Integrating Faces and Fingerprints for Personal Identification

Lin Hong and Anil Jain, *Fellow*, *IEEE*

Abstract—An automatic personal identification system based solely on fingerprints or faces is often not able to meet the system performance requirements. Face recognition is fast but not extremely reliable, while fingerprint verification is reliable but inefficient in database retrieval. We have developed a prototype biometric system which integrates faces and fingerprints. The system overcomes the limitations of face recognition systems as well as fingerprint verification systems. The integrated prototype system operates in the identification mode with an admissible response time. The identity established by the system is more reliable than the identity established by a face recognition system. In addition, the proposed decision fusion scheme enables performance improvement by integrating multiple cues with different confidence measures. Experimental results demonstrate that our system performs very well. It meets the response time as well as the accuracy requirements.

Index Terms—Biometrics, fingerprint matching, minutiae, face recognition, eigenface, decision fusion.

1 Introduction

With the evolution of information technology, our society is becoming more and more electronically connected. Daily transactions between individuals or between individuals and various organizations are conducted increasingly through highly interconnected electronic devices. The capability of automatically establishing the identity of individuals is thus essential to the reliability of these transactions. Traditional personal identification approaches which use "something that you know," such as a Personal Identification Number (PIN), or "something that you have," such as an ID card are not sufficiently reliable to satisfy the security requirements of electronic transactions because they lack the capability to differentiate between a genuine individual and an impostor who fraudulently acquires the access privilege [17]. *Biometrics*, which refers to identification of an individual based on her physiological or behavioral characteristics, relies on "something which you are or you do" to make a personal identification and, therefore, inherently has the capability to differentiate between a genuine individual and a fraudulent impostor [17], [27].

Any human physiological or behavioral characteristic can be used as a *biometric characteristic* (*indicator*) to make a personal identification as long as it satisfies the following requirements [6], [17]:

1) *universality*, which means that each person should have the characteristic;
2) *uniqueness*, which indicates that no two persons should be the same in terms of the characteristic;
3) *permanence*, which means that the characteristic should not be changeable; and
4) *collectability*, which indicates that the characteristic can be measured quantitatively.

However, in practice, a biometric characteristic that satisfies all the above requirements may not always be feasible for a practical biometric system. In a practical biometric system, there are a number of other issues which should be considered, including [6], [17]:

1) *performance*, which refers to the achievable identification accuracy, speed, robustness, the resource requirements to achieve the desired identification accuracy and speed, as well as operational or environmental factors that affect the identification accuracy and speed;
2) *acceptability*, which indicates the extent to which people are willing to accept a particular biometrics in their daily life; and
3) *circumvention*, which reflects how easy it is to fool the system by fraudulent methods.

A practical biometric system should be able to:

1) achieve an acceptable identification accuracy and speed with a reasonable resource requirements;
2) not be harmful to the subjects and be accepted by the intended population; and
3) be sufficiently robust to various fraudulent methods.

Currently, there are mainly nine different biometric techniques that are either widely used or under investigation, including [27]:

- face,
- facial thermogram,
- fingerprint,
- hand geometry,
- hand vein,
- iris,

• *The authors are with the Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824-1226. E-mail: {honglin, jain}@cse.msu.edu.*

Manuscript received 6 Oct. 1997; revised 8 Sept. 1998. Recommended for acceptance by V. Nalwa.
For information on obtaining reprints of this article, please send e-mail to: tpami@computer.org, and reference IEEECS Log Number 107416.

Fig. 1. Examples of biometric characteristics (indicators). (a) Face. (b) Facial thermogram. (c) Fingerprint. (d) Hand vein. (e) Retinal scan.

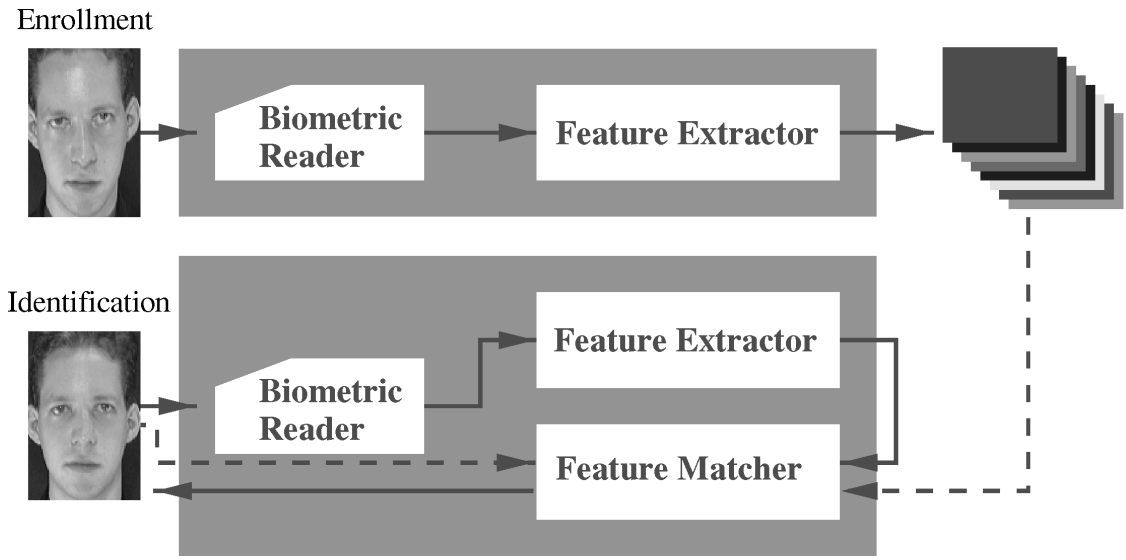


Fig. 2. A generic biometric system architecture.

- retinal pattern,
- signature, and
- voice-print

(some of the examples are shown in Fig. 1) [6], [7], [8], [16], [17]. All these biometric techniques have their own advantages and disadvantages and are admissible depending on the application domain.

A generic biometric system architecture is depicted in Fig. 2. Logically, it can be divided into two modules:

1) enrollment module and
2) identification module.

During the enrollment phase, the biometric characteristic of an individual is first scanned by the biometric reader to produce a digital representation of the characteristic. In order to facilitate the matching and identification, the digital representation is usually further processed by a feature extractor to generate a compact but expressive representation, called a *template*. Depending on the application, the template may be stored in the central database of the biometric system or be recorded in the smart card or magnetic card issued to the individual. The identification module is responsible for identifying individuals at the point-of-access. In the operational phase, the biometric reader captures the characteristic of the individual to be identified and converts it to a raw digital format, which is further processed by the feature extractor to produce a compact representation that is of the same format as the template. The resulting representation is fed to the feature matcher which compares it against the template(s) to establish the identity.

1.1 Operational Mode

A biometric system may operate in

1) the *verification mode* or
2) the *identification mode* [17].

A biometric system operating in the verification mode *authenticates* an individual's identity by comparing the individual only with his/her own template(s) (Am I whom I claim I am?). It conducts one-to-one comparison to determine whether the identity claimed by the individual is true or not. A biometric system operating in the identification mode recognizes an individual by searching the entire template database for a match (Who am I?). It conducts one-to-many comparisons to establish the identity of the individual.

Generally, it is more difficult to design an identification system than to design a verification system [17]. For a verification system, the major challenge is the system accuracy. It is usually not very difficult to meet the response time requirement, because only one-to-one comparison is conducted. On the other hand, for an identification system, both the accuracy and speed are critical. An identification system needs to explore the entire template database to establish an identity. Thus, more requirements are imposed on the feature extractor and, especially, the feature matcher.

Some biometric approaches are more suitable for operating in the identification mode than the others. For example, although significant progress has been made in fingerprint identification and a number of fingerprint classification and matching techniques have been proposed, it is still not practical to conduct a real-time search even on a relatively small-size fingerprint database (several thousand images) without dedicated hardware matchers, external alignment, and multiple-fingerprint indexing mechanism [21]. On the other hand, it is feasible to design a face-recognition system operating in the identification mode, because

1) face comparison is a relatively less expensive operation and
2) efficient indexing techniques are available and the performance is admissible [23].

