion weights on a case-by-case basis.

Fusion using the algorithm outlined by Dass et al. (2005) shows that the likelihood-based framework consistently achieves high performance rates. Figure 15 presents results on two multimodal databases, NIST–BSSR1 and West Virginia University (WVU). The NIST Biometric Scores Set–Release I (NIST–BSSR1) is a multimodal database in which matching scores were obtained using two fingerprints (on two index fingers) and two face matchers for 517 users. The West Virginia University multimodal database (WVU–Multimodal) consists of 320 subjects with 5 samples each of fingerprint and iris modalities. More details of the two databases have been given by Dass et al. (2005). Table 4 provides summary information for the two databases. Compared with the best single modality, the likelihood-based fusion gives improvements in the genuine acceptance rate (GAR) of 14.2% and 9.1% for the NIST and WVU databases at the false acceptance rate (FAR) level of .1%.

6. RECENT ADVANCES IN COMMERCIAL SYSTEMS

Several advances in fingerprint recognition technology have been made by commercial vendors. Until recently, the three main methods for acquiring fingerprint impressions have been the "ink technique" and acquisitions based on optical and solid-state sensors (Maltoni et al. 2003). In the ink technique, the subject's finger is coated with black ink and rolled over a paper card. The card is then scanned to produce a fingerprint impression. The advent of optical "live scan" sensors gave rise to digital fingerprint impressions. These sensors are based on the total internal reflection (TIR) principle, measuring the reflectivity of light of the sensing surface when a fingertip is placed on it. Solid-state sensors use silicon-based capacitive sensors to convert information in the fingertip surface into electrical signals. To date, several new sensing technologies have emerged. The multispectral fingerprint imaging (MSI) technique has been introduced by Lumidigm Inc. (Rowe, Corcoran, Nixon, and Ostrom 2005). This device scans various skin layers by using different wavelengths of light. Fingerprint images acquired using the MSI technology are significantly better quality for wet and dry fingers. Another new fingerprint-sensing technology based on a multicamera system has been introduced by TBS Inc. (Parziale and Diaz-Santana 2006). The "touchless" TBS sensor avoids contact of the fingertip to any sensing surface, thereby reducing deformations

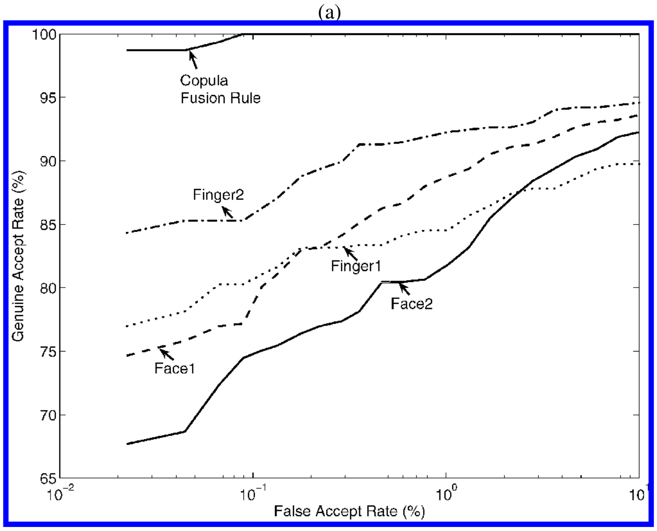

Figure 15. Improvement in authentication performance using the fusion rule based on Gaussian copula functions (Dass et al. 2005): The ROC curves for the fusion and individual biometric systems based on the NIST–BSSR1 (a) and WVU (b) databases.

due to skin elasticity during the acquisition process. A touchless fingerprint sensing device is also available from Mitsubishi (*http://global.mitsubish.electric.com*).

The resolution of a digital image, measured in terms of the number of dots or pixels per inch (dpi or ppi), is an important characteristic of the image. Images in the resolution range of 250–500 dpi are effective in recovering fingerprint minutiae and ridge flow information, but ineffective for detecting finer features. For this reason, higher-resolution sensors are currently under development. Although solid-state sensors still cannot achieve this high resolution due to the cost factor, several optical sensors with resolution 1,000 dpi are commercially available. Optical sensors with resolution range of 4,000–7,000 dpi are currently under development.

