Integrating Faces and Fingerprints for Personal Identification

Lin Hong and Anil Jain
Michigan State University
Department of Computer Science
East Lansing, MI 48824
{honglin,jain}@cps.msu.edu

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 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 schema 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.

Key words:

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 inter-connected electronic devices. The capability of automatically establishing the identity of individuals is thus essential to the reliability of these transactions. Traditional personal identification technologies 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 imposter who fraudulently acquires the access privilege [16]. Biometrics is a technology which identifies an individual based on his/her physiological or behavioral characteristics. It relies on “something which you are” to make personal identification and, therefore, inherently has the capability to differentiate between a genuine individual and a fraudulent imposter [16].

A human physiological or behavioral characteristic can be used in a biometric system as long as (i) every individual has the characteristic; (ii) no two individuals are the same in terms of the characteristic; (iii) the characteristic is not volatile; (iv) the characteristic can be measured quantitatively; (v) people are willing to accept the characteristic as an identity indicator; and (vi) it is not easily counterfeited. Currently, there are mainly nine different biometric techniques that are either widely used or under investigation, including face, facial thermograms, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, and voice-print (examples are shown in Figure 1) for [6, 8, 7, 16]. Each of these biometric
techniques has its own advantages and disadvantages and is admissible depending on the application.

![Face, Facial thermograms, Fingerprint, Hand vein, Retinal scan]

Figure 1. Examples of biometric characteristic.

A generic biometric system architecture is depicted in Figure 2. Logically, it can be divided into two modules: (i) enrollment module and (ii) identification module. The enrollment module is responsible for enrolling individuals into the biometric system such that the biometric system can identify the individuals in the operation phase. During the enrollment process, the biometric characteristic of an individual is first scanned by the biometric reader to produce a raw digital representation of the characteristic. In order to facilitate the matching, the digital data is further processed by a feature extractor to generate a compact but expressive representation, called a template. Depending on the application, the template may be stored in the central database of the biometric system or be recorded in the magnetic card issued to the individual. The identification module is responsible for identifying individuals at the point-of-access. In the operation phase, biometric characteristic of the individual to be identified is presented to the biometric reader and a compact representation that is of the same format as the template is produced. The sensed representation is fed to the feature matcher which compares it to the stored template(s) to establish the identity.
A biometric system may operate in: (i) the verification mode, or (ii) the identification mode [16]. A biometric system operating in the verification mode authenticates an individual’s identity by comparing the individual with his/her own template(s). 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. 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 [16]. 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. However, for an identification system, both the accuracy and speed are critical. An identification system needs to explore the entire template database tc
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, it is still not practical to conduct real-time searching even on a relatively small size fingerprint database (several thousand images) without dedicated hardware matchers and indexing mechanisms such as fingerprint class indexing [7]. On the other hand, it is feasible to design a face recognition system operating in the identification mode, because (i) face comparison is a relatively less expensive operation, and (ii) efficient indexing techniques are available and the performance is admissible [20].

A biometric system establishes the identity of an individual by comparing the sensed representations of the individual’s biometric characteristic. Due to intra-class 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, 16]. For each type of decision, there are two possible outcomes, true or false. Therefore, there are a total of four possible outcomes: (i) a genuine individual is accepted, (ii) a genuine individual is rejected, (iii) an impostor is rejected, and (iv) an impostor is accepted. Outcomes (i) and (iii) are correct whereas (ii) and (iv) 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: (i) false acceptance rate (FAR), an impostor being accepted as a genuine individual and (ii) false reject rate (FRR), a genuine individual being rejected as an impostor. A small FRR usually leads a larger FAR while a smaller FAR usually implies a larger FRR. Generally, the system performance requirement is specified in terms of FAR [16]. A FAR of
zero means that no impostor is accepted as a genuine individual.

Different biometric characteristics possess different discrimination capability in terms of FAR and FRR [16]. At the one extreme, we have biometric characteristics such as face and dynamic signature that are inherently better at accepting genuine individuals, but do not perform well in deterring impostors. For example, an individual can easily change his/her own facial appearance by makeup to fool human and face recognition systems (Figure 3). At the other extreme, we have the biometric characteristics such as retinal scans, fingerprints, and iris that are better at preventing impostors but are less efficient in identifying genuine individuals. Somewhere between these two extremes are those biometric characteristics such as hand geometry and hand vein which perform about the same at deterring impostors and accepting genuine individuals [16].
Figure 4. System architecture of the prototype integrated biometric identification system.

