Proceedings of Biometric Authentication Workshop, LNCS 3087, pp. 259-269,
Prague, May 2004

# Integrating Faces, Fingerprints, and Soft Biometric Traits for User Recognition

Anil K. Jain, Karthik Nandakumar, Xiaoguang Lu, and Unsang Park

Department of Computer Science and Engineering
{jain,nandakum,lvxiaogu,parkunsa}@cse.msu.edu
Michigan State University, MI - 48824, USA

**Abstract.** Soft biometric traits like gender, age, height, weight, ethnicity, and eye color cannot provide reliable user recognition because they are not distinctive and permanent. However, such ancillary information can complement the identity information provided by the primary biometric traits (face, fingerprint, hand-geometry, iris, etc.). This paper describes a hybrid biometric system that uses face and fingerprint as the primary characteristics and gender, ethnicity, and height as the soft characteristics. We have studied the effect of the soft biometric traits on the recognition performance of unimodal face and fingerprint recognition systems and a multimodal system that uses both the primary traits. Experiments conducted on a database of 263 users show that the recognition performance of the primary biometric system can be improved significantly by making use of soft biometric information. The results also indicate that such a performance improvement can be achieved only if the soft biometric traits are complementary to the primary biometric traits.

## 1 Introduction

Biometric systems recognize users based on their physiological and behavioral characteristics [1]. Unimodal biometric systems make use of a single biometric trait for user recognition. It is difficult to achieve very high recognition rates using unimodal systems due to problems like noisy sensor data and non-universality and/or lack of distinctiveness of the chosen biometric trait. Multimodal biometric systems address some of these problems by combining evidence obtained from multiple sources [2]. A multimodal biometric system that utilizes a number of different biometric identifiers like face, fingerprint, hand-geometry, and iris can be more robust to noise and alleviate the problem of non-universality and lack of distinctiveness. Hence, such a system can achieve a higher recognition accuracy than unimodal systems. However, a multimodal system will require a longer verification time thereby causing inconvenience to the users.

It is possible to improve the recognition performance of a biometric system without compromising on user-friendliness by utilizing ancillary information about the user like height, weight, age, gender, ethnicity, and eye color. We refer to these traits as soft biometric traits because they provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate any two individuals (see Figure 1 for examples of soft biometric traits). The soft biometric traits can either be continuous or discrete. Traits such as gender, eye color, and ethnicity are discrete

in nature. On the other hand, traits like height and weight are continuous variables. Heckathorn et al. [3] have shown that a combination of soft attributes like gender, race, eye color, height, and other visible marks like scars and tattoos can be used to identify an individual only with a limited accuracy. Hence, the ancillary information by itself is not sufficient to recognize a user. However, soft biometric traits can complement the traditional (primary) biometric identifiers like fingerprint and hand-geometry and hence improve the performance of the primary biometric system.


**Fig. 1.** Examples of soft biometric traits.

In order to utilize soft biometrics, there must be a mechanism to automatically extract these features from the user during the recognition phase. As the user interacts with the primary biometric system, the system should be able to automatically extract the soft biometric characteristics like height, weight, age, gender, and ethnicity in a non-obtrusive manner without any interaction with the user. In section 2 we present some of the methods that could be used for automatic extraction of the soft biometric information. Section 3 describes our framework for the integration of soft biometrics with the primary biometric system. The objective of this work is to analyze the impact of

introducing soft biometric variables like gender, ethnicity, and height into the decision making process of a recognition system that uses faces and fingerprints as the primary biometric traits. The experimental results presented in section 4 give an insight on the effects of different soft biometric variables on the recognition performance.