One advantage of such high-level resolution sensors is that finer fingerprint features, consisting of sweat pores, ridge contours, incipient ridges, and scars (see Jain, Chen, and Demirkus 2006, 2007) can be observed and extracted. These finer features are grouped as level 3 features in a hierarchy, where levels 1 and 2 consists of the ridge flow information and the minutiae (Kryszczuk, Drygajlo, and Morier 2004; Roddy and Stosz 1997; Jain et al. 2006, 2007). Several studies incorporating level 3 features have reported performance improvement in recognition systems (see, e.g., Jain et al. 2006, 2007; Stosz and Alyea 1994).

Current commercial systems also incorporate preventive measures against spoof (liveliness) attacks. This is a security threat where the fingerprint system can be tricked into accepting an artificial input (called a gummy fingerprint). This kind of attack was famously described by Matsumoto, who used a gelatin material (similar to that contained in candies) to spoof a variety of sensors (Rowe et al. 2005). With the advent of new sensor technology, research has been carried out on developing methods for preventing spoof attacks based on the multispectral sensors (Nixon and Rowe 2005). Another approach, based on discriminating the extent of distortion present in real fingerprint acquisitions compared with false ones, was reported by Antonelli, Cappelli, Maio, and Maltoni (2006) and Chen, Jain, and Dass (2005b). Commercial vendors have also developed methods for enhancing template security based on fingerprint vaults and watermark encryption strategies (see, e.g., Uludag, Pankanti, Prabhakar, and Jain 2004; Jain and Uludag 2003; and references therein). Smart cards with in-built sensors, feature extractor, matcher, and template storage chips from makers such as Privaris Inc. have been proposed to curb credit card theft and identity fraud (Jain and Pankanti 2006).

Table 4. Summary of multibiometric databases

Database	Biometric traits	*K*	No. of users
NIST-multimodal	Fingerprint (two fingers) Face (two different matchers)	4	517
WVU-multimodal	Fingerprint, iris	2	320

NOTE: *K* denotes the number of matchers used for each database.

Other commercial advances have been aimed at developing quantitative measures for the quality of fingerprint images (Chen et al. 2005a). One goal is to incorporate quality measures in a fusion framework, because authentication is severely affected by the quality of the underlying biometric. This is an important point to consider, because it has practical consequences. In real environments, one cannot expect that all input biometrics corresponding to an individual will be of the best quality. In that case, a fusion framework in which low-quality images will automatically be assigned lower weights will be of great interest and importance. Developing methodology for validating the performance of fingerprint systems claimed by system vendors is also gaining interest. The challenge here is to derive tests and confidence statements to either validate or reject claims on system performance (Dass et al. 2006a). Other concerns of commercial systems include ergonomics (user-friendliness of the system), throughput (number of users recognized per unit of time), and system cost.

7. SUMMARY AND CONCLUSION

We have attempted to give a brief overview of fingerprint-based recognition and to describe current challenges faced in making these systems perform more effectively. Four important aspects of fingerprint-based recognition as well as recent advances in commercial systems have been discussed. Fingerprint recognition systems face many problems and challenges. Despite these challenges, new applications (e.g., deployment of fingerprint recognition systems in Disney theme parks, inside mobile phones, flash drives, and memory sticks) continue to appear, strongly suggesting that this type of authentication is here to stay. Statistics can play a pivotal role in this area by providing insight into the stochastic processes (signal as well as noise) involved in the development of effective methodology and algorithms for recognition.

8. ACKNOWLEDGMENTS

This work was supported by the National Science Foundation (ITR grant 0312646) and the Army Research Office (grant W911NF-06-1-0418).

[Received July 2006. Revised September 2006.]

REFERENCES

Antonelli, A., Cappelli, R., Maio, D., and Maltoni, D. (2006), "Fake Finger Detection by Skin Distortion Analysis," *IEEE Transactions on Information Forensics and Security*, 1, 360–373.

Bazen, A. M., and Gerez, S. H. (2002), "Systematic Methods for the Computation of the Directional Fields and Singular Points of Fingerprints," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24, 905–919.

Bhanu, B., and Tan, X. (2003), "Indexing Based on Novel Features of Minutiae Triplets," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25, 616–622.

Bigun, E. S., Bigun, J., Duc, B., and Fischer, S. (1997), "Expert Conciliation for Multimodal Person Authentication Systems Using Bayesian Statistics," in *Proceedings of the First International Conference on Audio- and Video-Based Biometric Person Authentication*, pp. 291–300.