In order to build a biometric system that is able to (i) operate efficiently in identification mode and (ii) achieve desirable accuracy, an integration schema 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 schema which exploits all the information at the output of each approach can be use to made a more reliable decision. In this paper, we introduce a prototype integrated biometric system which make personal identification by integrating both faces and fingerprints. The prototype integrated biometric system shown in Figure 4 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 databases 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 intra-class variations are small.

During the past 25 years, a substantial amount of research effort has been devoted to face recognition [5, 22]. In the early 1970’s, face recognition was mainly based on measured facial attributes such as eyes, eyebrows, nose, lips, chin shape, etc. [5]. Due to insufficiency
of computational resources and lack of reliable feature extraction algorithms, only a very limited number tests were conducted and the recognition performance was far from desirable [5]. After the dormant 1980’s, there was a resurgence in face recognition research in the early 1990’s. In addition to continuing efforts on attribute-based techniques [5], a number of new face recognition techniques were proposed, including principle component analysis (PCA) [21], linear discriminant analysis (LDA) [20], singular value decomposition (SVD) [10], and a variety of neural network-based techniques [22]. The performance of these approaches are 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” [18].

Generally, there are two major tasks in face recognition: (i) locating faces in input images and (ii) recognizing the located faces. 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 for a biometric system using faces. Face recognition from a general view point also remains an open problem because transformations such as position, orientation, and scale and changes illumination produce substantially large intra-class variations [18]. Again, in the context of personal identification, the variations in acquired face images can be restricted to a certain limit, which enables the current techniques to achieve a desirable performance [5, 18].

In our system, the eigenface approach is used for the following reasons: (i) in the context of personal identification, the background, transformations, and illumination can be controlled, (ii) eigenface approach has a compact representation - a facial image can be
concisely represented by a feature vector with a few elements, (iii) it is feasible to index an eigenface-based template database using different indexing techniques such that the retrieval can be conducted efficiently [20], (iv) the eigenface approach is a generalized template matching approach which was demonstrated to be more accurate than the attribute-based approach [4].

The eigenface-based face recognition consists of the following two stages [21]: (i) training stage in which a set of 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 (ii) 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 value of $W \times H$ 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 dimension subspace using principle component analysis [21]. Let $\Psi_1, \Psi_2, \ldots, \Psi_N$ denote the $N$ $W \times H$-dimensional training vectors with zero-mean. Let the $M$ basis vectors, $u_1, u_2, \ldots, u_M$ be a set of orthonormal vectors that best describe the distribution of face images in the $M$-dimensional subspace (eigenspace), $MlN$. The $kth$ vector, $u_k, k = 1, 2, \ldots, M$, is computed such that [21]

$$\lambda_k = \frac{1}{N} \sum_{i=1}^{N} (u_k^T \Psi_i)^2$$

(1)

is maximum, subject to

$$u_i^T u_j = \begin{cases} 
1, & \text{if } i = j \\
0, & \text{otherwise}
\end{cases}$$

(2)

The value $\lambda_k$ is the $kth$ largest eigenvalue of the covariance matrix $\Sigma$ which can be estimated using the training samples by

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

(3)

The vector $u_k$ is the $kth$ eigenvector of the covariance matrix $\Sigma$ corresponding to $\lambda_k$.

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

$$\Phi_k = u^T \Psi_i, \ i = 1, 2, \cdots, N,$$  

(4)

where $u = (u_1, u_2, \ldots, u_M)$. Figure 5 shows the first 10 eigenfaces corresponding to the 10 largest eigenvalues.

In the operational phase, a detected face image, $\Gamma$, which is normalized to zero mean, is vectorized and projected onto the eigenfaces component according to $\Pi = u^T \Gamma$. With both training samples and test samples being projected onto $M$-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 [16]. Thus, a k-nearest neighbor classifier is typically used, in which the distance, $d$, called Distance From Feature Space (DFFS) [21] between a template, $\Phi$, and a test pattern, $\Pi$, is defined as $\|\Phi - \Pi\|$, where $\|\bullet\|$ means $L_2$ 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 [13]. It’s formation is determined by the initial conditions of the embryonic mesoderm from which it develops [13]. Humans have used fingerprints for personal identification for a long time. The biological properties of fingerprints are well understood which are summarized as follows: (i) individual epidermal ridges and furrows have different characteristics for
different fingerprints; \( (iii) \) the configuration types are individually variable, but they vary within limits which allow for systematic classification, \( (iii) \) the configurations and minute details of individual ridges and furrows are permanent and do not change with time [13].