1.2 Identification Accuracy

Due to *intraclass variations* in the biometric characteristics, the identity can be established only with certain confidence. A decision made by a biometric system is either a "genuine individual" type of decision or an "impostor" type of decision [7], [17]. For each type of decision, there are two possible outcomes, *true or false*. Therefore, there are a total of four possible outcomes:

1) a genuine individual is accepted,
2) a genuine individual is rejected,
3) an impostor is rejected, and
4) an impostor is accepted.

Outcomes 1 and 3 are correct, whereas outcomes 2 and 4 are incorrect. The confidence associated with different decisions may be characterized by the genuine distribution and the impostor distribution, which are used to establish two error rates:

1) *false acceptance rate* (FAR), which is defined as the probability of an impostor being accepted as a genuine individual and
2) *false reject rate* (FRR), which is defined as the probability of a genuine individual being rejected as an impostor.

FAR and FRR are dual of each other. A small FRR usually leads to a larger FAR, while a smaller FAR usually implies a larger FRR. Generally, the system performance requirement is specified in terms of FAR [17]. A FAR of zero means that no impostor is accepted as a genuine individual.

In order to build a biometric system that is able to operate efficiently in identification mode and achieve desirable accuracy, an integration scheme which combines two or more different biometric approaches may be necessary. For example, a biometric approach that is suitable for operating in the identification mode may be used to index the template database and a biometric approach that is reliable in deterring impostors may be used to ensure the accuracy. Each biometric approach provides a certain confidence about the identity being established. A decision fusion scheme which exploits all the information at the output of each approach can be used to make a more reliable decision.

We introduce a prototype integrated biometric system which makes personal identification by integrating both faces and fingerprints. The prototype integrated biometric system shown in Fig. 3 operates in the identification mode. The proposed system integrates two different biometric approaches (face recognition and fingerprint verification) and incorporates a decision fusion module to improve the identification performance.

In the following sections, we will describe each component of the proposed integrated system. Section 2 addresses the face-recognition technique being employed. Section 3 presents the fingerprint-verification module along with minutiae extraction and minutiae matching. A decision fusion framework which integrates faces and fingerprints is formulated in Section 4. Experimental results on the MSU fingerprint database captured with an online fingerprint scanner and public-domain face databases are described in Section 5. Finally, the summary and conclusions are given in Section 6.

2 Face Recognition

Face recognition is an active area of research with applications ranging from static, controlled mug-shot verification to dynamic, uncontrolled face identification in a cluttered background [5]. In the context of personal identification, face recognition usually refers to static, controlled full-frontal portrait recognition [5]. By static, we mean that the facial portraits used by the face-recognition system are still facial images (intensity or range). By controlled, we mean that the type of background, illumination, resolution of the acquisition devices, and the distance between the acquisition devices and faces, etc. are essentially fixed during the image acquisition process. Obviously, in such a controlled situation, the segmentation task is relatively simple and the intraclass variations are small.

During the past 25 years, a substantial amount of research effort has been devoted to face recognition [5], [25], [1]. In the early 1970s, face recognition was mainly based on measured facial attributes such as eyes, eyebrows, nose, lips, chin shape, etc. [5]. Due to lack of computational resources and brittleness of feature extraction algorithms, only a very limited number of tests were conducted and the recognition performance of face-recognition systems was far from desirable [5]. After the dormant 1980s, there was a resurgence in face-recognition research in the early 1990s. In addition to continuing efforts on attribute-based techniques [5], a number of new face-recognition techniques were proposed, including:

- principle component analysis (PCA) [22], [12], [24],
- linear discriminant analysis (LDA) [23],
- singular value decomposition (SVD) [10], and
- a variety of neural network-based techniques [25].

The performance of these approaches is impressive. It was concluded that "face-recognition algorithms were developed and were sufficiently mature that they can be ported to real-time experimental / demonstration system" [19].

Generally, there are two major tasks in face recognition:

1) locating faces in input images and
2) recognizing the located faces.

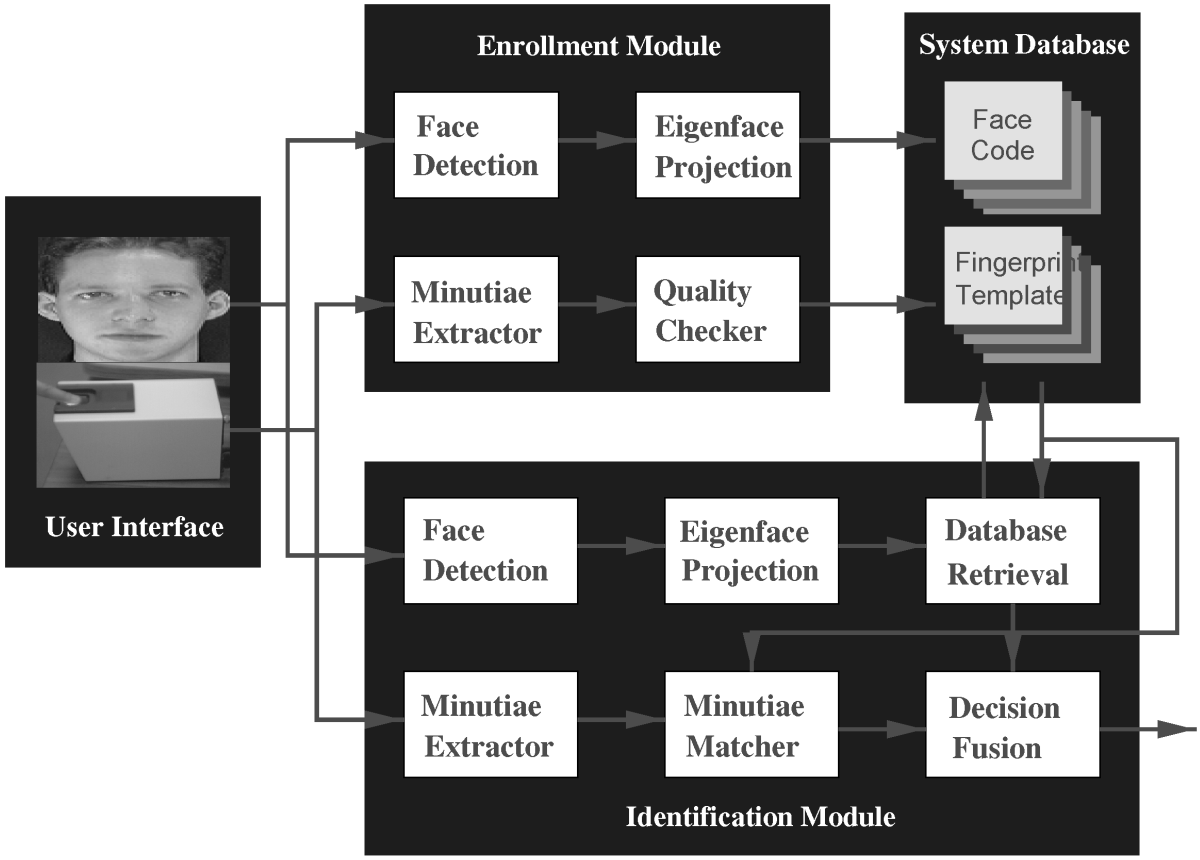


Fig. 3. System architecture of the prototype integrated biometric identification system.

Face location itself continues to be a challenging problem for uncontrolled and cluttered images [5]. Fortunately, in the context of personal identification, the background is controlled or almost controlled, so face location is generally not considered to be a difficult problem. Face recognition from a general viewpoint also remains an open problem because transformations such as position, orientation, and scale and changes in illumination produce large *intraclass variations* [19]. Again, in the context of personal identification, the variations in acquired face images can be restricted to a certain range which enables the current techniques to achieve a desirable performance [5], [19].