Cappelli, R., Lumini, A., Maio, D., and Maltoni, D. (1999), "Fingerprint Classification by Directional Image Partitioning," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 21, 402–421.

Cappelli, R., Maio, D., and Maltoni, D. (2000), "Combining Fingerprint Classifiers," in *Proceedings of the First International Workshop on Multiple Classifier Systems*, pp. 351–361.

Chang, J., and Fan, K. (2002), "A New Model for Fingerprint Classification by Ridge Distribution Sequences," *Pattern Recognition*, 35, 1209–1223.

Chen, Y., Dass, S., and Jain, A. K. (2005a), "Fingerprint Quality Indices for Predicting Authentication Performance," in *Proceedings of the Conference Audio- and Video-Based Biometric Person Authentication*, pp. 160–170.

Chen, Y., Jain, A. K., and Dass, S. C. (2005b), "Fingerprint Deformation for Spoof Detection," presented at Biometric Symposium, a special session at the Biometric Consortium Conference, Crystal City, VA.

Cherubini, U., Luciano, E., and Vecchiato, W. (2004), *Copula Methods in Finance*, New York: Wiley.

Chong, M. M. S., Ngee, T. H., Jun, L., and Gay, R. K. L. (1997), "Geometric Framework for Fingerprint Image Classification," *Pattern Recognition*, 30, 1475–1488.

Cole, S. (2006), "Is Fingerprint Identification Valid? Rhetorics of Reliability in Fingerprint Proponents Discourse," *Law & Policy*, 28, 109–135.

Dass, S. C. (2004), "Markov Random Field Models for Directional Field and Singularity Extraction in Fingerprint Images," *IEEE Transactions on Image Processing*, 13, 1358–1367.

Dass, S. C., and Jain, A. K. (2004), "Fingerprint Classification Using Orientation Field Flow Curves," in *Proceedings of the Indian Conference on Computer Vision, Graphics and Image Processing*, pp. 650–655.

Dass, S. C., Nandakumar, K., and Jain, A. K. (2005), "A Principled Approach to Score Level Fusion in Multimodal Biometric Systems," in *Proceedings of the Conference on Audio- and Video-Based Biometric Person Authentication*, pp. 1049–1058.

Dass, S. C., Zhu, Y., and Jain, A. K. (2006a), "Validating a Biometric Authentication System: Sample Size Requirements," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28, 1902–1913.

——— (2006b), "Compound Stochastic Models for Fingerprint Individuality," *Proceedings of the International Conference on Pattern Recognition (ICPR)*, 3, 532–535.

Daubert v. Merrel Dow Pharmaceuticals, 113 S. Ct. 2786 (1993).

Dempster, A. P., Laird, N. M., and Rubin, D. B. (1997), "Maximum Likelihood for Incomplete Data via the EM Algorithm," *Journal of the Royal Statistical Society*, Ser. B, 39, 1–38.

Federal Bureau of Investigation (1994), Press release, available at *http://www.fbi.gov/pressrel/pressrel04/ mayfield052404.htm*.

Fraley, C., and Raftery, A. E. (2002), "Model-Based Clustering, Discriminant Analysis and Density Estimation," *Journal of the American Statistical Association*, 97, 611–631.

Germain, R. S., Califano, A., and Colville, S. (1997), "Fingerprint Matching Using Transformation Parameters," *IEEE Transactions on Computational Science and Engineering*, 4, 42–49.

Griffin, P. (2004), "Optimal Biometric Fusion for Identity Verification," Preprint RDNJ-03-0064, Identix Corporate Research Center.

Hample, F. R., Rousseeuw, P. J., Ronchetti, E. M., and Stahel, W. A. (1986), *Robust Statistics: The Approach Based on Influence Functions*, New York, Wiley.

Henry, E. R. (1990), *Classification and Uses of Fingerprints*, London: Routledge.

Hong, L., Wan, Y., and Jain, A. K. (1998), "Fingerprint Image Enhancement: Algorithm and Performance Evaluation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20, 777–789.

Huber, P. J. (1981), *Robust Statistics*, New York: Wiley.

Jain, A. K., and Pankanti, S. (2006), "A Touch of Money," *IEEE Spectrum*, 43, 22–27.