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 [13, 11, 14, 16, 23]. A total of one hundred and fifty different local ridge characteristics, called minute details, have been identified [13]. 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 \( (i) \) ridge ending and \( (ii) \) 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 50 to 100 minutiae. Examples of minutiae are shown in Figure 6(c). For a given fingerprint, a minutiae can be characterized by its type, its \( x \) and
Figure 7. Results of our minutiae extraction algorithm on a fingerprint image (512 x 512) captured with an optical scanner.

y coordinates, and its direction, $\theta$, whose definitions are also shown in Figure 6(c).

Fingerprint verification consists of two main stages [11, 13]: (i) minutiae extraction and (ii) minutiae matching. 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 degrade gracefully with the quality of fingerprint images. We have developed a minutiae extraction algorithm [11] based on the algorithm proposed in [19]. It mainly consists of three steps: (i) orientation field estimation in which the orientation field of input fingerprint images is estimated and the region of interest is located, (ii) ridge extraction in which ridges are extracted and thinned, and (iii) minutiae detection and postprocessing in which minutiae are extracted from the thinned ridge maps and refined. For each detected minutiae, the following parameters are recorded: (i) x-coordinate, (ii) y-coordinate, (iii) orientation which is defined as the local ridge orientation of the associated ridge, and (iv) 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. Figure 7 shows the results of our minutiae extraction algorithm on a fingerprint image captured with an optical scanner.

Figure 8. Results of applying the matching algorithm to an input minutiae set and a template; (a) input minutiae set; (b) template minutiae set; (c) alignment result based on the minutiae marked with green circles; (d) matching result where template minutiae and their correspondences are connected by green lines.
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: (i) 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 (ii) 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.

4 Decision Fusion

Decision fusion which integrates multiple cues has proved beneficial for improving the accuracy of a recognition system [2, 3, 12]. Generally, multiple cues may be integrated at one of the following three different levels [3]: (i) Abstract level; the output from each module is only
a set of possible labels without any confidence information; in this case, the simple majority rule may be employed to reach a more reliable decision [24], (ii) Rank level; the output from each module is a set of possible labels ranked by decreasing confidence values, but the confidence value are not specified; (iii) 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 schema, (i) measures that indicate the confidence of the decision criterion need to be defined and (ii) a decision fusion criterion needs to be formulated.

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 ($\ll 1\%$) [16]. If the parametric form of the underlying impostor distribution is not known, non-parametric techniques need to be used. In order to guarantee that the estimated impostor distribution is reliable at characterizing the small FARs, a large representative test set that satisfy the following two requirements is needed (i) it should be large enough to represent the population and (ii) 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 Imposter Distribution for Fingerprint Verification

A model that can precisely characterize the imposter distribution of a minutiae matching algorithm is not easy, since (i) the minutiae in a fingerprint are distributed randomly in the region of interest; (ii) the region of interest of each fingerprint is different; (iii) each fingerprint tends to have a different number of minutiae; (iv) there are a significant number of spurious minutiae and missing minutiae; (v) sensing, sampling, and feature extraction may result in errors in minutiae positions; and (vi) sensed fingerprints may have different distortions. However, it is possible to obtain a general model of the overall imposter distribution by making some simplifying assumptions.

Let us assume that the region of interest of all fingerprints is of the same size, a $W \times H$ (for example, $500 \times 500$) region. The $W \times H$ region is tessellated into small cells of size $w \times h$ which are assumed to be sufficiently large (for example, $50 \times 50$) such that possible deformations and transformation errors are within the bound specified by the cell size. Therefore, there are a total of $\frac{W}{w} \times \frac{H}{h} (= N_c)$ different cells in the region of interest of a fingerprint. Assume that each fingerprint has the same number of minutiae, $N_m (\leq N_c)$, which are distributed randomly in different cells. Assume that each cell contains at most one minutiae. Each minutiae directs to one of the $D$ (for example, 8) possible directions with equal probability. Thus, for a given cell, the probability, $P_{\text{empty}}$, that the cell is empty is $\frac{N_m}{N_c}$ and the probability, $P$, that the cell has a minutiae directed in a specific direction is $\frac{1-P_{\text{empty}}}{D}$. 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. With the above 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 $P$ [17]:

$$g(Y) = \frac{N_m!}{Y!(N_m - Y)!} P^Y (1 - P)^{(N_m - Y)}.$$  \hspace{1cm} (5)

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

$$G(y) = g(Y < y) = \sum_{k=0}^{y-1} g(k).$$  \hspace{1cm} (6)

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. In practice, $g(Y)$ is usually approximated by a Gaussian distribution with unknown mean and variance.