In our system, the eigenface approach is used for the following reasons:

1) in the context of personal identification, the background, transformations, and illumination can be controlled,
2) eigenface approach has a compact representation—a facial image can be concisely represented by a feature vector with a few elements,
3) it is feasible to index an eigenface-based template database using different indexing techniques such that the retrieval can be conducted efficiently [23],
4) the eigenface approach is a generalized template matching approach which was demonstrated to be more accurate than the attribute-based approach in one study [4].

The eigenface-based face recognition consists of the following two stages [24]:

1) *training stage*, in which a set of N training face images are collected; eigenfaces that correspond to the M highest eigenvalues are computed from the training set; and each face is represented as a point in the M-dimensional eigenspace, and
2) *operational stage*, in which each test image is first projected onto the M-dimensional eigenspace; the M-dimensional face representation is then deemed as a feature vector and fed to a classifier to establish the identity of the individual.

A $W \times H$ face image $I(x, y)$ can be represented as a $W \times H$-dimensional feature vector by concatenating the rows of $I(x, y)$ together. Thus, each $W \times H$ face image becomes a point in the $W \times H$-dimensional space. The total number of pixels in a face image is typically large, on the order of several thousands for even small image sizes. Face images in such a high-dimensional space are not randomly distributed. Therefore, it is efficient and beneficial to project them to a lower-dimensional subspace using principle component analysis [24]. Let Ψ_1, Ψ_2, ..., Ψ_N denote the N $W \times H$-dimensional training vectors with zero-mean. Let the M basis vectors, $\mathbf{u}_1$, $\mathbf{u}_2$, ..., $\mathbf{u}_M$ be a set of orthonormal vectors that best describe, the distribution of face images in the M-dimensional subspace (eigenspace), $M \leq N$. The kth eigenvector, $\mathbf{u}_k$, $k = 1, 2, ..., M$, is computed such that [24]

$$\lambda_k = \frac{1}{N} \sum_{i=1}^{N} \left(\mathbf{u}_k^T \Psi_i \right)^2 \tag{1}$$

is maximum, subject to

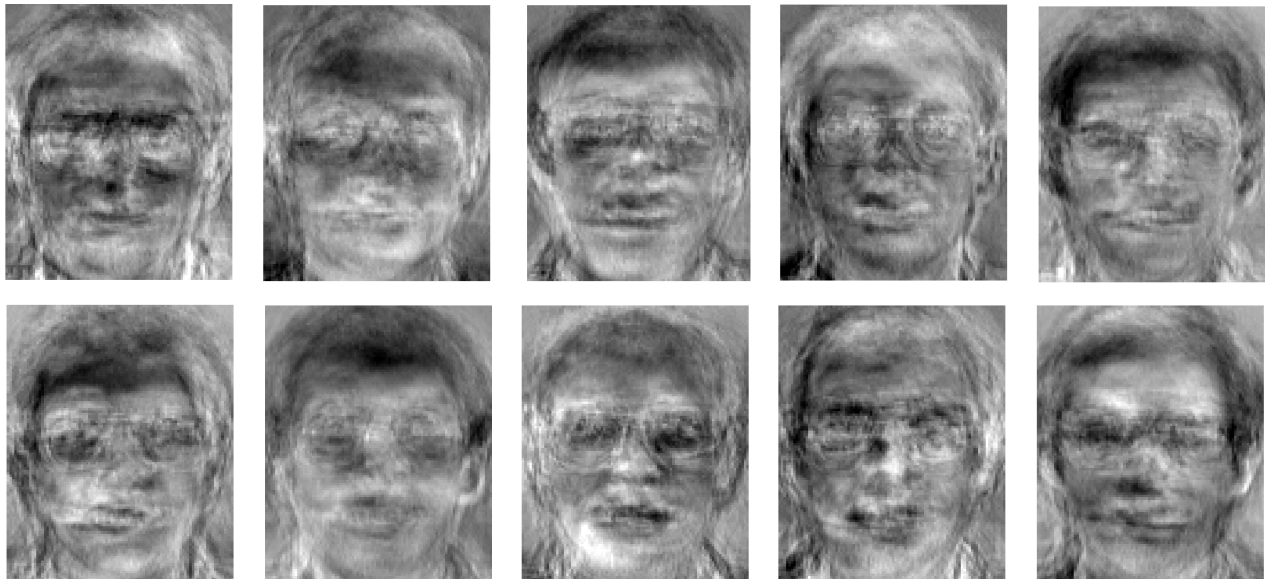


Fig. 4. First 10 eigenfaces obtained from 542 images of size 92×112, which are listed from left to right and top to bottom in a decreasing order of the corresponding eigenvalues.

$$\mathbf{u}_i^T \mathbf{u}_j = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

The value λ_k is the kth largest eigenvalue of the covariance matrix Σ which can be estimated using the training samples by

$$\hat{\Sigma} = \frac{1}{N} \sum_{i=1}^{N} \Psi_i \Psi_i^T . \tag{3}$$

The vector $\mathbf{u}_k$ is the kth eigenvector of the covariance matrix Σ corresponding to λ_k.

With the M-dimensional eigenspace defined, training vectors, $\Psi_1, \Psi_2, \cdots, \Psi_N$, can be represented as a set of M-dimensional feature vectors, $\Phi_1, \Phi_2, \cdots, \Phi_N$:

$$\Phi_k = \mathbf{u}^T \Psi_i, \qquad i = 1, 2, \cdots, N, \tag{4}$$

where $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2, ..., \mathbf{u}_M)$. Fig. 4 shows the first 10 eigenfaces corresponding to the 10 largest eigenvalues, which were computed based on 542 training images (of size 92×112).

In the operational phase, a detected face image, Γ, which is normalized to zero mean, is vectorized and projected onto the eigenvectors according to $\Pi = \mathbf{u}^T \Gamma$. With both training samples and test samples being projected onto an M-dimensional eigenspace, face recognition can be accomplished by a classifier operating in the eigenspace. In the context of personal identification, only a very limited number of training samples are available for each individual [17]. Thus, a k-nearest neighbor classifier is typically used, in which the distance, d, called Distance From Feature Space (DFFS) [24] between a template, Φ, and a test pattern, Π, is defined as $\|\Phi - \Pi\|$, where $\|\bullet\|$ denotes L_2 *norm*.

3 Fingerprint Verification

A fingerprint is the pattern of ridges and furrows on the surface of a fingertip. It is formed by the accumulation of dead, cornified cells that constantly slough as scales from the exposed surface [14]. Its formation is determined in the fetal period [15]. Humans have used fingerprints for personal identification for a long time. The biological properties of fingerprints are well understood which are summarized as follows:

1) individual epidermal ridges and furrows have different characteristics for different fingerprints;
2) the configuration types are individually variable, but they vary within limits which allow for systematic classification;
3) the configurations and minute details of individual ridges and furrows are permanent and do not change with time except by routine injury, scratches, and scarring, as may be seen in Fig. 5 and Fig. 9 [15].

The uniqueness of a fingerprint is exclusively determined by the local ridge characteristics and their relationships. Fingerprint matching generally depends on the comparison of local ridge characteristics and their relationships [14], [11], [17]. A total of 150 different local ridge characteristics, called minute details, have been identified [14]. These local ridge characteristics are not evenly distributed. Most of them depend heavily on the impression conditions and quality of fingerprints and are rarely observed in fingerprints. The two most prominent ridge characteristics, called minutiae, are *ridge ending* and *ridge bifurcation*. A ridge ending is defined as the point where a ridge ends abruptly. A ridge bifurcation is defined as the point where a ridge forks or diverges into branch ridges. A fingerprint typically contains about 40 to 100 minutiae. Examples of minutiae are shown in Fig. 5c. For a given fingerprint, a minutia can be characterized by its type, its x and y coordinates, and its direction, θ, whose definitions are also shown in Fig. 5c.

Fingerprint verification consists of two main stages [11], [14]:

1) minutiae extraction and
2) minutiae matching.

Fig. 5. Fingerprints and minutiae. (a) and (b) Two different impressions of the same finger. (c) Ridge ending and ridge bifurcation.