Jain, A. K., and Ross, A. (2004), "Multibiometric Systems," *Communications of the ACM, Special Issue on Multimodal Interfaces*, 47, 34–40.

Jain, A. K., and Uludag, U. (2003), "Hiding Biometric Data," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25, 1494–1498.

Jain, A. K., Bolle, R., and Pankanti, S. (eds.) (1999a), *BIOMETRICS: Personal Identification in Networked Society*, Boston: Kluwer.

Jain, A. K., Chen, Y., and Demirkus, M. (2006), "Pores and Ridges: Fingerprint Matching Using Level 3 Features," *Proceedings of the International Conference on Pattern Recognition*, 4, 477–480.

——— (2007), "Pores and Ridges: High-Resolution Fingerprint Matching Using Level 3 Features," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29, 15–27.

Jain, A. K., Hong, L., Pankanti, S., and Bolle, R. (1997), "An Identity Authentication System Using Fingerprints," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 85, 1365–1388.

Jain, A. K., Nandakumar, K., and Ross, A. (2005), "Score Normalization in Multimodal Biometric Systems," *Pattern Recognition*, 38, 2270–2285.

Jain, A. K., Prabhakar, S., and Hong, L. (1999b), "A Multichannel Approach to Fingerprint Classification," 21, 348–359.

Jain, A. K., Prabhakar, S., Hong, L., and Pankanti, S. (2000), "Filterbank-Based Fingerprint Matching," *IEEE Transactions on Image Processing*, 9, 846–859.

Karu, K., and Jain, A. K. (1996), "Fingerprint Classification," *Pattern Recognition*, 29, 389–404.

Kittler, J., Hatef, M., Duin, R. P., and Matas, J. G. (1998), "On Combining Classifiers," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20, 226–239.

Kryszczuk, K., Drygajlo, A., and Morier, P. (2004), "Extraction of Level 2 and Level 3 Features for Fragmentary Fingerprints," in *Proceedings of the Second COST Action 275 Workshop*, pp. 83–88.

Lam, L., and Suen, C. Y. (1995), "Optimal Combination of Pattern Classifiers," *Pattern Recognition Letters*, 16, 945–954.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., and Jain, A. K. (2002), "FVC2002: Fingerprint Verification Competition," in *Proceedings of the International Conference on Pattern Recognition*, pp. 744–747, available at *http://bias.csr.unibo.it/fvc2002/databases.asp*.

——— (2004), "FVC2004: Fingerprint Verification Competition," in *Proceedings of the International Conference on Biometric Authentication*, pp. 1–7, available at *http://bias.csr.unibo.it/fvc2004/*.

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

Mardia, K. V. (1972), *Statistics of Directional Data*, New York: Academic Press.

McLachlan, G. J., and Krishnan, T. (1997), *The EM Algorithm and Extensions*, New York: Wiley.

Moayer, B., and Fu, K. S. (1975), "A Syntactic Approach to Fingerprint Pattern Recognition," *Pattern Recognition*, 7, 1–23.

——— (1976a), "An Application of Stochastic Languages to Fingerprint Pattern Recognition," *Pattern Recognition*, 8, 173–179.

——— (1976b), "A Tree System Approach for Fingerprint Pattern Recognition," *IEEE Transactions on Computers*, 25, 262–274.

Moon, H., and Phillips, P. J. (2001), "Computational and Performance Aspects of PCA-Based Face Recognition Algorithms," *Perception*, 30, 303–321.

Nakamura, O., Goto, K., and Minami, T. (1982), "Fingerprint Classification by Directional Distribution Patterns," *Systems, Computers, Controls*, 13, 81–89.

Nelsen, R. B. (1999), *An Introduction to Copulas*, New York: Springer.

Nixon, K. A., and Rowe, R. K. (2005), "Multispectral Fingerprint Imaging for Spoof Detection," in *Proceedings of SPIE Conference on Biometric Technology for Human Identification*, pp. 214–215.

O'Gorman, L., and Nickerson, J. V. (1987), "An Approach to Fingerprint Filter Design," *Pattern Recognition*, 22, 362–385.

Pankanti, S., Prabhakar, S., and Jain, A. K. (2002), "On the Individuality of Fingerprints," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24, 1010–1025.

