F2ID: A Personal Identification System Using Faces and Fingerprints

Anil Jain, Lin Hong, and Yatin Kulkarni
Department of Computer Science
Michigan State University
East Lansing, MI 48824
{jain,honglin,kulkar10}@cps.msu.edu

Key words: Biometrics, Personal identification, Minutiae, Fingerprint matching, Face recognition, Eigenface, Decision fusion.

Abstract

A "real-time" automatic personal identification system should meet the conflicting dual requirements of accuracy and response time. In addition, it also should be user-friendly. We introduce a "medium-size" "real-time" automatic personal identification system, F2ID, which integrates faces and fingerprints to make a personal identification. F2ID overcomes some of the limitations of face recognition systems and fingerprint verification systems and can achieve a desirable identification accuracy with a tolerable response time. We have tested our system on a limited set of face and fingerprint images collected in a laboratory environment. Experimental results show that that our system meets both the identification accuracy as well as the speed requirements.

1 Introduction

In today's complex, geographically mobile, increasingly electronically wired information society, the ability to achieve highly accurate *automatic* personal identification is becoming very important [6, 2]. Traditional automatic personal identification technologies which are based on "something that you know," such as a Personal Identification Number (PIN), and/or "something that you have," such as an ID card have a number of inherent disadvantages. Tokens may be lost, stolen, forgotten, or misplaced. PIN may be forgotten or guessed by the impostors. All the traditional identification methods suffer from a common problem - they are unable to differentiate between an *authorized person* and an *imposter* who fraudulently acquires the "knowledge" or "token" of the authorized person [2, 3].

Biometrics refers to automatic identification of a person based on his physiological or behavioral characteristics [6, 3]. It is inherently more reliable and more capable in differentiating between an authorized person and a fraudulent imposter, since it requires that the person to be identified be physically present at the point-of-identification and relies on "something which you are or you do." Biometrics has the potential to become the dominant automatic personal identification in the near future [7]. Currently, there are mainly nine different biometric techniques that are either widely used or under development, including *face, facial thermograms, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, and voice-print* (Figure 1) [2, 7]. Each of these biometric techniques has its own advantages and disadvantages and is admissible depending on the application domain.

face facial thermograms fingerprint iris retinal scan

Figure 1: Examples of biometric characteristic.

We introduce a prototype automatic personal identification system, F2ID, which integrates two different biometric approaches (face recognition and fingerprint verification) to make a personal identification. In section 2, we introduce the architecture of the F2ID system and address the major design issues. Experimental results on a set of images collected in a laboratory environment are given in section 3. Finally, the summary and conclusions are given in section 4.

2 F2ID System

We are interested in designing a "real-time" *medium-size* fully automatic personal identification system. By "real-time" we mean that the system should have a response time which is tolerable to an online user, *i.e.* a couple of seconds. By medium-size we mean that the system is intended for an application domain where the total number of enrolled users is of the order of a few thousands. Such applications can be found in access control, information security, *etc.* in a small to medium size environment. For example, such a system can be integrated in an intra-net environment for user identification.

It is very difficult to build a fully automatic identification system based solely on a single biometrics, that is able to (*i*) operate in "real-time" and (*ii*) achieve high accuracy. An integration schema which combines two or more different biometric approaches is likely to provide a feasible solution [4]. A biometrics that is suitable for operating in the "real-time" identification mode may be used to index the template database and a different biometrics that is reliable in deterring impostors may be used to guarantee the accuracy. In addition, each biometrics provides a certain confidence about the identity being established. A decision fusion schema which exploits all the information at the output of each individual biometrics can be used to make a more reliable decision.