Fig. 6. Results of our minutiae extraction algorithm on a fingerprint image (512×512) captured with an optical scanner. (a) Input image. (b) Orientation field. (c) Ridge map. (d) Extracted minutiae.

Due to a number of factors such as aberrant formations of epidermal ridges of fingerprints, postnatal marks, occupational marks, problems with acquisition devices, etc., acquired fingerprint images may not always have well-defined ridge structures. Thus, a reliable minutiae extraction algorithm should not assume perfect ridge structures and should degrade gracefully with the quality of fingerprint images. We have developed a minutiae extraction algorithm [11] based on the algorithm proposed in [20]. It mainly consists of three steps:

1) *orientation field* (*ridge flow*) *estimation*, in which the orientation field of input fingerprint images is estimated and the region of interest is located,
2) *ridge extraction*, in which ridges are extracted and thinned, and
3) *minutiae detection and postprocessing*, in which minutiae are extracted from the thinned ridge maps and refined.

For each detected minutia, the following parameters are recorded:

- x-coordinate,
- y-coordinate,
- orientation, which is defined as the local ridge orientation of the associated ridge, and
- the associated ridge.

The recorded ridges which are used for alignment in the minutiae matching are represented as one-dimensional discrete signals which are normalized by the average inter-ridge distance. In an automatic fingerprint identification, ridge endings and ridge bifurcations are usually not differentiated from one another. Therefore, no minutiae type information is recorded. A minutia is completely determined by its position and orientation. Fig. 6 shows the results of our minutiae extraction algorithm on a fingerprint image captured with an optical scanner.

The minutiae matching determines whether two minutiae patterns are from the same finger or not. A similarity metric between two minutiae patterns is defined and a thresholding on the similarity value is performed. By representing minutiae patterns as two-dimensional "elastic" point patterns, the minutiae matching may be accomplished by an "elastic" point pattern matching as long as it can automatically establish minutiae correspondences (in the presence of translation, rotation, and deformations) and detect spurious minutiae and missing minutiae. We have developed an alignment-based "elastic" matching algorithm [11], which is capable of finding the correspondences between minutiae without resorting to an exhaustive search and has the ability to adaptively compensate for the nonlinear deformations and inexact transformations between different fingerprints. The alignment-based matching algorithm decomposes the minutiae matching into two stages:

1) *Alignment stage*, where transformations such as translation, rotation, and scaling between an input and a template in the database are estimated, and the input minutiae are aligned with the template minutiae according to the estimated parameters; and
2) *Matching stage*, where both the input minutiae and the template minutiae are converted to "strings" in the polar coordinate system, and an "elastic" string matching algorithm is used to match the resulting strings, and

finally, the normalized number of corresponding minutiae pairs is reported.

Let

$$P = \left(\left(x_1^P, y_1^P, \theta_1^P \right)^T, \ldots, \left(x_p^P, y_p^P, \theta_p^P \right)^T \right)$$

and

$$Q = \left(\left(x_1^Q, y_1^Q, \theta_1^Q \right)^T, \ldots, \left(x_q^Q, y_q^Q, \theta_q^Q \right)^T \right)$$

denote the p minutiae in the template and the q minutiae in the input image, respectively. The alignment-based matching algorithm is depicted as follows:

1) Estimate the translation and rotation parameters between the ridge associated with each input minutia and the ridge associated with each template minutia and align the two minutiae patterns according to the estimated parameters.
2) Convert the template pattern and input pattern into the polar coordinate representations with respect to the corresponding minutiae on which alignment is achieved and represent them as two symbolic strings by concatenating each minutia in an increasing order of radial angles:

$$P^* = \left(\left(r_1^P, e_1^P, \theta_1^P \right)^T, \ldots, \left(r_p^P, e_p^P, \theta_p^P \right)^T \right) \quad (5)$$

$$Q^* = \left(\left(r_1^Q, e_1^Q, \theta_1^Q \right)^T, \ldots, \left(r_q^Q, e_q^Q, \theta_q^Q \right)^T \right), \quad (6)$$

where r_i^P, e_i^P, and θ_i^P represent the corresponding radius, radial angle, and normalized minutiae orientation with respect to the reference minutiae, (x, y, θ), respectively.
3) Match the resulting strings P^* and Q^* with a modified dynamic-programming algorithm to find the "edit distance" between P^* and Q^*.
4) Use the minimum edit distance between P^* and Q^* to establish the correspondence of the minutiae between P^* and Q^*. The matching score, S, is then defined as:

$$S = \frac{100 M_{PQ}^2}{pq}, \quad (7)$$

where M_{PQ} is the number of minutiae which fall in the bounding boxes of template minutiae. The bounding box of a minutia specifies the allowable tolerance in the positions of the corresponding input minutiae with respect to the template minutiae. Fig. 7 shows an example of minutiae matching.

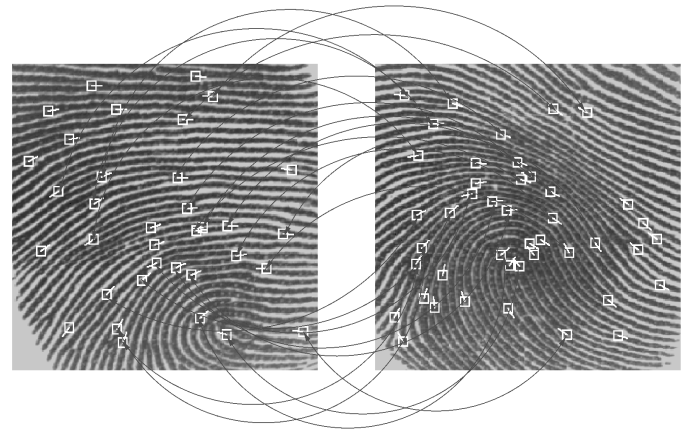


Fig. 7. Fingerprint matching.

4 Decision Fusion

Decision fusion which integrates multiple cues has proved beneficial for improving the accuracy of a recognition system [2], [3], [13]. Generally, multiple cues may be integrated at one of the following three different levels [3]:

1) Abstract level; the output from each module is only a set of possible labels without any confidence associated with the labels; in this case, the simple majority rule may be employed to reach a more reliable decision [26];
2) Rank level; the output from each module is a set of possible labels ranked by decreasing confidence values, but the confidence values themselves are not specified;
3) Measurement level; the output from each module is a set of possible labels with associated confidence values; in this case, more accurate decisions can be made by integrating different confidence measures to a more informative confidence measure.

In our system, the decision fusion is designed to operate at the measurement level. Each of the top n possible identities established by the face recognition module is verified by the fingerprint verification module. In order to carry out such a decision fusion scheme, we need to define a measure that indicates the confidence of the decision criterion and a decision fusion criterion.

As discussed in Section 1, the confidence of a given decision criterion may be characterized by its FAR (false acceptance rate). In order to estimate FAR, the impostor distribution needs to be computed. How should we compute the impostor distribution? In practice, it can only be estimated from empirical data. But, this estimation problem requires some care. In the context of personal identification, the required FAR value is often a very small number ($\ll 1$ percent) [17]. If the parametric form of the underlying impostor distribution is not known, nonparametric techniques need to be used. In order to guarantee that the estimated impostor distribution is reliable for characterizing the small FARs, a *large* representative test set that satisfies the following two requirements is needed: It should be large enough to represent the population, and it should contain enough samples from each category of the population. The above requirements are not easily satisfied in practice. An extrapolation based on the knowledge of the parametric form of the underlying impostor distribution is needed.

4.1 Impostor Distribution for Fingerprint Verification

A model that can precisely characterize the impostor distribution of a minutia matching algorithm is not easy, since:

1) the minutiae in a fingerprint are distributed randomly in the region of interest;

2) the region of interest of each input fingerprint may be different;
3) each input fingerprint tends to have a different number of minutiae;
4) there may be a significant number of spurious minutiae and missing minutiae;
5) sensing, sampling, and feature extraction may result in errors in minutiae positions; and
6) sensed fingerprints may have different distortions.

However, it is possible to obtain a general model of the overall impostor distribution by making some simplifying assumptions.

