Asian Journal of Information Technology, 5 (3) : 285-289, 2006

Random Pulling Model (RPM) for Face Authentication

[1]D. Saigaa, [2]K. Benmahamed, [3]S. Lelandais and [4]N. Benoudjit
[1]Automatics Department, University Mohamed khider B.P 145 RP Biskra (07000), Algeria
[2]Electronics Department, University of Setif (19000), Algeria
[3]Complex Systems Laboratory (LSC), University of Evry Val Essonne, French
[4]Electronics Department, University of Batna (05000), Algeria

Abstract: In this study, a new model named: Random Pulling Model (RPM) is presented as an alternative feature extraction algorithm for use in automatic face recognition/authentication tasks. We show that the promising RPM algorithm extracts from faces features that are relevant and efficient for authentication. The feasibility of the RPM method has been successfully tested on face authentication using 2360 XM2VTS frontal face images corresponding to 295 subjects, which were acquired under variable illumination and facial expressions.

Key words: Random Pulling Model (RPM), face authentication, PCA (Principal Component Analysis), face image

INTRODUCTION

Face authentication has gained considerable attention these last years, through the increasing need for access verification systems using several modalities (voice, face image, fingerprints, pin codes, etc.). Such systems are used for the verification of a user's identity on the Net, when using a bank automaton, when entering a secured building, etc[1-3]. Face authentication is different from face recognition (or classification)[4-5]

- face authentication system should decide itself if a test face is assigned to a client (i.e., one who claims his/her own identity) or to an impostor (i.e., one who pretends to be some one else)
- face recognition system usually assists a human expert to determine the identity of a test face by computing all similarity scores between the test-face and each human face stored in the system database and by ranking them. Although RPM (Random Pulling Model) could be beneficial both for face authentication and recognition, we will concentrate on the first in this study.

In face authentication, as in most image processing problems, features are extracted from the images before processing. Working with rough images is not efficient: in face authentication, several images of a single person may be dramatically different, because of changes in viewpoint, in colour and illumination, or simply because the person's face looks different from day to day. Therefore extracting relevant features, or discriminant ones, is a must. Nevertheless, one hardly knows in advance which possible features will be discriminant or not. For this reason, one of the methods often used to extract features in face authentication is PCA (Principal Component Analysis)[6-7]. In this study, we show how the promising RPM (Random Pulling Model) technique extracts features that are more closely related to our intuition of discriminant information and that improve the success rate compared to an equivalent system using PCA.

FACE AUTHENTICATION

Face authentication systems typically compare a feature vector X extracted from the face image to verify with a client template, consisting in similar feature vectors Y_i extracted from images of the claimed person stored in a database ($1 \le i \le p$, where p is the number of images of this person in the learning set). The matching may be made in different ways, one being to take the Euclidean distance between vectors (this method will be taken as an example here). If the distance between X and Y_i is lower than a threshold, the face from which X is extracted will be deemed to correspond with the face from which Y_i is extracted. Choosing the best threshold is an important part of the problem: a too small threshold will lead to a high False Rejection Rate (FRR), while a too high one will lead to a high False Acceptance Rate (FAR); FRR and FAR are defined as the proportion of feature vectors extracted from images in a evaluation set being wrongly classified, respectively wrongly authentified and wrongly rejected[1,4,5,8]. The evaluation and test sets must be independent (though with faces of the same people) from

Corresponding Author: D. Saigaa, Automatics Department, University Mohamed khider B.P 145 RP Biskra (07000), Algeria

the learning set, in order to get objective results. One way of setting the threshold is to choose the one leading to equal FRR and FAR. If the a priori probabilities of having false acceptances (impostors) and false rejections are equal, this corresponds to the minimization of the number of wrong decisions, as a result of Bayes' law. Other criteria could be considered, such as using individual thresholds for each person in the database; again, as our goal is to measure the advantages of RPM by report to PCA feature extraction, we will not investigate other ways of fixing thresholds and use the global threshold leading to FRR = FAR in the remaining of this study.