In the context of personal identification, face recognition refers to static, controlled full frontal portrait recognition [1], which "was developed and was sufficiently mature that it can be ported to real-time experimental/demonstration system" [8]. Face recognition is computationally inexpensive and efficient indexing techniques are available for face recognition [9]. Therefore, it is feasible to design a face recognition system operating in the identification

mode. On the other hand, fingerprint verification is computationally demanding, because it is based on point pattern matching in the presence of rotation, translation, position errors, non-linear distortions, spurious points, and missing points [5]. However, fingerprints matching (*i*) is one of the most reliable personal identification technique, and (*ii*) has long been established and justified [7]. It is feasible to use fingerprint verification to guarantee identification accuracy. In fact, face recognition and fingerprint verification complement each other in terms of speed and identification accuracy.

An integrated biometric system which makes personal identification by integrating face recognition and fingerprint verification is able to operate efficiently in identification mode and achieve the desirable accuracy. We introduce the F2ID system, an integrated automatic personal identification system which operates in a "real-time" identification mode with a very high reliability.

2.1 System Architecture

The F2ID system mainly consists of four components: (*i*) image acquisition module, (*ii*) template database, (*iii*) enrollment module, and (*iv*) identification module. The system block diagram is shown in figure 2. The image acquisition module is responsible for acquiring face and fingerprint images of a user who intends to access the system. The template database is a physical database which contains all the template records of the users who are enrolled in the system.

The task of the enrollment module is system management which includes user enrollment, user deletion, user update, training, system parameter specification, *etc.* Each enrolled user is represented by a record which contains the profile of the user and a number of representative face templates and fingerprint templates. For face images, the eigenface representation of the input face images is generated by projecting the original input images to the eigenspace. For the fingerprint images, a minutiae extraction algorithm is applied and the minutiae patterns which are the commonly used representation of fingerprints are extracted [5].

The identification procedure essentially consists of three stages: (*i*) face recognition, (*ii*) fingerprint verification, and (*iii*) decision fusion. Face recognition is responsible for retrieving the top n matches of a query from the template database where n is usually