### 4.2 Imposter 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 guarantee that the genuine individual will be identified if he or she is in the database. Generally, the probability that a retrieved match is incorrect is different for different ranks. The probability that the first match is incorrect tends to be lower than the probability that the second match is incorrect, the probability that the second match
is incorrect tends to be lower than the probability that the third match is incorrect, and so on. On the other hand, the top \( n \) matches are obtained by searching through the entire database, in which \( N \) comparisons need to be conducted explicitly (in the linear search case), or implicitly (in organized search cases such as the tree search), where \( N \) is the number of templates stored in the database. The top \( n \) matches arranged in the increasing order of DFFS (Distance From Feature Space, section 2) values is more informative and the relative distances between consecutive DFFSs can tolerate shifts in mean DFFS values. Therefore, the impostor distribution is different at different ranks and depends on relative DFFS, \( \Delta \): the impostor distribution at rank \( i \) depends on \( F_i(\Delta)P_{\text{order}}(i) \), where \( F_i(\Delta) \) represents the probability that the consecutive DFFS between impostors and their claimed individuals at rank \( i \) are larger than \( \Delta \) and \( P_{\text{order}}(i) \) represents the probability that the retrieved match at rank \( i \) is an impostor. In practice, \( F_i(\Delta) \) and \( P_{\text{order}}(i) \) need to be estimated from empirical data.

Let \( \Phi_1, \Phi_2, \ldots, \Phi_N \) be the \( N \) face templates stored in the database. 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 \( X^t \) denote the DFFS between an individual and his/her own template which is a random variable with density function \( f^t(X^t) \) and let \( X^f_1, X^f_2, \ldots, X^f_{N-1} \) denote the DFFSs between an individual and the templates of the other individuals in the database, which are random variables with density functions, \( f^f_1(X^f_1), f^f_2(X^f_2), \ldots, f^f_{N-1}(X^f_{N-1}) \), respectively. Assume that \( X^t \) and \( X^f_1, X^f_2, \ldots, X^f_{N-1} \) are statistically independent and \( f^t(X^t) = f^f_1(X^f_1) = \ldots = f^f_{N-1}(X^f_{N-1}) = f^f(X^f) \). For an individual, \( \Pi \), which has a template stored in the database, \( \{\Phi_1, \Phi_2, \ldots, \Phi_N\} \), the rank, \( I \), of \( X^t \) among \( X^f_1, X^f_2, \ldots, X^f_{N-1} \) is a random variable.
with probability

\[ P(I = i) = \frac{(N - 1)!}{i!(N - 1 - i)!} p^i (1 - p)^{(N - 1 - i)}, \quad (7) \]

where

\[ p = \int_{-\infty}^{\infty} \int_{-\infty}^{X_t} f(t)(X_t)f(X^t)dX^tdt. \quad (8) \]

When \( p \ll 1 \) and \( N \) is sufficiently large, \( P(I) \) may be approximated by a Poisson distribution [17].

\[ P(I) \approx \frac{e^{(-a)} a^I}{I!}, \quad (9) \]

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

\[ P_{order}(i) = 1 - P(I = i). \quad (10) \]

Although the assumption that \( X_1^f, X_2^f, ..., X_{N-1}^f \) 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, \( \Pi, X_1^f, X_2^f, ..., X_{N-1}^f \) 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,

$$\Delta_i = X^f_{i+1} - X^f_i, 1 \leq i \leq N - 1.$$  \hspace{1cm} (11)

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

$$f_i(\Delta_i) = \int_{-\infty}^{\infty} w_i(X^f, \Delta_i) dX^f,$$  \hspace{1cm} (12)

$$w_i(X^f, \Delta_i) = C F^f(X^f)^{N-1+i}[1 - F^f(X^f + \Delta_i)]^i f^f(X^f)f^f(X^f + \Delta_i),$$  \hspace{1cm} (13)

$$C = \frac{(N-1)!}{(i-1)!(N-2-i)!},$$  \hspace{1cm} (14)

where $F^f(X^f) = \int_{-\infty}^{X^f} f^f(X^f) dX^f$ [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, $\Delta$, is

$$F_i(\Delta) = \int_{\Delta}^{\infty} f_i(\Delta_i) d\Delta.$$  \hspace{1cm} (15)

The above equations hold even if the mean value of $X^f_1, X^f_2, ..., X^f_{N-1}$ shifts. Therefore, it can tolerate, to a certain extent, DFFS variations which is a desirable property.