Parziale, G., and Diaz-Santana, E. (2006), "The Surround Imager: A Multi-camera Touchless Device to Acquire 3D Rolled Equivalent Fingerprints," in *Proceedings of the International Conference on Biometrics*, pp. 244–250.

Perona, P. (1998), "Orientation Diffusions," *IEEE Transactions on Image Processing*, 7, 457–467.

Rao, A. R. (1990), *A Taxonomy for Texture Description and Identification*, New York: Springer-Verlag.

Rao, A. R., and Jain, R. C. (1992), "Computerized Flow Field Analysis: Oriented Texture Fields," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 14, 693–709.

Ratha, N. K., Chen, S., and Jain, A. K. (1995), "Adaptive Flow Orientation–Based Feature Extraction in Fingerprint Images," *Pattern Recognition*, 28, 1657–1672.

Roddy, A. R., and Stosz, J. D (1997), "Fingerprint Features: Statistical Analysis and System Performance Estimates," *Proceedings of the IEEE*, 85, 1390–1421.

Ross, A., and Jain, A. K. (2003), "Information Fusion in Biometrics," *Pattern Recognition Letters, Special Issue on Multimodal Biometrics*, 24, 2115–2125.

Ross, A., Dass, S. C., and Jain, A. K. (2005), "A Deformable Model for Fingerprint Matching," *Pattern Recognition*, 38, 95–103.

Rowe, R. K., Corcoran, S. P., Nixon, S. P., and Ostrom, R. E. (2005), "Multispectral Imaging for Biometrics," in *Proceedings of SPIE Conference on Biometric Technology for Human Identification, Orlando*, pp. 90–99.

Saks, M. J., and Koehler, J. J. (2005), "The Coming Paradigm Shift in Forensic Identification Science," *Science*, 309, 892.

Saltzman, J. (2005a), "SJC Bars a Type of Prints at Trial," *The Boston Globe*, December 28, 2005.

——— (2005b), "Massachusetts Supreme Judicial Court to Hear Arguments on Banning Fingerprint Evidence," *The Boston Globe*, September 5, 2005.

Snelick, R., Indovina, M., Yen, J., and Mink, A. (2003), "Multimodal Biometrics: Issues in Design and Testing," in *Proceedings of the Fifth International Conference on Multimodal Interfaces*, pp. 68–72.

Srinivasan, V. S., and Murthy, N. N. (1992), "Detection of Singular Points in Fingerprint Images," *Pattern Recognition*, 25, 139–153.

Stoney, D. A., and Thornton, J. I. (1986), "A Critical Analysis of Quantitative Fingerprint Individuality Models," *Journal of Forensic Sciences*, 31, 1187–1216.

Stosz, J. D., and Alyea, L. A. (1994), "Automated System for Fingerprint Authentication Using Pores and Ridge Structure," in *Proceedings of SPIE Conference on Automatic Systems for the Identification and Inspection of Humans*, pp. 210–223.

Thompson, W., and Cole, S. (2005), "Lessons From the Brandon Mayfield Case," *The Champion*, 29, 42–44.

Uludag, U., Pankanti, S., Prabhakar, S., and Jain, A. K. (2004), "Biometric Cryptosystems: Issues and Challenges," *Proceedings of the IEEE, Special Issue on Multimedia Security for Digital Rights Management*, 92, 948–960.

U.S. v. Byron Mitchell. Criminal Action No. 96-407, U.S. District Court for the Eastern District of Pennsylvania (1999).

U.S. v. Crisp, 324 F 3d 261 (4th Cir 2003) (2003).

U.S. v. Llera Plaza, 179 F Supp 2d 492 (ED Pa 2002) (2002a).

U.S. v. Llera Plaza, 188 F Supp 2d 549 (ED Pa 2002) (2002b).

Wang, Y., Tan, T., and Jain, A. K. (2003), "Combining Face and Iris Biometrics for Identity Verification," in *Proceedings of the Fourth International Conference on AVBPA*, pp. 805–813.

Wilson, C. L., Candela, G. T., and Watson, C. I. (1994), "Neural Network Fingerprint Classification," *Journal of Artificial Neural Networks*, 2, 203–228.

This article has been cited by:

1. Bin Yu . 2007. Embracing Statistical Challenges in the Information Technology AgeEmbracing Statistical Challenges in the Information Technology Age. *Technometrics* **49**:3, 237-248. [Abstract] [PDF] [PDF Plus]