Let us assume that the input fingerprint and the template have already been registered and the region of interest of both the input fingerprint and the template is of the same size, a $W \times W$ (for example, 500×500) region. The $W \times W$ region is tessellated into small cells of size $w \times w$ which are assumed to be sufficiently large (for example, 40×40) such that possible deformation and transformation errors are within the bound specified by the cell size. Therefore, there are a total of $\frac{W}{w} \times \frac{W}{w} \left(= N_c\right)$ different cells in the region of interest of a fingerprint. Further, assume that each fingerprint has the same number of minutiae, N_m ($\leq N_c$), which are distributed randomly in different cells and each cell contains at most one minutiae. Each minutia is directed towards one of the D (for example, eight) possible orientations with equal probability. Thus, for a given cell, the probability, P_{empty}, that the cell is empty with no minutiae present is $\frac{N_m}{N_c}$ and the probability, P, that the cell has a minutia that is directed toward a specific orientation is $\frac{1-P_{empty}}{D}$. A pair of corresponding minutiae between a template and an input is considered to be identical if and only if they are in the cells at the same position and directed in the same direction (see Fig. 8). With the above simplifying assumptions, the number of corresponding minutiae pairs between any two randomly selected minutiae patterns is a random variable, Y, which has a binomial distribution with parameters N_m and P [18]:

$$g(Y = y) = \frac{N_m!}{y!(N_m - y)!} P^y (1 - P)^{(N_m - y)}. \quad (8)$$

The probability that the number of corresponding minutiae pairs between any two sets of minutiae patterns is less than a given threshold value, y, is

$$G(y) = g(Y < y) = \sum_{k=0}^{y-1} g(k). \quad (9)$$

The decision made by the proposed minutiae matching algorithm for an input fingerprint and a template is based on the comparison of the "normalized" number of corresponding minutiae pairs against a threshold. Therefore, under the assumption that minutiae in the region of interest of fingerprints of different individuals are randomly distributed, the probability that an impostor, I, is accepted is $\{1 - G(y_I)\}$, where y_I is the number of corresponding minutiae pairs between the impostor and the individual whom the impostor claims to be.

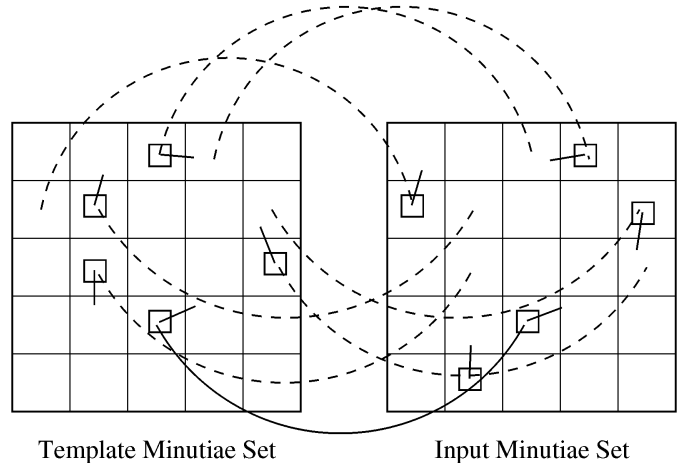


Fig. 8. Minutiae matching model, where a solid line indicates a match and a dashed line indicates a mismatch.

4.2 Impostor Distribution for Face Recognition

The characterization of impostor distribution for face recognition is more difficult. Due to the relatively low discrimination capability of face recognition, this module needs to keep the top n matches to improve the likelihood that the genuine individual will be identified if he or she is in the database.

Let $\Phi_1, \Phi_2, \ldots, \Phi_N$ be the N face templates stored in the database. The top n matches, $\Phi_1^r, \Phi_2^r, \ldots, \Phi_n^r$, are obtained by searching through the entire database, in which N comparisons are conducted explicitly (in the linear search case) or implicitly (in organized search cases such as the tree search). The top n matches are arranged in the increasing order of DFFS (Distance From Feature Space, Section 2) values. The smaller the DFFS value, the more likely it is that the match is correct. Since the relative distances between consecutive DFFSs are invariant to the mean shift of the DFFSs, it is beneficial to use relative instead of absolute DFFS values. The probability that a retrieved top n match is incorrect is different for different ranks. The impostor distribution should be a decreasing function of rank order and it is a function of both the relative DFFS values, Δ, and the rank order, i:

$$F_i(\Delta) P_{order}(i), \quad (10)$$

where $F_i(\Delta)$ represents the probability that the consecutive DFFS values between impostors and their claimed individuals at rank i are larger than a value Δ, and $P_{order}(i)$ represents the probability that the retrieved match at rank i is an impostor. In practice, $F_i(\Delta)$ and $P_{order}(i)$ need to be estimated from empirical data.

In order to simplify the analysis, we assume that each individual has only one face template in the database. Thus, there are a total of N individuals enrolled in the database and $I_1, I_2, \ldots, I_N$ are used as identity indicators. Let X^α denote the DFFS between an individual and his/her own template which is a random variable with density function $f^\alpha(X^\alpha)$ and let $X_1^\beta, X_2^\beta, \ldots, X_{N-1}^\beta$ denote the DFFS values between an individual and the templates of the other individuals in the database, which are random variables with density functions,

$f_1^\beta(X_1^\beta), f_2^\beta(X_2^\beta), \ldots, f_{N-1}^\beta(X_{N-1}^\beta)$, respectively. Assume that X^α and $X_1^\beta, X_2^\beta, \ldots, X_{N-1}^\beta$ are statistically independent and $f_1^\beta(X_1^\beta) = f_2^\beta(X_2^\beta) = \ldots f_{N-1}^\beta(X_{N-1}^\beta) = f^\beta(X^\beta)$. For an individual, Π, which has a template stored in the database, $\{\Phi_1, \Phi_2, ..., \Phi_N\}$, the rank, I, of X^α among $X_1^\beta, X_2^\beta, \ldots, X_{N-1}^\beta$ is a random variable with probability

$$P(I = i) = \frac{(N-1)!}{i!(N-1-i)!} p^i (1-p)^{(N-1-i)}, \quad (11)$$

where

$$p = \int_{-\infty}^{\infty} \int_{-\infty}^{X_\alpha} f^\alpha(X^\alpha) f^\beta(X^\beta) dX^\beta dX^\alpha. \quad (12)$$

When $p \ll 1$ and N is sufficiently large, $P(I)$ may be approximated by a Poisson distribution [18],

$$P(I) \doteq \frac{e^{(-a)} a^I}{I!}, \quad (13)$$

where $a \doteq np$. Obviously, $P(I)$ is exactly the probability that matches at rank i are genuine individuals. Therefore,

$$P_{order}(i) = 1 - P(I = i). \quad (14)$$

Although the assumption that $X_1^\beta, X_2^\beta, \ldots, X_{N-1}^\beta$ are *i.i.d.* may not be true in practice, it is still reasonable to use the above parametric form to estimate the probability that retrieved matches at rank i are impostors. Our experimental results support this claim.