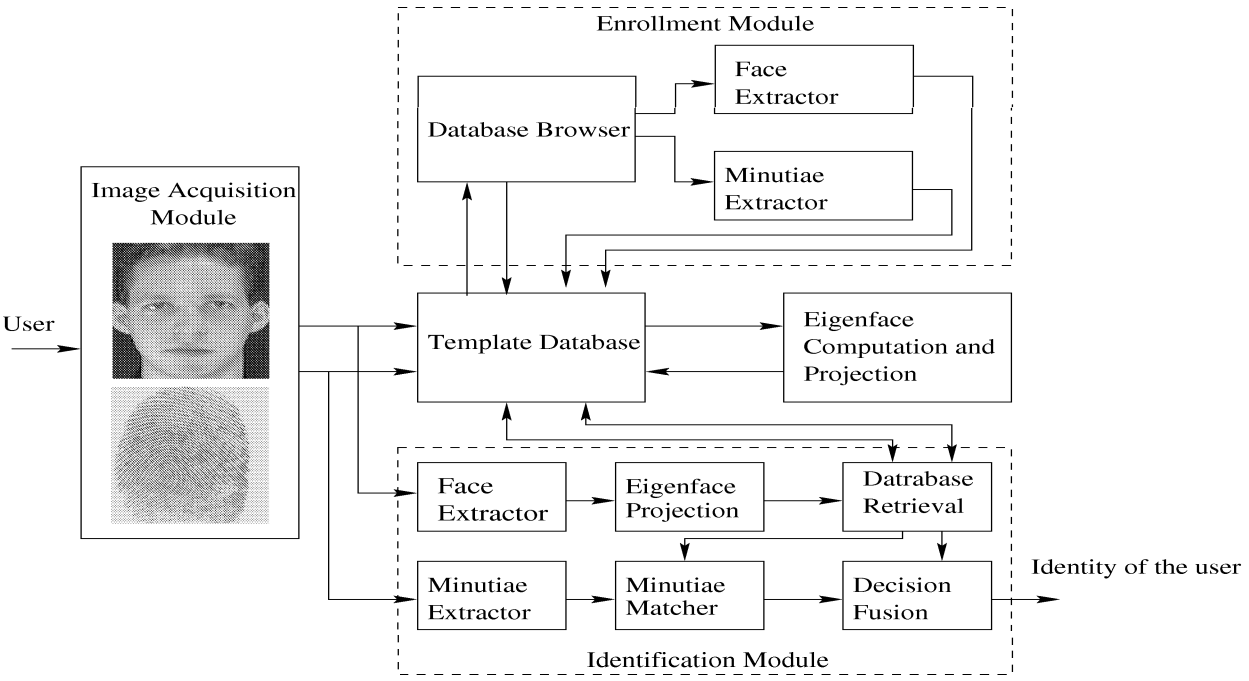
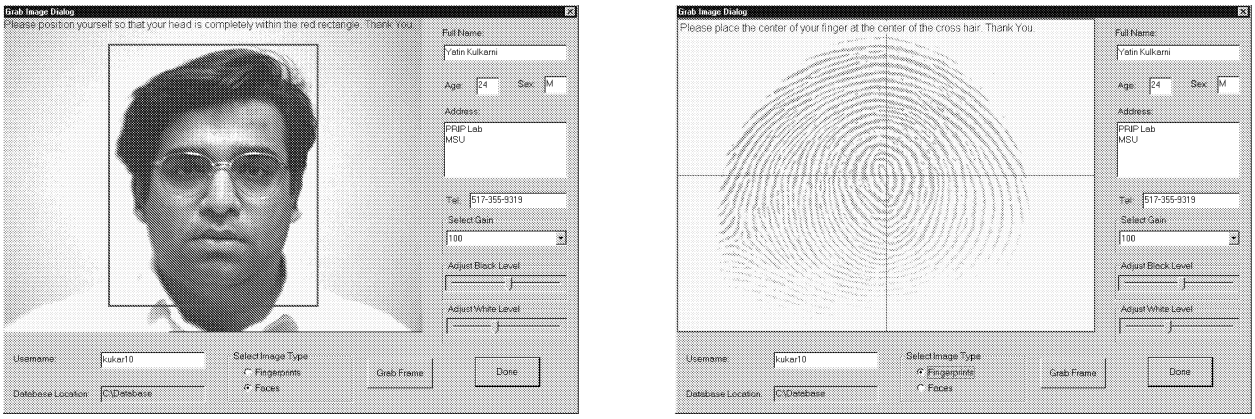


Figure 2: The block diagram of the F2ID system

a small number ($n = 5$ in our experiments). Fingerprint verification is responsible for matching the fingerprints of the top n retrieved individuals with the query and providing the corresponding fingerprint matching scores. The decision fusion integrates the matching scores from face recognition and matching scores from fingerprint verification to establish the final decision.

2.2 System Design Issues

Digital image acquisition is one of the most critical component for automatic personal identification. In order to acquire good quality images, the following mechanisms need to be provided: (i) feed-back and self-regulation guide, and (ii) quality control. For a cooperative user, feed-back provides an efficient mechanism to guarantee the quality of input images; if the user does not place the corresponding biometric characteristic properly, the feed-back mechanism will allow the user to adjust the placement accordingly. In our application domain, users are expected to be cooperative. We have designed a convenient graphical user



face acquisition fingerprint acquisition

Figure 3: The GUI for image acquisition; a user is expected to position his face inside the rectangle and to impress his finger at the center of the scanner.

interface (GUI) (figure 3) to acquire face and fingerprint images. Also, it is desirable that user's face and fingerprint be located (segmented) properly after the images are acquired. A simple and fast face location algorithm was implemented to guarantee that a user should be posed properly. For fingerprint image, we require that the number of extracted minutiae be larger than a threshold value, $T_{minutiae}$ (25).

A lot of user interaction is involved in the enrollment mode. It is critical that a friendly graphic user interface be provided. We have designed a GUI which greatly facilitate the operation of the system in the operational mode. A snap shot of the enrollment GUI is shown in figure 4.

