An Automatic Feature Based Face Authentication System

Stefano Arca, Paola Campadelli*, Elena Casiraghi, Raffaella Lanzarotti

Dipartimento di Scienze dell'Informazione
Università degli Studi di Milano
Via Comelico, 39/41 20135 Milano, Italy
{arca, campadelli, casiraghi, lanzarotti}@dsi.unimi.it

Abstract. In this paper a fully automatic face verification system is presented. A face is characterized by a vector (*jet*) of coefficients determined applying a bank of Gabor filters in correspondence to 19 facial fiducial points automatically localized. The identity claimed by a subject is accepted or rejected depending on a similarity measure computed among the jet characterizing the subject, and the ones corresponding to the subjects in the gallery. The performance of the system has been quantified according to the Lausanne evaluation protocol for authentication.

1 Introduction

Human face recognition has been largely investigated for the last two decades [13]. Within this context, we can define two specific tasks: authentication and identification [9]: the former aims to verify the identity declared by a subject on the basis of some biometric characteristics, the latter aims to recognize a person who does not declare his/her identity, but who is assumed to be one of the persons which constitute a referring gallery. Faces can be biometrically characterized in the same way for these two tasks; what differs is the comparison criterion: in the case of authentication, it is necessary to define an absolute threshold, while in the case of identification the identity of the test face is determined as the one of the gallery image which has the best match with the test itself.

In [2] we presented an identification system, which automatically localizes 19 fiducial points[1] and characterizes the face applying a bank of Gabor filters in correspondence to each fiducial point. In that case given a test image, the system computes its face characterization, and looks for in a gallery the subject who maximizes a suitably defined similarity function.

In this paper we present an authentication system in which the biometric characterization is similar to the one proposed in [2], while the identification is completely new. This authentication task corresponds to an "open-universe

* Work partially supported by project "Acquisizione e compressione di Range Data e tecniche di modellazione 3D di volti da immagini", COFIN 2003

[1] the eyebrow and chin vertices, the nose tip, the eye and lip corners and upper and lower middle points, the nose lateral extremes and the mean point between the eyes

scenario" where persons unknown to the system may claim access. The subjects whose features are stored in the gallery are referred to as *Clients* while persons claiming false identity are called *Impostors*.

The whole system has been experimented on 744 images (of 186 subjects without glasses) taken from the XM2VTS [12]. We divided the database into two sets: the clients and the impostors. Moreover the set of the clients is divided in three subsets: the first constitutes the gallery (one image per subject), the second is used as client-evaluation set, and the third as the client-test set. The impostors set is divided in the impostor-evaluation and test sets respectively. Both the evaluation sets are used to establish the verification threshold.

The performance measures (Section 4) and the results (Section 5) are shown according to the Lausanne evaluation protocol presented in [8].

2 Localization of the facial features and of the corresponding fiducial points

The first steps consist in detecting the face in the image and localizing the corresponding facial features (eyes, nose, mouth, and chin). In [1, 5] we proposed a scale-independent method which assumes the mouth is closed and the eyes are open and without glasses.

Given the feature sub-images, we proceed processing each of them separately, with the aim of extracting the most characteristic fiducial points. In [1] we presented a method to determine robustly and efficiently the fiducial points associated to the eyebrows, the nose and the chin; regarding the eyes and the mouth we adopted the deformable template technique which estimates the whole features contour, but which is computationally very expensive. In [2] we proposed an efficient alternative for the eyes, based on the analysis of the edges obtained by means of the first derivative of Gaussian filters, while for the mouth we considered the mouth corners used for the template initialization and we derived the upper and lower middle points as a function of them. Moreover, we proposed a module able to recognize automatically which fiducial points have been wrongly determined, and which recovers them on the basis of the positions and dimensions of the reliable features.

These modules, applied to the 744 images of the XM2VTS database, determine a good estimation of the fiducial points in the 97.5%. An example of the obtained results is shown in figure 1.