Without any loss of generality, we assume that, for a given individual, Π, $X_1^\beta, X_2^\beta, \ldots, X_{N-1}^\beta$ are arranged in increasing order of values. Define the non-negative distance between the $(i+1)$th and ith DFFS values as the ith DFFS distance,

$$\Delta_i = X_{i+1}^\beta - X_i^\beta, \quad 1 \le i \le N-1. \quad (15)$$

The distribution, $f_i(\Delta_i)$, of the ith distance, Δ_i, is obtained from the joint distribution $w_i(X^\beta, \Delta_i)$ of the ith value, X^β, and the ith distance, Δ_i,

$$f_i(\Delta_i) = \int_{-\infty}^{\infty} w_i(X^\beta, \Delta_i) dX^\beta, \quad (16)$$

$$w_i(X^\beta, \Delta_i) = CF^\beta(X^\beta)^{i-1}[1 - F^\beta(X^\beta + \Delta_i)]^{N-i} f^\beta(X^\beta) f^\beta(X^\beta + \Delta_i), \quad (17)$$

$$C = \frac{(N-1)!}{(i-1)!(N-2-i)!}, \quad (18)$$

where $F^\beta(X^\beta) = \int_{-\infty}^{X^\beta} f^\beta(X^\beta) dX^\beta$ [9]. With the distribution, $f_i(\Delta_i)$, of the ith distance defined, the probability that the DFFS of the impostor at rank i is larger than a threshold value, Δ, is

$$F_i(\Delta) = \int_{\Delta}^{\infty} f_i(\Delta_i) d\Delta_i. \quad (19)$$

The above equations do not make any assumptions about the distributions of $X_1^\beta, X_2^\beta, \ldots, X_{N-1}^\beta$ as long as they are *i.i.d.* The equations also hold even if the mean values of $X_1^\beta, X_2^\beta, \ldots, X_{N-1}^\beta$ shift. Therefore, it can tolerate, to a certain extent, DFFS variations which is a desirable property. In our system, we assume that $X_1^\beta, X_2^\beta, \ldots, X_{N-1}^\beta$ are distributed with a Gaussian distribution with unknown mean and variance.

4.3 Decision Fusion

The impostor distribution for face recognition and the impostor distribution for fingerprint verification provide confidence measures for each of the top n matches retrieved by face recognition module. Without a loss of generality, we assume that at most one of the n possible identities established by the face recognition module for a given individual is the genuine identity of the individual. The final decision by integration either rejects all the n possibilities or accepts only one of them as the genuine identity. In practice, it is usually specified that the FAR of the system should be less than a given value [17]. Therefore, the goal of decision fusion, in essence, is to derive a decision criterion which satisfies the FAR specification.

It is reasonable to assume that the DFFS between two different individuals is statistically independent of the fingerprint matching score between them; facial similarity between two individuals does not imply that they have similar fingerprints, and vice versa. This assumption should not be confused with the situation where an impostor tries to fool the system by counterfeiting the face and/or fingerprints of the genuine individual. Let $F_i(\Delta)P_{order}(i)$ and $G(Y)$ denote the impostor distribution at rank i for face-recognition and fingerprint-verification modules, respectively. The composite impostor distribution at rank i may be defined as

$$H_i(\Delta, Y) = F_i(\Delta)P_{order}(i)G(Y). \quad (20)$$

Let $I_1, I_2, ..., I_n$ denote the n possible identities established by face recognition, $\{X_1, X_2, ..., X_n\}$ denote the corresponding n DFFSs, $\{Y_1, Y_2, ..., Y_n\}$ denote the corresponding n fingerprint matching scores, and FAR_o denote the specified value of FAR. The final decision, $ID(\Pi)$, for a given individual Π is determined by the following criterion:

$$ID(\Pi) = \begin{cases} I_k & \text{if} \begin{cases} H_k(\Delta_k, Y_k) < FAR_o, \text{and} \\ H_k(\Delta_k, Y_k) = \min\{H_1(\Delta_1, Y_1), \ldots, H_n(\Delta_n, Y_n)\} \end{cases} \\ \text{imposter} & \text{otherwise} \end{cases} \quad (21)$$

where $\Delta_i = X_{i+1} - X_i$. Since $H_i(\Delta, Y)$ defines the probability that an impostor is accepted at rank i with consecutive relative DFFS, Δ, and fingerprint matching score, Y, the above decision criterion satisfies the FAR specification.

Note that the decision criterion in (21) depends on the number of individuals, N, enrolled in the database, since F_i depends on N. However, it does not mean that F_i has to be recomputed whenever a new individual is enrolled in the database. In fact, if $N \gg 1$, the corresponding F_is for different values of N are quite similar to one another. On the other hand, the decision criterion still satisfies the FAR specification when N increases, though it may not be able to take full advantage of the information contained in the N comparisons. In practice, an update scheme which recomputes the decision criterion whenever the number of

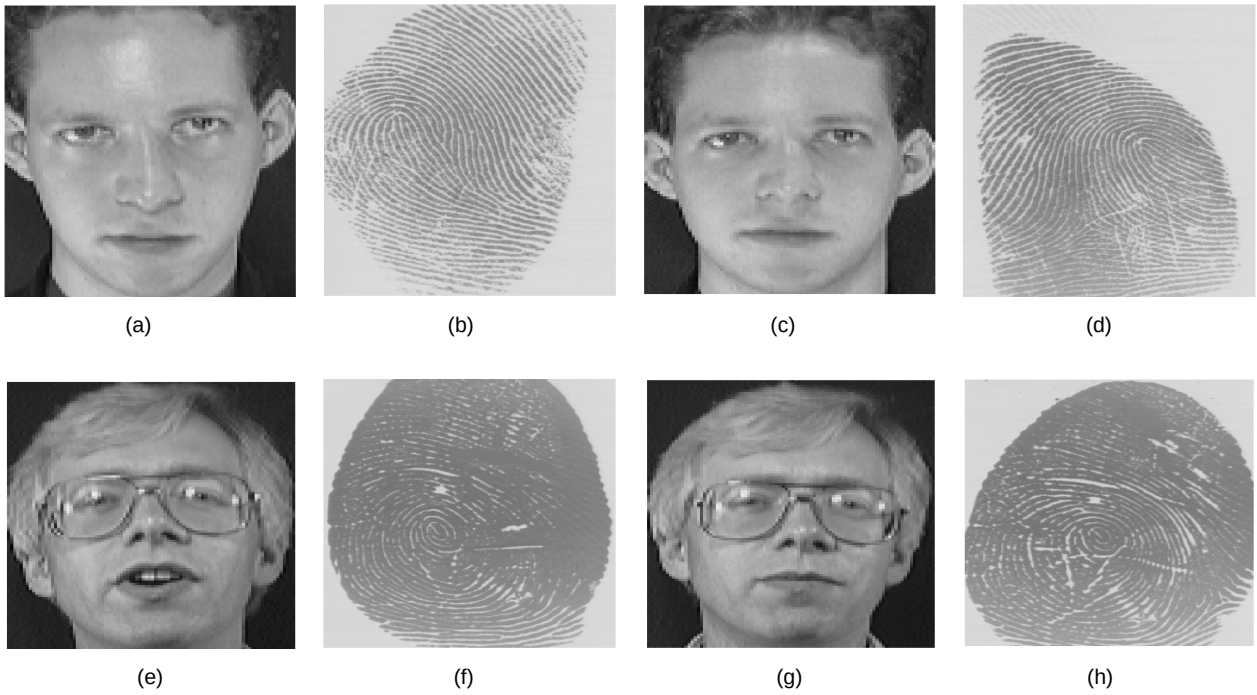


Fig. 9. Face and fingerprint pairs; the face images (92×112) are from the Olivetti Research Lab; the fingerprint images (640×480) are captured with a scanner manufactured by Digital Biometrics.

added individuals is larger than a prespecified value can be used to guarantee that the decision criterion exploits all the available information.

5 Experimental Results

The integrated biometric system was tested on the MSU fingerprint database and a public domain face database. The MSU fingerprint database contains a total of 1,500 fingerprint images (640×480) from 150 individuals with 10 images per individual, which were captured with an optical scanner manufactured by Digital Biometrics. When these fingerprint images were captured, no restrictions on the position, orientation, and impression pressure were imposed. The fingerprint images vary in quality. Approximately 90 percent of the fingerprint images in the MSU database are of reasonable quality similar to the images shown in Fig. 9b and Fig. 9d. Images of poor quality with examples shown in Fig. 9f and Fig. 9h are mainly due to large creases and smudges in ridges, dryness of the impressed finger, and high impression pressure. The face database contains a total of 1,132 images of 86 individuals; 400 images of 40 individuals with 10 images per individual are from the Olivetti Research Lab, 300 images of 30 individuals with 10 images per individual are from the University of Bern, and 432 images of 16 individuals with 27 images per individual are from the MIT Media Lab. The images were resampled from the original sizes to a fixed size of 92×112 and normalized to zero mean.