In order for a user to be identified, the templates of the user needs to be enrolled into the database. Let $\mathcal{T} = \{U_1, U_2, ..., U_N\}$ denote the template database, where U_i represents a particular user and N is the total number of users enrolled in the template database. Essentially, $\mathcal{T}$ constitutes the training samples of the system. $\mathcal{T}$ should satisfy the following two integrity requirements: (i) *template database integrity* and (ii) *template integrity*. Template database integrity requires that $U_i \neq U_j$, if U_i and U_j represent the templates of two different users; if two users possess the same template, then they can not be differentiated from each other by the system. Therefore, when a user is enrolled in the system, an identification procedure should be performed to guarantee that the corresponding template(s) of the user is(are) not identical to the templates of any users in the template database. Template in-

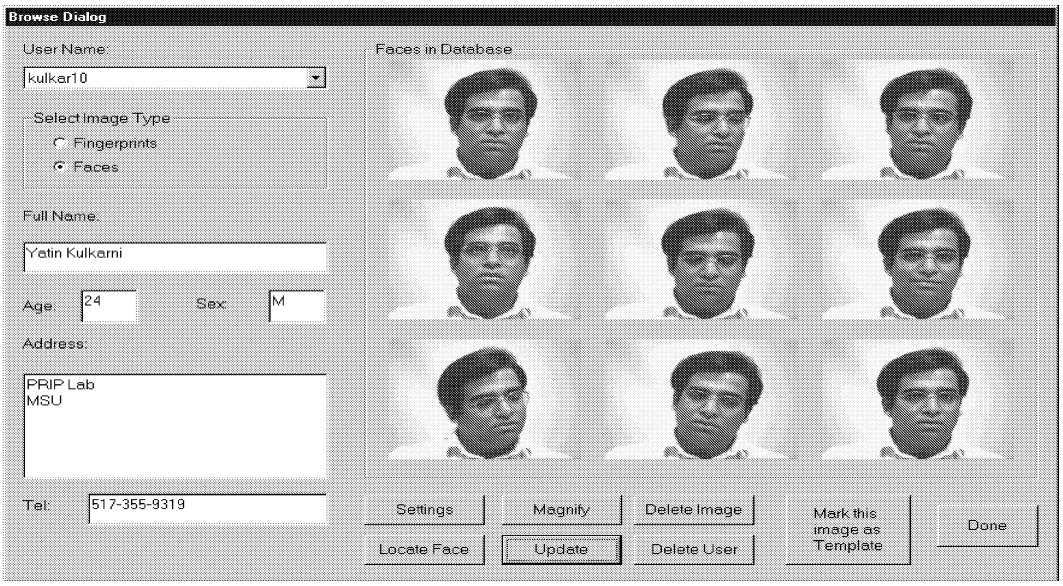


Figure 4: A snapshot of the graphic user interface for user enrollment

tegrity requires that the template(s) of a user should be of good quality and *representative*. The capability of an automatic personal identification system depends heavily on both the number and the representativeness of the templates. The more the number of templates and the more representative the templates, the more accurate is the system.

In the F2ID system, the eigenface-based face recognition approach is used, which needs an explicit *training procedure* to compute the eigenfaces that correspond to the M highest eigenvalues from the enrolled training face images and the prototypes of each training face images in the M-dimensional eigenspace. The training of fingerprint verification subsystem is performed implicitly. A minutiae template is extracted from an input fingerprint image and inserted into the database.