3 Face characterization

Once the fiducial points have been extracted, we proceed characterizing each of them in terms of the surrounding gray level portion of image. Following the idea of Wiskott [11], a Jet of 40 coefficients is assigned to each fiducial point, convolving the portion of gray image around the point with the following bank of 40 *Gabor kernels* (we consider 5 frequencies and 8 orientations):

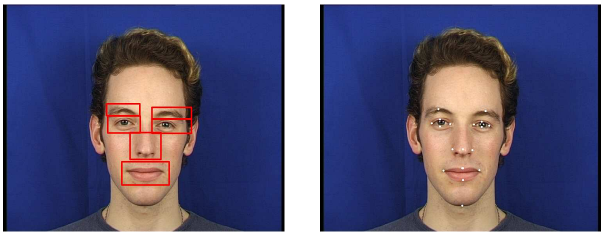


Fig. 1. features sub-images and fiducial points

$$\psi_j(\boldsymbol{x}) = \frac{k_j^2}{\sigma^2} exp\left(-\frac{k_j^2 x^2}{2\sigma^2}\right)\left[exp(i\boldsymbol{k}_j\boldsymbol{x}) - exp\left(-\frac{\sigma^2}{2}\right)\right]$$

Thus, given a test image T to be authenticated, we are interested in determining a similarity score between it and the image in the gallery corresponding to the claimed identity. To determine this score we propose a method which requires to take into account all the images as follows:

- for each fiducial point i, and for each image $k \in G$, compute the similarity between corresponding Jets:

  $$S^{k,i} = S(J^{T,i}, J^{k,i}) = \frac{\sum_z J_z^{T,i} J_z^{k,i}}{\sqrt{\sum_z (J_z^{T,i})^2 \sum_z (J_z^{k,i})^2}}$$

  where $z = 0, ..., 39$.
- for each i, order the values $\{S^{k,i}\}$, and assign to each a weight $w^{k,i}$ as a function of its ordered position p.
  The weight $w^{k,i} = f(p)$ is determined as:

  $$f(p) = c \cdot [\ln(x+y) - \ln(x+p)],$$

  where $y = \frac{|G|}{4}$, $x = e^{-\frac{1}{2}}$, and c is a normalization factor.
- for the gallery image A corresponding to the claimed identity, consider the set, *Best10*, of the 10 fiducial points which have got the highest weights, and determine the score:

  $$\text{Score}(A) = \sum_{i \in Best10} w^{A,i} S^{A,i}.$$

  If the score is greater than a threshold th the subject is authenticated otherwise he/she is rejected.

It is clear that the algorithm performance strongly depends on the value given to the threshold th. A too high value of th would indeed make difficult the access to the impostors but at the same time would reject a lot of clients; on the other hand a too low value of th would increase the detection rate of the clients, together with the number of the impostors accepted.

In order to set the value of th which makes the global error low, we studied the behavior of the authentication system on the evaluation sets varying the value of th as presented in the following section.

4 Performance measure

To evaluate the performance of the verification system, two measures are used: the *false acceptance* (FA) and *false rejection* (FR) rates. False acceptance is the case when an impostor, claiming the identity of a client, is accepted. In contrast, false rejection is the case when a client, claiming his true identity, is rejected. The FA and FR rates are given by:

$$FA = \frac{EI}{I} \qquad FR = \frac{EC}{C} \tag{1}$$

where EI is the number of impostor accepted, I is the number of impostors trials, EC is the number of client rejected and C is the number of clients trials.

In order to set a reliable threshold, we carried out several experiments, testing the system with thresholds normalized in the range $[1-100]$. This step results in the ROC plotted in figure 2.