We randomly selected 640 fingerprints of 64 individuals as the training set and the remaining as the test set. The mean and standard deviation of the impostor distribution (Fig. 10a) were estimated to be 0.70 and 0.64 from the 403,200 (640×630) impostor matching scores of "all against all" verification test by fitting the probability model described in Section 4.1, respectively. A total of 542 face images were used as training samples. Since variations in position, orientation, scale, and illumination exist in the face database, the 542 training samples were selected such that the representative views are included. Eigenfaces were estimated from the 542 training samples and the first 64 eigenfaces were used for face recognition. The top $n = 5$ impostor distributions were approximated. Generally, the larger the value of n, the lower the false reject rate of face recognition. However, as n increases, more candidates need to be verified by fingerprint verification. There is obviously a trade-off between the accuracy and speed of a biometric system. Fig. 10b shows the impostor distribution at rank no. 1.

We randomly assigned each of the remaining 86 individuals in the MSU fingerprint database to an individual in the face database (see Fig. 9 for some examples). Since the DFFS value between two different individuals is statistically independent of the fingerprint matching scores between the two individuals, such a random assignment of a face to a fingerprint is admissible. One fingerprint for each individual is randomly selected as the template for the individual. To simulate the practical identification scenario, each of the remaining 590 faces was paired with a fingerprint to produce a test pair. In the test, with a prespecified confidence value (FAR), for each of the 590 fingerprint and face pairs, the top five matches are retrieved using face recognition. Then fingerprint verification is applied to each of the top five matches, and a final decision is made by decision fusion.

The prespecified FAR for a biometric system is usually very small (< 0.0001). In order to demonstrate that the biometric system does meet such a specification, a large number of representative samples are needed. Unfortunately,

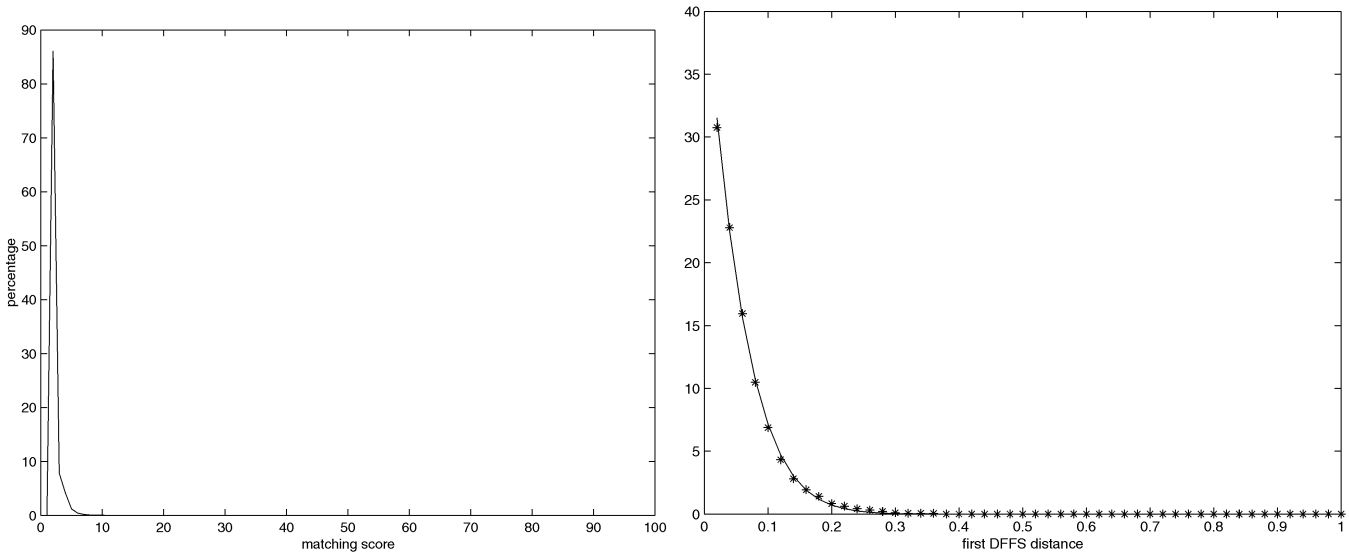


Fig. 10. Impostor distributions. (a) Impostor distribution for fingerprint verification; the mean and standard deviation of the impostor distribution are estimated to be 0.70 and 0.64, respectively. (b) The impostor distribution for face recognition at rank No. 1, where the stars (*) represent empirical data and the solid curve represents the fitted distribution; the mean square error between the empirical distribution and the fitted distribution is 0.0014.

obtaining such a large number of test samples is both expensive and time consuming. In our test, we reuse faces by different assignment practices—each time, a different fingerprint is assigned to a given face to form a face and fingerprint probe pair. Obviously, such a reuse scheme might result in unjustified performance improvement. In order to diminish the possible gain in performance due to such a reuse scheme, we multiplied the estimated impostor distribution for face recognition by a constant of 1.25, which essentially reduces contribution of face recognition to the final decision by a factor of 1.25. On the other hand, fingerprint verification operates in the one-to-one verification mode, so different assignments may be deemed as different impostor forgeries. Therefore, the test results using such a random assignment scheme are able to reasonably estimate the underlying performance numbers. In our test, 1,000 different assignments were tried. A total of 590,000 ($590 \times 1{,}000$) face and fingerprint test pairs were generated and tested. The FRRs of our system with respect to different prespecified FARs, as well as the FRRs obtained by "all-to-all" verifications using only fingerprints ($2{,}235{,}000 = 1{,}500 \times 1{,}490$ tests) or faces ($342{,}750 = 350 \times (590 - 5) + 240 \times (590 - 15)$ tests) are listed in Table 1. Note that the FRRs in integration column include the error rate (1.8 percent) of genuine individuals not present in the top five matches. The receiver operating curves are plotted in Fig. 11, in which the authentic acceptance rate (the percentage of genuine individuals being accepted, i.e., 1 – FRR) is plotted against FAR. We can conclude from these test results that the integration of fingerprints and faces does result in a significantly better recognition performance.

In order for an automatic personal identification system to be acceptable in practice, the response time of the system needs to be within a few seconds. Table 2 shows that our implemented system does meet the response time requirement.

6 Summary and Conclusions

We have developed a prototype biometric system which integrates faces and fingerprints in authenticating a personal identification. The proposed system overcomes the limitations of both face-recognition systems and fingerprint-verification systems. The integrated system operates in the identification mode. The decision-fusion scheme formulated in the system enables performance improvement by integrating multiple cues with different confidence measures. Experimental results demonstrate that our system performs very well. It meets the response time as well as the accuracy requirements.

TABLE 1
False Reject Rates (FRR) on the Test Set With Different Values of FAR

FAR	False Reject Rates (FRR)		
	Face	Fingerprint	Integration
1%	15.8%	3.9%	1.8%
0.1%	42.2%	6.9%	4.4%
0.01%	61.2%	10.6%	6.6%
0.001%	64.1%	14.9%	9.8%

The false reject rates of face recognition are obtained based on 342,750 pairwise comparisons; the false reject rates of fingerprint verification are obtained based on 2,235,000 pairwise comparisons; the false reject rates of the integrated system are obtained based on 590,000 probes.

TABLE 2
Average CPU Time for One Test on a Sun SPARC 20 Workstation.

Face Recognition (seconds)	Fingerprint Verification (seconds)	Total (seconds)
0.9	3.2	4.1

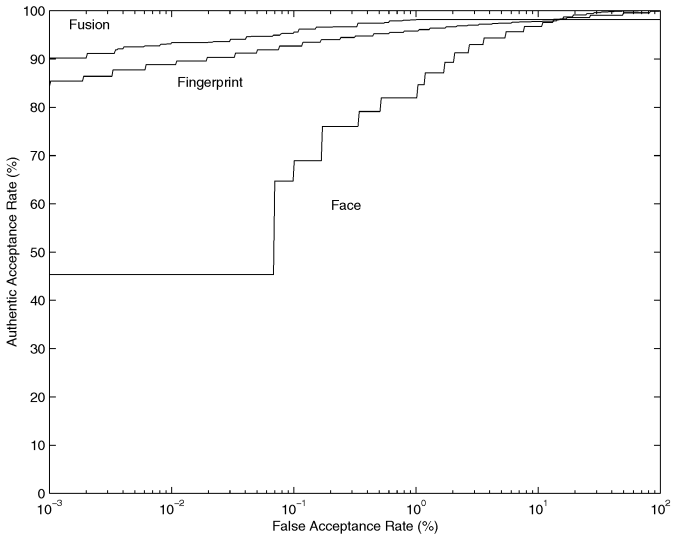


Fig. 11. Receiver operating curves; the vertical axis is (1–FRR).

