Biometric Authentication for a Mobile Personal Device

Qian Tao and Raymond N. J. Veldhuis
Signals and Systems Group
University of Twente
Enschede, the Netherlands
{q.tao, r.n.j.veldhuis}@el.utwente.nl

Abstract—Secure access is prerequisite for a Mobile Personal Device (MPD) in a Personal Network (PN). An authentication method using biometrics, specifically face, is proposed in this paper. A fast face detection and registration method based on a Viola-Jones detector is implemented, and a face-authentication method based on subspace metrics is developed. Experiments show that the authentication method is effective with an Equal Error Rate (EER) of 1.2%, despite its simplicity.

Index terms—biometrics; authentication; MPD; PN; subspace.

I. INTRODUCTION

In the context of the Personal Network (PN), the security of user information in the network becomes especially important. Therefore, the Mobile Personal Device (MPD), which links the user and the network in mobile situations, puts forward high demands on the user authentication.

The traditional way to protect the information is by tokens or PINs (Personal Identification Number), which are easy to implement, but constantly under the risk of being stolen, or forgotten. Biometrics, the unique biological or behavioral characteristics of a person, is one of the most popular and promising alternatives to solve this problem [1]. It is convenient for the user because it cannot be lost or forgotten, and it is virtually the only form of authentication that ensures the physical presence of the user. Based on biometrics, our work aims at building a secure, convenient, and efficient interface between the MPD and the user in the PN.

This paper is organized as follows. Section II addresses the challenges of biometric authentication in the MPD, Section III proposes our solution, and Section IV presents the preliminary results of the proposed system.

II. BIOMETRIC AUTHENTICATION IN THE MPD

A. Security Aspects

There are two types of authentication in the MPD scenarios: authentication at logon time and at run time. The second type of authentication is important because it can prevent unauthorized users from taking an MPD in operation and accessing confidential user information from the PN.

The false-accept rate (FAR) and the false-reject rate (FRR) are used to quantify the biometric authentication performance. The FAR specifies the probability that an imposter can use the device, and is, therefore, closely related to security. The traditional PIN code can achieve the FAR as low as \(10^{-n}\), where \(n\) is the length of the PIN digits. With the incorporation of biometric authentication, the security at run time will be realized. To guarantee the security both at logon time and run time, the FAR of the biometric authentication system should be sufficiently low.

B. Convenience Aspects

The FRR, on the other hand, is closely related to user convenience. A false reject will force the user to re-enter biometric data, which will cause annoyance. This obviously leads to the requirement of low FRR of the biometric authentication system.

In terms of convenience, a much higher degree of user-friendliness can be achieved if the biometric authentication is transparent, which means that the authentication can be done without explicit user actions. Transparency should be considered as a requirement for the authentication at run time, because regularly requiring a user, who may be concentrating on a task, to present the biometric data is neither practical nor convenient.

C. Complexity Aspects

Ongoing authentication will constantly consume the computational resources of the MPD. Because the MPD operates in the PN, it offers the possibility that biometric templates are stored in a central database and that the authentication is done in the network. Although the constraints on the algorithmic complexity become less stringent, this option brings a higher security risk. Firstly, when biometric data has to be transmitted over the network it is vulnerable to eavesdropping [2]. Secondly, the biometric templates need to be stored in a database and are vulnerable to attacks [3]. These are problems difficult to solve. Conceptually, it is also preferable to make the MPD authentication more independent of other parts of the PN.

Therefore, the authentication needs to be implemented in the MPD, and this requires that the complexity of the algorithm be kept low, such that it can be executed on the MPD state-of-the-art hardware, and while executed, does not disturb other MPD functions.
III. FACE RECOGNITION AS THE SOLUTION

The biometric we choose for the MPD application should satisfy all three requirements listed above simultaneously. Face recognition is among all biometrics a good choice. It is the only biometrics that can be really transparent. By mounting a camera on the MPD, the face images of the user can be caught almost constantly. This is attractive because the cost for a camera is low, and modern MPDs such as mobile phone and Personal Digital Assistant (PDA) normally have a camera installed.

A. Face Preprocessing

Face preprocessing includes three steps, namely face detection, face registration, and face normalization.

For fast face detection Viola and Jones proposed a detection scheme which is very efficient by using simple rectangular binary features and the integral image [4], and has proved to be robust against varying background and foreground. The training of the Viola-Jones detectors is slow, but the detector only needs to be trained once offline, and then they can be hardcoded in the device.

The importance of accurate face registration (alignment to a reference) has been proved in [5][6]. For the MPD application, a Viola Jones detector is trained for 13 different facial features (landmarks), as illustrated in the second row of Fig. 1. These landmarks are combined into a shape, and then rigidly registered to the reference shape. Furthermore, the face region is masked to exclude the background influences. As illustrated in the third row of Fig. 1 that only the upper part of the face is considered, which is relatively constant under varying expressions. Besides face registration, illumination normalization is also an important issue in face recognition [7].