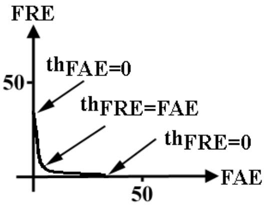


Fig. 2. ROC Curve

Starting from this curve, we focus the attention on four thresholds, which are chosen since on the evaluation data they allow to obtain desired values of the false acceptance (FAE) and false rejection (FRE) values:

$$\begin{aligned}
&th_{FAE=0} = argmin_{th}\,(FRE|FAE=0)\\
&th_{FAE=FRE} = (T|FAE=FRE)\\
&th_{FRE=0} = argmin_{th}\,(FAE|FRE=0)\\
&th_{sum} = argmin_{th}\,(FRE+FAE)
\end{aligned} \tag{2}$$

This will lead to obtain 8 scores on the test set:

$$\begin{array}{ll} FA_{FAE=0} & FR_{FAE=0} \\ FA_{FAE=FRE} & FR_{FAE=FRE} \\ FA_{FRE=0} & FR_{FRE=0} \\ FA_{sum} & FR_{sum} \end{array}$$

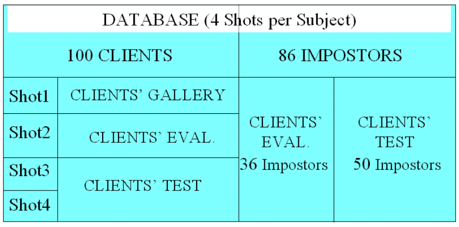
For each threshold, the *weighted error rate* (TER) can be obtained as follows:

$$\begin{aligned} WE_{FAE=0} &= \omega_{FA} \cdot FA_{FAE=0} + \omega_{FR} \cdot FR_{FAE=0} \\ WE_{FAE=FRE} &= \omega_{FA} \cdot FA_{FAE=FRE} + \omega_{FR} \cdot FR_{FAE=FRE} \\ WE_{FRE=0} &= \omega_{FA} \cdot FA_{FRE=0} + \omega_{FR} \cdot FR_{FRE=0} \\ WE_{sum} &= \omega_{FA} \cdot FA_{sum} + \omega_{FR} \cdot FR_{sum} \end{aligned} \tag{3}$$

The weights ω_{FA} and ω_{FR} are set depending on the relative importance of the false acceptance and rejection rates. If a general face verification system is used, we can weight the error rates equally, $\omega_{FA} = 0.5$ and $\omega_{FR} = 0.5$.

5 Experimental results

We report here the experiments carried out on the subset of the XM2VTS database consisting of all the 744 images of 186 subjects without glasses (4 shots per subject). The experimental setup is shown in figure 3: the images in the database are divided to form two sets (*clients* and *impostors*).



<table>
<tr><td colspan="4">DATABASE (4 Shots per Subject)</td></tr>
<tr><td colspan="2">100 CLIENTS</td><td colspan="2">86 IMPOSTORS</td></tr>
<tr><td>Shot1</td><td>CLIENTS' GALLERY</td><td rowspan="4">CLIENTS' EVAL.
36 Impostors</td><td rowspan="4">CLIENTS' TEST
50 Impostors</td></tr>
<tr><td>Shot2</td><td>CLIENTS' EVAL.</td></tr>
<tr><td>Shot3</td><td rowspan="2">CLIENTS' TEST</td></tr>
<tr><td>Shot4</td></tr>
</table>

Fig. 3. Experimental setup;

Specifically, we randomly selected as clients 100 subjects; the remaining 86 subjects form the set of the *impostors*.
The clients' gallery (100 images) is composed by selecting for each client the first shot. The clients' evaluation set is composed by the second shot of each client; the remaining 2 images for each client, form the clients' test set. The impostors' test set is composed of all the shots of 50 randomly selected impostors; while

the impostors' evaluation set is composed of the remaining images of the other 36 impostors.

With this setting we obtained the results shown in table 1. For each threshold, obtained in section 4, we show the FA, FR, and the weighted error rate, WE, with respect to the evaluation and the test sets.

Experimental Results						
Thresholds	**Evaluation**			**Test**		
	% FAE	**% FRE**	**% WE**	**% FA**	**% FR**	**% WE**
$th_{FAE=0}$	0	30	15	0	35.41	17.71
$th_{FAE=FRE}$	2.17	2	2.08	2.14	3.64	2.89
$th_{FRE=0}$	40.93	0	20.46	41.46	0	20.73
th_{sum}	1.78	2	1.89	1.82	3.64	2.73

Table 1. Authentication results.