FEATURE EXTRACTION

Taking decisions on rough images has been shown[9] to be dramatically sensitive to illumination conditions, viewpoints, expression and day-to-day differences in a face of the same person, to the point that two very similar (to the human eye) images could be extremely different if compared pixel by pixel. It is therefore necessary to extract relevant, discriminant features from the images and to compare the features instead of the rough images. Of course, the more discriminant are the features, the easier will be the subsequent authentication.

Face recognition/authentication depends heavily on the particular choice of features used by the classifier [10,11].

The random pulling model: In this approach, an image A_i with two dimensions of a face is transformed into a vector X_i of dimension (nxm), by connecting the lines (or columns) where n and m are respectively the numbers of lines and columns of the image A_i. Once vector X_i is formed we call upon a random pulling of d points among the set of the points of the vector X_i while keeping the drawn positions of the points in order to use those for all later random pulling. The d points drawn for each vector image form a vector Y_i. The vector Y_i is employed thereafter like a representation (feature) of the face image A_i.

Similarity measures and classification rule for RPM feature: The Random Classifier (RC) applies the RPM method on the (lower dimensional) augmented feature vector X_i. When an image is presented to the RC classifier, the high dimensionality feature vector X_i of the image is first formed and the lower dimensional feature, Y_i, is derived by using the procedure.

The similarity measures used in these experiments to evaluate the efficiency of different representation and authentication methods include L1 distance measure, δ_{L1} and *cosine* similarity measure, $\delta_{\cos}$, which are defined as follows:

$$\delta_{L_1}(x,y) = \sum_i |x_i - y_i| \quad (1)$$

$$\delta_{\cos}(x,y) = -\frac{x^T y}{\|x\| \, \|y\|} \quad (2)$$

where $\|\bullet\|$ denotes the norm operator.

Two parameters must be determined in the method: d and the threshold used for the authentication procedure. For each value of d, the threshold is fixed to have FAR= FRR; d is chosen to minimize this error rate. Finally, the performances of the method (including the threshold value) are measured on an independent test set (on this set, FAR will not be necessarily equal to FRR).

RESULTS AND DISCUSSION

These experiments were performed on frontal face images from the XM2VTS database[12]. The XM2VTS database is a multimodal database consisting of face images, video sequences and speech recordings taken of 295 subjects, four taken over a period of four months. This database is available at the cost of distribution from the University of Surrey[13]. The database is primarily intended for research and development of personal identity verification systems where it is reasonable to assume that the client will be cooperative. Since the data acquisition was distributed over a long period of time, significant variability of appearance of clients, e.g. changes of hair style, facial hair, shape and presence or absence of glasses, is present in the recordings (Fig. 1).

The subjects were volunteers, mainly employees and PhD students at the University of Surrey of both sexes and many ethnical origins. The XM2VTS database contains 4 sessions. During each session two head rotation and speaking shots were taken. From the speaking shot, where subjects are looking just below the camera while reading a phonetically balanced sentence, a single image with a closed mouth was chosen. Two shots

Fig. 1: Sample images from XM2VTS database

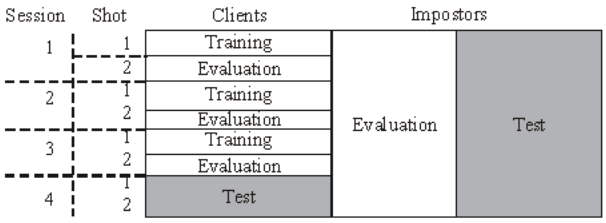

Fig. 2: XM2VTS database with Lausanne protocol configuration I

at each session, with and without glasses, were acquired for people regularly wearing glasses.

For the task of personal verification, a standard protocol for performance assessment has been defined. The so called Lausanne protocol splits randomly all subjects into a client and impostor groups[14]. The client group contains 200 subjects; the impostor group is divided into 25 evaluation impostors and 70 test impostors. Eight images from 4 sessions are used.