The decision-fusion scheme formulated in this paper may be applied to similar scenario in other domains to provide a better discrimination performance. For example, in image database retrieval, a less reliable but computationally attractive algorithm may be used to retrieve the top n matches; then a more reliable, but computationally more expensive algorithm may be used to verify the top n matches; and finally an integrated decision criterion may be used to reach a more reliable decision.

We must point out that the proposed system has been designed for a template database containing several thousand templates. Since it has not yet been shown that face recognition is sufficiently efficient in correctly retrieving a small number of top matches from a huge template database with millions of templates, our approach may not scale up very well. In addition, our decision fusion scheme assumes that the similarity values between faces are statistically independent of the similarity values between fingerprints. While the assumption is valid for fingerprints and faces, it may not be true for other biometric characteristics.

The specified FAR of a deployed biometric system is usually a very small number ($\ll 1$ percent). In order to provide a more convincing demonstration that the system can meet such a specification, large representative test samples are needed. We are in the process of conducting such a test on a larger face and fingerprint database.

ACKNOWLEDGMENTS

We gratefully acknowledge our many useful discussions with Sharath Pankanti and Ruud Bolle of the IBM T. J. Watson Research Lab.

REFERENCES

[1] J. Atick, P. Griffin, and A. Redlich, "Statistical Approach to Shape From Shading: Reconstruction of 3D Face Surfaces From Single 2D Images," *Neural Computation*, to appear.

[2] E.S. Bigun, J. Bigun, B. Duc, and S. Fischer, "Expert Conciliation for Multi Modal Person Authentication Systems by Bayesian Statistics," *Proc. First Int'l Conf. Audio Video-Based Personal Authentication*, pp. 327–334, Crans-Montana, Switzerland, Mar. 1997.

[3] R. Brunelli and D. Falavigna, "Personal Identification Using Multiple Cues," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 17, no. 10, pp. 955–966, Oct. 1995.

[4] R. Brunelli and T. Poggio, "Face Recognition: Features Versus Templates," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 15, no. 10, pp. 1,042–1,052, Oct. 1993.

[5] R. Chellappa, C. Wilson, and A. Sirohey, "Human and Machine Recognition of Faces: A Survey," *Proc. IEEE*, vol. 83, no. 5, pp. 705–740, 1995.

[6] R. Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues," *Information Technology & People*, vol. 7, no. 4, pp. 6–37, 1994.

[7] J.G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1,148–1,161, Nov. 1993.

[8] S.G. Davies, "Touching Big Brother: How Biometric Technology Will Fuse Flesh and Machine," *Information Technology & People*, vol. 7, no. 4, pp. 60–69, 1994.

[9] E.J. Gumbel, *Statistics of Extremes*. New York: Columbia Univ. Press, 1958.

[10] Z. Hong, "Algebraic Feature Extraction of Image for Recognition," *Pattern Recognition*, vol. 24, no. 2, pp. 211–219, 1991.

[11] A. Jain, L. Hong, and R. Bolle, "On-Line Fingerprint Verification," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 19, no. 4, pp. 302–314, Apr. 1997.

[12] M. Kirby and L. Sirovich, "Application of the Karhunen-Loeve Procedure for the Characterization of Human Faces," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 12, no. 1, pp. 103–108, Jan. 1990.

[13] J. Kittler, Y. Li, J. Matas, and M.U. Sanchez, "Combining Evidence in Multimodal Personal Identity Recognition Systems," *Proc. First Int'l Conf. Audio Video-Based Personal Authentication*, pp. 327–334, Crans-Montana, Switzerland, Mar. 1997.

[14] H.C. Lee and R.E. Gaensslen, *Advances in Fingerprint Technology*. New York: Elsevier, 1991.

[15] A. Moenssens, *Fingerprint Techniques*. London: Chilton Book Company, 1971.

[16] V. Nalwa, "Automatic On-Line Signature Verification," *Proc. IEEE*, vol. 85, no. 2, pp. 213–239, 1997.

[17] E. Newham, *The Biometric Report*. New York: SJB Services, 1995.

[18] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*. New York: McGraw-Hill, 1965.

[19] P.J. Phillips, P.J. Rauss, and S.Z. Der, *FERET* (*Face Recognition Technology*) *Recognition Algorithm Development and Test Results*. Adelphi, Md.: U.S. government publication, ALR-TR-995, Army Research Laboratory, 1996.

[20] N. Ratha, S. Chen, and A.K. Jain, "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images," *Pattern Recognition*, vol. 28, no. 11, pp. 1,657–1,672, 1995.

[21] N. Ratha, K. Karu, S. Chen, and A.K. Jain, "A Real-Time Matching System for Large Fingerprint Database," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 18, no. 8, pp. 799–813, Aug. 1996.

[22] L. Sirovich and M. Kirby, "Low Dimensional Procedure for Characterization of Human Faces," *J. Optical Soc. Am.*, vol. 4, no. 3, pp. 519–524, 1987.

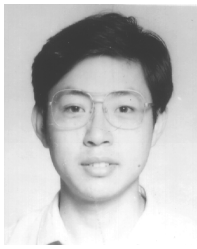
[23] D.L. Swets and J. Weng, "Using Discriminant Eigenfeatures for Image Retrieval," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 18, no. 8, pp. 831–836, Aug. 1996.

[24] M. Turk and A. Pentland, "Eigenfaces for Recognition," *J. Cognitive Neuroscience*, vol. 3, no. 1, pp. 71–86, 1991.

[25] D. Valentin, H. Abdi, A.J. O'Toole, and G. Cottrell, "Connectionist Models of Face Processing: A Survey," *Pattern Recognition*, vol. 27, no. 9, pp. 1,209–1,230, 1994.

[26] Y.A. Zuev and S.K. Ivanov, "The Voting as a Way to Increase the Decision Reliability," *Proc. Foundations of Information/Decision Fusion With Applications to Eng. Problems*, pp. 206–210, Washington, D.C., Aug. 1996.

[27] A.K. Jain, R. Bolle, and S. Pankanti, eds., *Biometrics: Personal Identification in Networked Society*. Norwell, Mass.: Kluwer Academic Publishers, in press.



Lin Hong received the BS and MS degrees in computer science from Sichuan University, China, in 1987 and 1990, respectively, and the PhD degree in computer science from Michigan State University in 1998. His currently research interests include multimedia, biometrics, data mining, pattern recognition, image processing, and computer vision application. He is now working at Visionics Corporation.

Anil Jain is a university distinguished professor and chair of the Department of Computer Science at Michigan State University. His research interests include statistical pattern recognition, Markov random fields, texture analysis, neural networks, document image analysis, fingerprint matching, and 3D object recognition. He received the best paper awards in 1987 and 1991 and certificates for outstanding contributions in 1976, 1979, 1992, and 1997 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* (1990-1994). He is the coauthor of *Algorithms for Clustering Data* (Prentice-Hall, 1988), has edited the book *Real-Time Object Measurement and Classification* (Springer-Verlag, 1988), and coedited the books, *Analysis and Interpretation of Range Images* (Springer-Verlag, 1989), *Markov Random Fields* (Academic Press, 1992), *Artificial Neural Networks and Pattern Recognition* (Elsevier, 1993), *3D Object Recognition* (Elsevier, 1993), and *BIOMETRICS: Personal Identification in Networked Society* to be published by Kluwer in 1998. He is a fellow of the IEEE and IAPR and has received a Fulbright research award.