3 Experimental Results

For an operational automatic personal identification system, a number of properties need to be assessed, including performance, resource requirements, cost, physical size, user acceptability/friendliness, maintenance requirement, environmental factors, *etc.* Among them, the most important property is the performance. In automatic personal identification, *false*

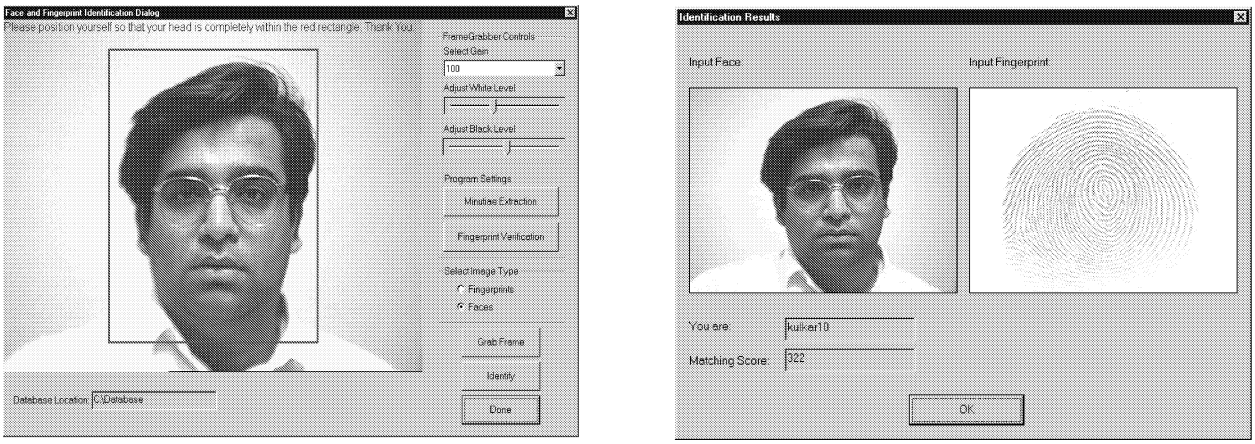
Figure 5: Face and fingerprint images (640×480).

acceptance rate (FAR) which indicates the probability of an impostor being accepted and *false reject rate* (FRR) which indicates the probability of a genuine person being rejected are used as indicators of the identification accuracy.

For an automatic personal identification system, performance evaluation may be performed at different levels. At the *algorithm level*, the performance benchmark characterizes the discriminating capability of the algorithm itself, which essentially depends on the capability of the biometric characteristic, its representation, and matching algorithm. The algorithm performance benchmark should be estimated on standard databases to provides an objective assessment of the technique itself. On the other hand, at the *system level*, the performance benchmark assesses the capability of the system at the point-of-identification, which is the perceived performance of the system. The perceived performance of a system depends heavily on how the system is used, whether users are willing to cooperate, *etc.* A test which simulates the operating environment is needed to assess the perceived performance benchmark of an implemented system.

3.1 Database

The performance evaluation of the integrated identification algorithm itself was reported in [4]. Here, we are interested in providing a perceived performance benchmark. A database of faces and fingerprints of 89 persons was collected. For each person, 9 face images (a total of 801 images) and 4 fingerprint images (a total of 356 images) were acquired. The face images were acquired using a Panasonic video camera under normal indoor lighting conditions. The rotation of the face was restricted to 30^o and the scaling factor was allowed between 0.90 to 1.10, approximately. The fingerprint images were acquired using an optical



face image acquisition identification result

Figure 6: An example of identification.

fingerprint scanner manufactured by Digital Biometrics with the restriction that fingers be placed approximately at the center of the scanner and the orientation of fingers be within 90^o. Examples of acquired face and fingerprint images are shown in Figures 5.

3.2 Performance

The leave-one-out method was used to assess the performance of the system. For each person, one fingerprint with acceptable quality was selected as the template. All but one face images were used to train the face recognition subsystem. The remaining face image was paired with the fingerprint to form a test sample. This process was repeated 801 times. An example of identification is shown in Figure 6. The identification accuracy of the integrated system as well as the identification accuracies of face recognition and fingerprint identification are compiled in Table 1, where the number of false rejects are listed along with the corresponding number of false acceptances. The response time of the integrated system for one typical identification is 3 seconds (Table 2). In comparison, identification using only fingerprints on a database of 89 persons takes 35 seconds. From these preliminary experimental results, we can see that the F2ID system can achieve a desirable identification accuracy with an acceptable response time. It meets the goal of a "real-time" *medium-size* automatic personal identification system.