From these sets consisting of face images, training, evaluation and test sets are built. There exist two configurations that differ by a selection of particular shots of people into the training, evaluation and test sets. The training set is used to construct client models. The evaluation set is selected to produce client and impostor access scores, which are used to find a threshold that determines if a person is accepted or not (it can be a client-specific threshold or global threshold). According to the Lausanne protocol the threshold is set to satisfy certain performance levels (error rates) on the evaluation set. Finally the test set is selected to simulate realistic authentication tests where impostor's identity is unknown to the system.

The performance measures of a verification system are the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). False acceptance is the case where an impostor, claiming the identity of a client, is accepted. False rejection is the case where a client, claiming his true identity, is rejected. FAR and FRR are given by:

$$FAR = EI/Im*100\%, \quad FRR = EC/Cl*100\% \qquad (3)$$

where EI is the number of impostor acceptances, Im is the number of impostor claims, EC the number of client rejections and Cl the number of client claims. Both FAR and an FRR are influenced by an acceptance threshold. To simulate real application the threshold is set on the data from evaluation set to obtain certain false acceptance on the evaluation set (FAR) and false rejection error (FRR). The same threshold is afterwards applied to the test data and FAR and FRR on the test set are computed.

Table 1: Photos distribution in the various sets

Set	Clients	Impostor
Training	600(3 by subject)	0
Evaluation	600(3 by subject)	200(8 by subject)
Test	400(2 by subject)	400(8 by subject)

Fig. 3: a) Original image, b) Image after Cutting and down-sampling.

In these experiments we chose the distribution of the images in the various sets according to the configuration described by the Fig. 2[14]. The sizes of the various sets are included Table 1.

By looking at the images we clearly note the appearance of characteristics not desired on the level of the neck, like the collars of shirt, the sports shirts, etc. In addition, the hair is also a characteristic changing during the time (change of cut, colour, baldness...). The background appears on the images; it is used for nothing and inflates the size of the data unnecessarily. Finally the ears cause also a problem. Indeed, if the person presents herself slightly differently in front of the camera (rotation), we can see only one ear. This is why we decided to cut the image vertically and horizontally and to keep only one window of size 132×120 centered on the face. This window is automatically extracted from the frontal image by a technique based on projections of gradients, similar to that proposed by[15]. Then we pass the images by a 2×2 uniform filter to be able to carry out a decimation of factor 2. What reduces by 4 the size of the cut out image. The face image will pass thus from a dimension 256×256 = 65536 to a dimension 66×60 = 3960 (after cutting and decimation), as illustrated in Fig. 3.

Afterwards, we apply a photo-normalization. That is to say that for each image, we withdraw from each pixel the average value of those on the image and that we divide those by their standard deviation. Finally we make standardization. The photo-normalization acts on an image whereas standardization acts on a group of images (for each component, one withdraws the average of this component for all the images and one divides by the standard deviation).

For comparison purpose, we first implemented the Eigenfaces method[4] and the proposed method and tested their performance using the face images as illustrated in Fig. 4.

Fig. 4: Example XM2VTS images used in our experiments (cropped to the size of 132×120 to extract the facial region and filtered for down-sampled by two)

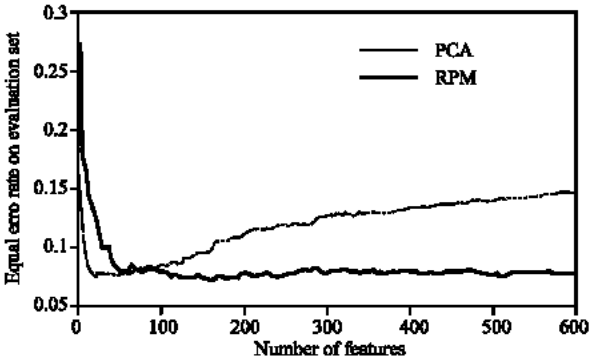

Fig. 5: Comparative face Authentication performance of the PCA method and the RPM method using distance measure

Note that the images are acquired during different photo sessions; they display both different lighting conditions and facial expressions. Three images are chosen from the eight images available for each subject for training and three images are chosen for evaluation, while the remaining images (unseen during training and evaluation) is used for testing. In particular, the above figure shows in the top two rows the examples of training and evaluation respectively images used in these experiments and in the bottom row the examples of test images.