### 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 may 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 should be less than a given value [16]. Therefore, the goal of decision
fusion, in essence, is to derive a decision criterion which satisfies the FAR specification.

It is safe to assume that the DFFS between two different individuals is statistically inde-
dependent of the fingerprint matching score between them; facial similarity between two indi-
viduals does not imply that they have similar fingerprints, and vice versa. Let $F_i(\Delta)P_{\text{order}(i)}$
and $G(Y)$ denote the impostor distribution at rank $i$ for face recognition and fingerprint veri-
fication modules, respectively. The composite impostor distribution at rank $i$ may be defined
as

$$H_i(\Delta, Y) = F_i(\Delta)P_{\text{order}(i)}G(Y).$$  \hfill (16)

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

$$ID(\Pi) = \begin{cases} I_k, & \text{if } \begin{cases} H_k(\Delta X_k, Y_k) < FAR_o, \text{ and} \\ H_k(\Delta X_k, Y_k) = \min\{H_1(\Delta X_1, Y_1), \ldots, H_n(\Delta X_n, Y_n)\} \end{cases} \\ \text{impostor, otherwise.} \end{cases}$$  \hfill (17)
where $\Delta X_i = X_{i+1} - X_i$. Since $H_i(\Delta, Y)$ defines the probability that an impostor is accepted at rank $i$ with consecutive relative DFFS, $\Delta$, and fingerprint matching score, $Y$, the above decision criterion satisfies the FAR specification.

5 Experimental Results

To test our system, the MSU fingerprint database and a public domain face databases are used. The MSU fingerprint database contains a total of 1,500 fingerprint images ($640 \times 480$) 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% of the fingerprint images in the MSU database are of reasonable quality similar to those images shown in Figures 9(b) and (d). Images of poor quality with examples shown in Figures 9(f) and (h) 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 MIT Media Lab. The images were re-sampled from the original sizes to a fixed size of $92 \times 112$ and normalized to zero mean.
Figure 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.

Figure 10. Impostor distributions; (a) impostor distribution for fingerprint verification; (b) the impostor distribution for face recognition at rank No. 1, where the stars (*) represent empirical data and the solid curve represents the fitting result.
<table>
<thead>
<tr>
<th>FAR</th>
<th>False Reject Rate (FRR)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Face</td>
</tr>
<tr>
<td>1%</td>
<td>15.8%</td>
</tr>
<tr>
<td>0.1%</td>
<td>42.2%</td>
</tr>
<tr>
<td>0.01%</td>
<td>61.2%</td>
</tr>
<tr>
<td>0.001%</td>
<td>64.1%</td>
</tr>
</tbody>
</table>

Table 1. False reject rates (FRR) on the test set with different values of FAR.

Figure 11. Receiver Operating Curves; the vertical axis is (1-FRR).

We randomly selected 640 fingerprints of 64 individuals as the training set and the remaining as the test set. The mean and variance of the impostor distribution (Figure 10(a)) 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. 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. The top 5 impostor distributions were approximated. Figure 10(b) 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 Figure 9 for some examples). Since the DFFS 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 pre-specified confidence value (FAR), for each of the 590 fingerprint and face pairs, the top 5 matches are retrieved using face recognition. Then fingerprint verification is applied to each of the top 5 matches and a final decision is made by decision fusion.

The pre-specified 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 set of representative samples (generally, \( \frac{10}{FAR} \)) are needed. Unfortunately, obtaining such a large number of test samples is both expensive and time consuming. In our test, we re-use faces by different assignment practices. In order to diminish the possible gain in performance due to such a re-use schema, we multiplied the estimated impostor distribution for face recognition by a constant of 1.25, which is sufficiently conservative. 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 schema are able to reasonably estimate the underlying performance numbers. In our test, 1000 different assignments were tried. A total of 590,000 (590 \times 1000) face and fingerprint test pairs were generated and tested. The FRRs of our system with respect to different pre-specified FARs, as well as the FRRs obtained by “all-to-all” verifications using
only fingerprints (2,235,000 = 1500 × 1490 tests) or faces (342,750 = 350 × (590 − 5) + 240 × (590 − 15) tests) are listed in Table 1. Note that the FRRs in integration column include the error rate (1.8%) of genuine individuals not present in the top 5 matches. The receiver operating curves are plotted in Figure 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 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 schema 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.
The decision fusion schema formulated in this paper may be applied to similar scenarios 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 a 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 schema 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 in other scenarios.

The specified FAR of a deployed biometric system is usually a very small number ($\ll 1\%$). 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 databases.

References