$T_{fingerprint}$	$n = 5$		$n = 10$		$n = 15$		Fingerprint		Face	
	#FA	#FR	#FA	#FR	#FA	#FR	#FA	#FR	#FA	#FR
50	2	39	1	17	1	11	1	0	85	0
100	0	59	0	38	0	32	0	21	85	0

Table 1: False accept (FA) and false reject (FR) rates; the integrated results were obtained based on 801 tests; the fingerprint identification results were obtained based on 267 tests; the face recognition results were obtained based on 801 tests; the range of the fingerprint threshold, $T_{fingerprint}$, is $(1, 1000)$; the higher the value of $T_{fingerprint}$, the lower the FAR but the higher the FRR.

Face Location (seconds)	Face Retrieval (seconds)	Fingerprint verification (seconds)	Total (seconds)
0.5	0.5	2.0	3.0

Table 2: The wall time of the F2ID system on a Pentium 200MHz PC ($n = 5$).

4 Conclusions and Summary

We have introduced a "medium-size" automatic identification system which integrates faces and fingerprints to make a personal identification and addressed a number of design issues. The system overcomes some of the limitations of face recognition systems and fingerprint verification systems. Experimental results demonstrate that our system performs well. It meets the response time as well as the accuracy requirements. Note that the F2ID system may not scale up to a huge database with millions of records, because it has not yet been shown that face recognition is sufficiently accurate in retrieval from a huge database.

Automatic quality control is critical to the perceived performance of an automatic personal identification system. The earlier the quality control is performed, the better the perceived performance. For face recognition, quality control can be performed at the face detection and location stage. In our system, for simplicity, only a very simple face detection and normalization algorithm is used. We expect that a more efficient face detection and normalization algorithm will help improve the performance of the system. For fingerprint verification, it is desirable that the quality checking be applied at an early stage to guarantee that the acquired fingerprint images are of good quality. If the acquired images are of poor quality, the quality control algorithm should be able to apply a fingerprint enhancement algorithm to improve the quality of the images. In addition, by integrating additional

biometrics, a further performance improvement can be obtained. We are in the process of adding speaker verification to this integrated system.

References

[1] R. Chellappa, C. Wilson, and A. Sirohey. Human and machine recognition of faces: A survey. *Proceedings IEEE*, 83(5):705–740, 1995.

[2] R. Clarke. Human identification in information systems: Management challenges and public policy issues. *Information Technology & People*, 7(4):6–37, 1994.

[3] S. G. Davies. Touching big brother: How biometric technology will fuse flesh and machine. *Information Technology & People*, 7(4):60–69, 1994.

[4] L. Hong and A. Jain. Integrating faces and fingerprints for personal identification. In *Proc. 4th ACCV (to appear)*, Hongkong, 1998.

[5] A. Jain, L. Hong, S. Pankanti, and R. Bolle. An identity-authentication system using fingerprints. *Proceedings of IEEE*, 85(9):1365–1388, 1997.

[6] J. Campbell Jr., L. Alyea, and J. Dunn. Biometric security: Government applications and operations. *http:/www.vitro.bloomington.in.us:8080/∼BC/*, 1996.

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

[8] P. J. Phillips, P. J. Rauss, and S. Z. Der. *FERET (Face Recognition Technology) Recognition Algorithm Development and Test Results.* U.S. Government Publication, ALR-TR-995, Army Research Laboratory, Adelphi, MD, 1996.

[9] D. L. Swets and J. Weng. Using discriminant eigenfeatures for image retrieval. *IEEE Trans. PAMI*, 18(8):831–836, 1996.