The equal error rate FAR=FRR obtained on the evaluation set in face authentication performance of these tow methods apply the distance measure (Fig. 5) and one

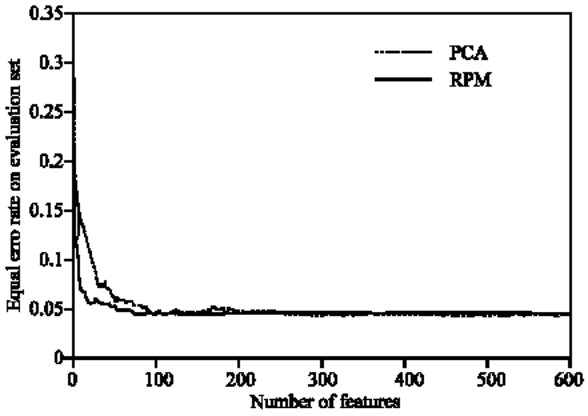

Fig. 6: Comparative face Authentication performance of the PCA method and the RPM method using distance measure

can see from the figure that the proposed method performs better followed by the Eigenfaces method; we use a small number of features.

The equal error rate FAR=FRR obtained on the evaluation set in face authentication performance of these tow methods apply the L1 distance measure (Fig. 5) and one can see from the figure that the RPM method performs better than followed by the Eigenfaces method.

It has been found experimentally that using δ_{cos} distance between feature vectors instead of the Euclidean distance further improves the results(Fig. 6), therefore the measurement of similarity by δ_{cos} distance is adapted better than the Euclidian norm to data in great dimension.

In particular, the proposed method (RPM) achieves 4.21% equal error rate on face authentication we apply the cosine similarity measure on evalution set using only 302 features.

Our approach (RPM) has a very significant advantage compared to the PCA. Although the PCA appears equivalent to the RPM by using δ_{cos} as a distance measure (Fig. 6). This advantage of the RPM method holds in the fact that the operation of training is not repeated when we modify the data base by introducing other people (faces). Although in PCA method, we need

Table 2: RPM results for XM2VTS database with Lausanne protocol configuration I

Type of Method and distance	Evaluation Set FAR = FRR	Test Set FAR	FRR	(FAR+FRR)/2	Dimension of feature vector
PCA and δ_{L1}	9.64	11.30	9.75	10.52	157
RPM and δ_{L1}	7.07	7.13	8.75	7..94	
PCA and δ_{L1}	14.05	17.99	11.75	14.87	500
RPM and δ_{L1}	7.57	7.47	7.75	7.61	
PCA and δ_{cos}	4.67	6.54	4.75	5.65	250
RPM and δ_{cos}	4.67	618	5.00	6.59	
PCA and δ_{cos}	4.67	6.57	4.75	5.66	302
RPM and δ_{cos}	4.21	5.80	5.50	5.54	

to repeat the training operation each time when we introduce a person into the data base, because the projection space changes.

Table 2 shows some results obtained, of RPM on different sizes of feature vector. The used images are first cut and filtered by a 2×2 uniform filter and down-sampled by two. Finally we make a photo-normalisation and standardization of these images. Tow matching distances are presented: Euclidean L1 and *cosine* (also called normalized correlation). The last column shows the number of feature vector used.