A simple high pass filter can act to equalize the luminance level across the image, as illustrated in Fig. 1.

![Fig. 1. Face feature extraction procedure (from top down): face detection, facial feature detection, face registration and masking, high-pass filtering.](image)

B. Face Authentication in a Personal Face Space

Subspace methods belong to one of the most popular methods in face recognition [8]. They are well defined and simple, but need a large dataset in order to accurately estimate the subspace. In the MPD application, the user is exposed extensively to the device, thus a large sample set can be obtained, which allows us to adopt a simple subspace method.

The enrollment of the face authentication system includes the training of the subspace and the classifier. Suppose we have the matrix X containing N feature vectors [x₁,..., xₙ] as its columns, then the matrix X₀ whose columns have zero mean can be calculated by subtracting the column mean x̄ from every column of X. Then the eigenfaces are computed by means of singular value decomposition (SVD).

\[
X₀ = USV^T
\] (1)

where the columns of U are the eigenfaces spanning the column space of X₀, and the columns of V spanning the row space of X₀. S is a diagonal matrix with the diagonal entries being the singular values. Let the first k columns of U be Uₛ with k such that most of the variance (e.g. 90%) is explained.

The projection of xᵢ on the face space is

\[
yᵢ = Uₛᵀ(xᵢ - x̄)
\] (2)

We derive a further reduced feature vector with only two dimensions: DIFS (distance in feature space) and DFFS (distance from feature space) [9], which are illustrated in Fig. 2. The DFFS measure is the residual error of the projection onto the face space, normalized with respect to the norm of the mean face vector:

\[
DFFS(xᵢ) = \frac{||(I - UₛUₛᵀ)(xᵢ - x̄)||}{||xᵢ||}
\] (3)

where I is the identity matrix. The DIFS measure is the Mahalanobis distance calculated by:

\[
DIFS(xᵢ) = \sqrt{yᵢᵀ(Sₖ⁻¹)yᵢ}
\] (4)

where yᵢ is computed from (2), and Sₖ is the upper left k×k submatrix of S in (1).

IV. EVALUATION OF THE BIOMETRIC AUTHENTICATION

A. Experiment Setup

The face images with a size of 320×240 pixels are collected by a Philips HQ-TRIP0DID webcam. In the experiment we
collected 4,000 frames for each of the 6 individuals. By flipping every image horizontally, 8,000 images are obtained per person. For face detectors, we use the pre-trained Viola-Jones detector provided by the Intel OpenCV library [10]. For training the facial landmark detectors, the BioID database is used [11]. The details of this process was reported in [12].

After face and landmark detection, the face image is registered to the size of 32 by 32, and the further reduced to $17 \times 21 = 357$ by masking. Illumination normalization is done by first filtering every image by a Gaussian low-pass filter, the scale of which normalized to 1/10 of the inter-ocular distance. Then this image is subtracted from the original image, retaining only the high-frequency details of the face.

For each individual, the face data was then split in such a way that 60% of the data are used for training the personal face space, 20% as the validation set for building the classifier, and 20% as the testing set for evaluating the performance of the subspace and the classifier. The subspace has a dimensionality of 200. For each individual, we randomly take 1,000 faces from each of the other 5 individual to train the classifier, and another 1,000 to evaluate the classifier.

From (3) and (4) we calculate the feature vector of DFFS and DIFS, both for the authentic user and the imposters. As an example, Fig. 3 illustrates the scatter plot of one authentic user and the imposters. The circles indicate the scattering of the training data and validation data, and the dots indicate the scattering of the testing data. A Parzen classifier based on posterior probability estimation of the distribution is trained [13], which is also illustrated in Fig. 3.

### B. FAR and FRR

By assuming different priors of the authentic user and the imposter, and adjusting the decision boundary of the Parzen classifier accordingly, the Receiver Operating Curve (ROC) can be acquired, which describes the relationship between the FRR and the FAR. Fig. 4 shows the ROC of both the training set and test set. The optimal operation point, therefore, can be selected from this curve based on the specific requirement of the application. As a general measure of classification performance, the Equal Error Rate (EER) is also calculated. As shown in Fig. 4, the EER of this face authentication for the testing set is about 1.2%, and almost zero for the validation set.

---

Fig. 3. The scatter plot of DFFS and DIFS for authentic user data and imposter data. Parzen classifier boundary is also shown.

Fig. 4. ROC of both validation data and testing data

---

V. CONCLUSIONS

The security of the MPD in the PN is very important. Our work aims at building up a secure, convenient, and efficient connection between the MPD and the user in the PN, based on biometrics authentication. Simple and effective algorithms are developed for face recognition in a MPD. Experiments show that our face authentication method can achieve an EER as low as 1.2% under current experiment setup. In the future work, extensive experiments on more users under large lighting variations will be done. With further efforts on optimizing the algorithm and building up the system in real MPD hardware, the perspective of the biometric authentication in a PN is promising.

---

**REFERENCES**