## 2 Automatic Extraction of Soft Biometric Characteristics

Soft biometric characteristics like gender, ethnicity, and age could be derived from the facial image of the user. Several studies have attempted to identify the gender, ethnicity, and pose of the users from their facial images. Gutta et al. [4] proposed a mixture of experts consisting of ensembles of radial basis functions for the classification of gender, ethnic origin, and pose of human faces. They also used a SVM classifier with RBF kernel for gating the inputs. Their gender classifier classified users as either male or female with an average accuracy rate of 96%, while their ethnicity classifier classified users into Caucasian, South Asian, East Asian, and African with an accuracy of 92%. These results were reported on good quality face images from the FERET database that had very little expression or pose changes. Based on the same database, Moghaddam and Yang [5] showed that the error rate for gender classification can be reduced to 3.4% by using an appearance-based gender classifier that uses non-linear support vector machines. Shakhnarovich et al. [6] developed a demographic classification scheme that extracts faces from unconstrained video sequences and classifies them based on gender and ethnicity. Their demographic classifier was a Perceptron constructed from binary rectangle features. The learning and feature selection modules used a variant of the AdaBoost algorithm. Their ethnicity classifier classified users as either Asian or non-Asian. Even under unconstrained environments, they showed that a classification accuracy of more than 75% can be achieved for both gender and ethnicity classification. For this data, the SVM classifier of Moghaddam and Yang had an error rate of 24.5% and there was also a notable bias towards males in the classification (females had an error rate of 28%). Balci and Atalay [7] reported a classification accuracy of more than 86% for a gender classifier that uses PCA for feature extraction and Multi-Layer Perceptron for classification. Jain and Lu [8] proposed a Linear Discriminant Analysis (LDA) based scheme to address the problem of ethnicity identification from facial images. The users were identified as either Asian or non-Asian by applying multiscale analysis to the input facial images. An ensemble framework based on the product rule was used for integrating the LDA analysis at different scales. This scheme had an accuracy of 96.3% on a database of 263 users (with approximately equal number of users from the two classes).

Automatic age determination is a more difficult problem due to the very limited physiological or behavioral changes in the human body as the person grows from one age group to another. There are currently no reliable biometric indicators for age determination [9]. Buchanan et al. [10] have been studying the differences in the chemical composition of child and adult fingerprints that could be used to distinguish children from adults. Kwon and Lobo [11] present an algorithm for age classification from facial images based on cranio-facial changes in feature-position ratios and skin wrinkle analysis. They attempted to classify users as “babies”, “young adults”, or “senior adults”. However, they do not provide any accuracy estimates for their classification scheme.

One can hope that age determination systems providing a reasonable estimate of the age of a person would be available in the near future.

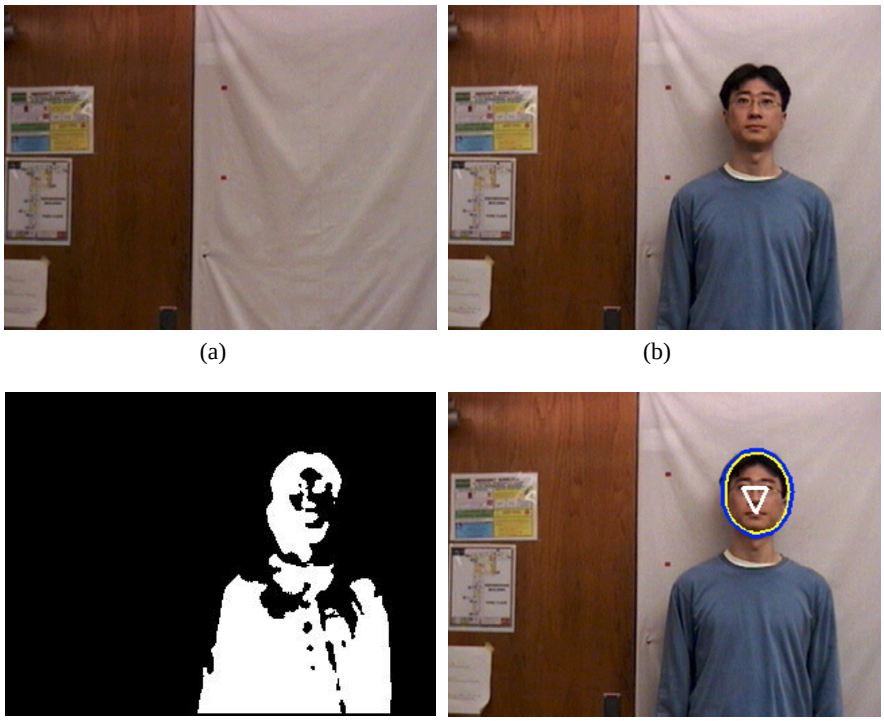
The weight of a user can be measured by installing a weight sensor at the place where the users stand while providing the primary biometric. The height can be estimated from a sequence of real-time images obtained when the user moves into the view of the camera. Figure 2 describes a mechanism for simultaneous extraction of the height information and the facial image of a user. In this setup we assume that the position of the camera and the background scene are fixed. The background image (Figure 2(a)) is initially stored in the system. Two markers are placed in the background for calibration. The first marker is placed at a height $H_{low}$ above the ground and the second marker is placed at a distance $H_{ref}$ above the first marker. The vertical distance between the two markers in the background image is measured as $D_{ref}$. In our experiments, $H_{low} = 150\ cm$, $H_{ref} = 30\ cm$,and $D_{ref} = 67\ pixels$. The background image is subtracted from the current frame (Figure 2(b)) to obtain the difference image (Figure 2(c)). A threshold is applied to the difference image to detect only those pixels having large intensity changes. Median filtering is applied to remove the salt and pepper noise in the difference image. The background subtraction is usually performed in color domain [12]. However, for the sake of simplicity in deciding the threshold value and in the median filtering operation, we performed the subtraction in the gray-scale domain. The difference image is scanned from the top to detect the top of the head and the vertical distance between the top of the head and the lowermost marker is measured as $D_{user}$ (in pixels). An estimate of the true height of the person ($H_{user}$ in cm) is computed as:

$$H_{user} = H_{low} + \frac{D_{user}}{D_{ref}} H_{ref}. \tag{1}$$

After the estimation of the height, the face of the user is detected in the captured frame using the algorithm proposed by Hsu et al. [13]. After the detection of the facial region in the frame (Figure 2(d)), the face is cropped out of the frame and is used by the face recognition and gender/ethnicity extraction modules. Since, we have not collected sufficient data using this extraction process, we used an off-line face database in our experiments.

## 3 Framework for Integration of Soft Biometrics

We use the same framework proposed in [14] for integrating the soft biometric information with the primary biometric system. In this framework, the biometric recognition system is divided into two subsystems. One subsystem is called the primary biometric system and it is based on traditional biometric identifiers like fingerprint, face and hand-geometry. The primary biometric system could be either unimodal or multimodal. The second subsystem, referred to as the secondary biometric system, is based on soft biometric traits like age, gender, and height. Figure 3 shows the architecture of a personal identification system that makes use of fingerprint, face and soft biometric measurements. Let $\omega_1, \omega_2, \cdots, \omega_n$ represent the $n$ users enrolled in the database. Let



(a) (b)

(c) (d)

**Fig. 2.** Extraction of height and facial image from the user (a) background image (b) Current frame (c) Difference Image (d) Location of the face in the current frame.

**x** be the feature vector corresponding to the primary biometric. Without loss of generality, let us assume that the output of the primary biometric system is of the form $P(\omega_i \mid \mathbf{x}),\ i = 1, 2, \cdots, n$, where $P(\omega_i \mid \mathbf{x})$ is the probability that the test user is $\omega_i$ given the feature vector **x**. If the output of the primary biometric system is a matching score, it is converted into posteriori probability using an appropriate transformation. For the secondary biometric system, we can consider $P(\omega_i \mid \mathbf{x})$ as the prior probability of the test user being user $\omega_i$.

Let $\mathbf{y} = [y_1,\ y_2,\ \cdots,\ y_k,\ y_{k+1},\ y_{k+2},\ \cdots,\ y_m]$ be the soft biometric feature vector, where $y_1$ through $y_k$ are continuous variables and $y_{k+1}$ through $y_m$ are discrete variables. The updated probability of user $\omega_i$, given the primary biometric feature vector **x** and the soft biometric feature vector **y** i.e., $P(\omega_i \mid \mathbf{x},\ \mathbf{y})$ can be calculated using the Bayes' rule.

$$P(\omega_i|\mathbf{x},\ \mathbf{y}) = \frac{p(\mathbf{y}|\omega_i)\ P(\omega_i|\mathbf{x})}{\sum_{i=1}^{n} p(\mathbf{y}|\omega_i)\ P(\omega_i|\mathbf{x})}\ . \tag{2}$$

DOCKET ALARM

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

**LAW FIRMS**
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

**FINANCIAL INSTITUTIONS**
Litigation and bankruptcy checks for companies and debtors.

**E-DISCOVERY AND LEGAL VENDORS**
Sync your system to PACER to automate legal marketing.