CONCLUSIONS

We have introduced in this paper the new RPM method for face authentication. The RPM method, which is robust to variations in illumination and facial expression of face images. The feasibility of the RPM method has been successfully tested on face authentication using a data set from the XM2VTS database, which is a standard test bed for face authentication technologies. Specifically we used 2360 frontal face images corresponding to 295 subjects, which were acquired under variable illumination and facial expressions. In particular, RPM method achieves 4.21% equal error rate on face authentication using only 302 features apply the ***cosine*** similarity measure (δ_{cos}) distance.

The advantage of our approach (RPM) holds in the fact that the operation of training is not remade when we modify the data base by adding other people (faces), contrary to PCA method

Further work may consist in replacing the simple decision system authentifying the faces through simple distance comparisons between feature vectors, by a multi-dimensional classifier (artificial neural network) on the components of these vectors, or we propose the use of information of color in an RPM approach for various existing color spaces and to see which space to choose. One can also propose the fusion of the results of various spaces.

REFERENCES

1. Havran, C., L. Hupet, J. Czyz, J. Lee, L. Vandendorpe and M. Verleysen, 2002. Independent component analysis for face authentication KES'2002 proceedings-Knowledge-Based Intelligent Inform. Engin. Sys., Crema, Italy, pp: 16-18.
2. Kittler, J.and K. Messer, 2002. Fusion of multiple experts in multimodal biometric personal identity verification systems, IEEE Workshop, Neural Networks for Signal Processing, pp: 3-12.
3. Norman P., H. Thian, S. Marcel and S. Bengio, 2003. Improving face authentication using virtual samples, IEEE Conf. Acoustics, Speech and Signal Processing, 3: 233-236.
4. Tefas, A., C. Kotropoulos and I. Pitas, 2001. Using support vector machines to enhance the performance of elastic graph matching for frontal face authentication, IEEE Transaction on Pattern Analysis and Machine Intelligence, 23: 735-746.
5. Kotropoulos, C.L., A. Tefas and I. Pitas, 2000. Frontal face authentication using discriminating grids with morphological feature vectors, IEEE Transactions on Multimedia, 2: 14-26.
6. Turk, M. and A. Pentland, 1991. Eigenfaces for recognition, J. Cognitive Neuroscience, 3: 71-86.
7. Djamel , Saigaa, N. Benoudjit, K. Bemahamed and S. Lelandaius, 2005. Authentification d'individus par reconnaissance de visages, University of Biskra Journal, Courier du Savoir, 6: 61-66.
8. Saigaa, D., N. Benoudjit, K. Bemahamed and S. Lelandaius, 2005. Face authentication using enhanced fisher linear discriminant model (EFM), WSEAS Int'l. Conf. on Computational Intelligence, Man-Machine Systems and Cybernetics (CIMMACS'05) in Miami, Florida, USA, pp: 17-19.
9. Belhumeur, P.N., J.P. Hespanha and D.J. Kriegman, 1997. Eigenfaces vs. Fisherfaces: Recognition using Class Specific Linear Projection, IEEE Trans. Pattern Analysis and Machine Intelligence, 19: 711-720.
10. Liu, C. and H. Wechsler, 2000. Evolutionary pursuit and its application to face recognition, IEEE Trans. Pattern Analysis and Machine Intelligence, 22: 570- 582
11. Liu, C. and H.Wechsler, 2000. Robust coding schemes for indexing and retrieval from large face databases, IEEE Trans. on Image Processing, 9: 132-137.
12. Messer, K., J. Matas, J. Kittler, J. Luettin and G. Maître, 1999. XM2VTSBD: The Extended M2VTS database. Int'l Conf. on Audio- and Video-based Biometric Authentication (AVBPA 99), Washington D.C., pp: 72-77.
13. http://xm2vtsdb.ee.surrey.ac.uk/.
14. Luettin, J. and G. Maître, 1998. Evaluation protocol for the extended M2VTS database(XM2VTSDB) IDIAP tech. report, Martigny.
15. Roberto, B. and T. Poggio, 1993. Face recognition: futures versus templates, IEEE Trans. Pattern Analysis and Machine Intelligence, 15: 1042- 1052.