The best results have been obtained using the threshold t_{sum} which minimizes the weighted error WE; note that in general there is a close agreement between the results obtained on the evaluation and test sets which shows that the selected thresholds generalize well.

6 Discussion

We presented a completely automatic system for face authentication. The method is based on a module for the feature extraction and description, which is self-correcting, and determines with high reliability the correct fiducial points. Moreover it is robust to illumination and scale variations. The authentication step computes for each probe image a score on the basis of both its characteristic jets vector, and the ones in the gallery.

A direct comparison of our system with others cannot be done: our feature detection works on images of people without glasses, thus we had slightly modified the experimental set, disregarding the images of people wearing glasses. However, the performance we achieve are comparable with the ones obtained in the competition reported in [7]. Moreover our system does not require any training session and any registration, which are two fundamental steps of methods based on LDA [6], SVM [4, 10], Multi Layer Perceptrons and Gaussian Mixture Model [3].

Further works aim to detect additional fiducial points in order to extract further information characterizing the faces; finally we intend to experiment and compare alternative methods to compute the scores.

References

1. S. Arca, P. Campadelli, and R. Lanzarotti. A face recognition system based on local feature analysis. *Proc. Int'l Conf. Audio- and Video-based Biometric Person Authentication, AVBPA2003 Guildford,UK published in the Lecture Notes in Computer Science*, 2688:182–189, 2003.
2. S. Arca, P. Campadelli, and R. Lanzarotti. An efficient method to detect facial fiducial points for face recognition. *Proc. the 17th Int'l Conf. Pattern Recognition, ICPR 2004 Cambridge,UK*, 2004.
3. F. Cardinaux, C. Sanderson, and S. Marcel. Comparison of an mlp and gmm classifiers for face verification on XM2VTS. *Proc. Int'l. Conf. Audio- and Video-based Biometric Person Authentication*, pages 911–920, 2003.
4. K. Jonsson, J. Kittler, Y.P. Li, and J. Matas. Support vector machines for face authentication. *Image and Vision Computing*, 20:369–375, 2002.
5. R. Lanzarotti. *Facial feature detection and description.* PhD thesis, Università degli Studi di Milano, 2003. Address: http://lanzarotti.dsi.unimi.it/.
6. H. Liu, C. Su, Y. Chiang, and Y. Hung. Personalized face verification system using owner-specific cluster-dependent lda-subspace. *Proc. Int'l Conf. Pattern Recognition*, 2004.
7. K. Messer, J. Kittler, M. Sadeghi, and al. Face verification competition on the XM2VTS database. *Proc. Int'l. Conf. Audio- and Video-based Biometric Person Authentication*, pages 964–974, 2003.
8. K. Messer, J. Matas, J. Kittler, J. Luettin, and G Maitre. XM2VTSDB: The extended M2VTS database. *Proc. Int'l. Conf. Audio- and Video-based Biometric Person Authentication*, 1999.
9. J. Phillips, P. Grother, R. Micheals, D.M. Blackburn, E. Tabassi, and J.M. Bone. Face recognition vendor test 2002: overview and summary. 2003. [Online], Available: http://www.frvt.org.
10. F. Smeraldi and J. Bigun. Retinal vision applied to facial features detection and face authentication. *Pattern recognition letters*, 23:463–475, 2002.
11. L. Wiskott, J. Fellous, N. Kruger, and C. von der Malsburg. Face recognition by elastic bunch graph matching. In L.C. Jain et al., editor, *Intelligent biometric techniques in fingerprints and face recognition*, pages 355–396. CRC Press, 1999.
12. XM2VTS DB. web. Address: http://www.ee.surrey.ac.uk/Research/VSSP/xm2vtsdb/.
13. W. Zhao, R. Chellappa, P.J. Phillips, and A. Rosenfeld. Face recognition: A literature survey. *ACM, Computing Surveys*, 35(4):399–458, 2003.