Available at
www.ComputerScienceWeb.com
POWERED BY SCIENCE @ DIRECT®

Pattern Recognition Letters 24 (2003) 215–225

Pattern Recognition Letters

www.elsevier.com/locate/patrec

# Membership authentication in the dynamic group by face classification using SVM ensemble

Shaoning Pang [*], Daijin Kim, Sung Yang Bang

*Department of Computer Science and Engineering, Pohang University of Science and Technology, San 31, Hyoja-Dong, Nam-Gu, Pohang 790-784, South Korea*

Received 5 March 2002; received in revised form 26 April 2002

**Abstract**

This paper presents a method for authenticating an individual's membership in a dynamic group without revealing the individual's identity and without restricting the group size and/or the members of the group. We treat the membership authentication as a two-class face classification problem to distinguish a small size set (membership) from its complementary set (non-membership) in the universal set. In the authentication, the false-positive error is the most critical. Fortunately, the error can be validly removed by using the support vector machine (SVM) ensemble, where each SVM acts as an independent membership/non-membership classifier and several SVMs are combined in a plurality voting scheme that chooses the classification made by more than the half of SVMs. For a good encoding of face images, the Gabor filtering, principal component analysis and linear discriminant analysis have been applied consecutively to the input face image for achieving effective representation, efficient reduction of data dimension and strong separation of different faces, respectively. Next, the SVM ensemble is applied to authenticate an input face image whether it is included in the membership group or not. Our experiment results show that the SVM ensemble has the ability to recognize non-membership and a stable robustness to cope with the variations of either different group sizes or different group members. Also, we still get a reasonable membership recognition rate in spite of the limited number of membership training data.

*Keywords:* Membership authentication; Gabor filter; Principal component analysis; Linear discriminant analysis; Support vector machine ensemble

## 1. Introduction

Authenticating membership in a group is a common task because privileges such as the right to entering an important lab are often assigned to many individuals. While permission to exercise a privilege requires that members of the group be distinguished from non-members, the members need not be distinguished from one another. Most existing research that authenticates membership in

[*] Corresponding author. Tel.: +82-54-279-8075; fax: +82-54-279-2299.

*E-mail addresses:* snpang@postech.ac.kr (S. Pang), dkim@postech.ac.kr (D. Kim), sybang@postech.ac.kr (S.Y. Bang).

0167-8655/03/$ - see front matter © 2002 Elsevier Science B.V. All rights reserved.
PII: S0167-8655(02)00213-1

a group do so by identifying an individual, then verifying that individual is a member. This requires that an individual must be identified to authenticate his or her membership. Such approaches are highly individual dependent, which makes supporting dynamic groups unwieldly: whenever individuals are added or changed in the group, existing system performance will fluctuate with the variation of membership in the group.

As is well known, high security membership verification needs such a composite system, which usually includes the authentication of face, fingerprint, eyeball and other biometric modalities. The importance of human face discrimination on facial identification resulted in many previous works on face recognition (Pentland and Turk, 1999; Turk and Pentland, 1991; Zhujie and Yu, 1994; Liao and Li, 2000; Gutta et al., 2000). In (Lyons et al., 2000), they used the Gabor wavelet-labelled elastic graph matching algorithm to gender recognition, in which the sizes of male and female group are very similar and/or relatively fixed. Also in (Lyons et al., 2000), the support vector machines (SVMs) were employed on the gender classification. However, the above research did not refer to stability in the classification performance of the used classifiers, which is an important factor in dynamic membership authentication where both the size of the group and the members in the group change dynamically.

Unlike previous works on face recognition, which classifies a face image as a picture of a given individual, we focus on the problem of face authentication of membership in dynamic groups. It is to distinguish a certain part of face images, the membership faces, from the remaining part of face images in a given face image group. Here, the membership group is dynamic, which means that (1) the size of the membership group varies arbitrarily and (2) the members in the membership group change randomly.

To cope with these variations, we propose a novel membership authentication method that combines an eigenface fusing technique and the idea of SVM ensemble. The eigenface fusing technique is proposed to deal with the dynamically change of membership group. In addition, we take the SVM ensemble for the robust authentication due to its outstanding stability power of the SVM ensemble, which was proven in our previous work (Pang et al., 2001). Therefore, the originally rigid face authentication problem is induced to the dynamic face groups discerning, in which not only a trusted part (membership) may add or remove members in the group, but the whole group can be varied as well.

This paper is organized as follows. Section 2 introduces the idea of dynamic membership authentication by face classification. Section 3 describes an effective facial feature encoding for a good classification. Section 4 presents the principle of SVM ensemble. Section 5 presents the experimental results and discussions. Finally, a conclusion is drawn.

## 2. Membership authentication by face classification

As mentioned above, the problem of membership authentication can be eventually treated as a binary classification. The differences from other binary classifications are that:

1. Both the size of the membership group and the members in the membership group are dynamically changed.
2. The size of the membership group usually is smaller than the size of the non-membership group.

Fig. 1 illustrates one typical example of a dynamic group, where the membership group $M$ is a subgroup of the universal set $G$, and $\overline{M} = G - M$ is the non-membership group. The dash-lined circle denotes some examples of different membership groups, which indicates that either the size or the member of the membership group is changeable.

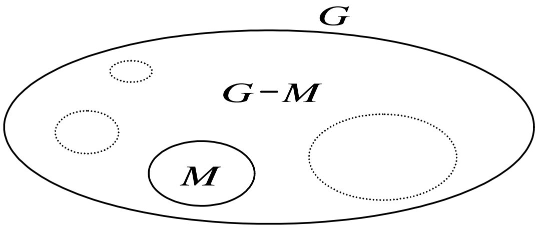

Fig. 1. An illustration of dynamic membership group.

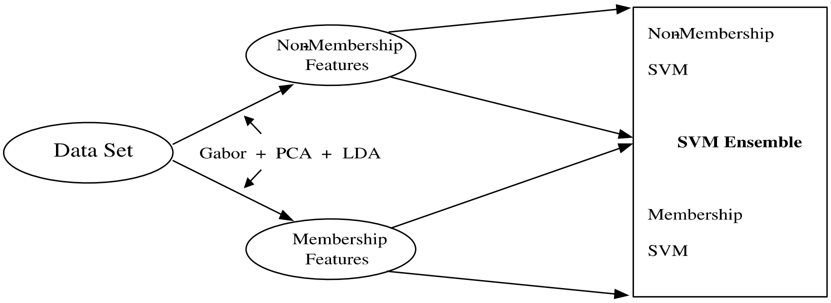

Fig. 2. Membership authentication algorithm.

Consider a certain human group $G$ with $N$ members. If there exists an arbitrary subgroup $M = \{\mathbf{x}_i | i = 1, \ldots, k\} \subset G$, where $k = |M| < N/2$, then it is a membership group, and the remaining peoples $\overline{M} = G - M$ make a non-member group. Thus, the membership authentication problem can be depicted by a typical binary classification problem as

$$f(\mathbf{x}) = \begin{cases} 1 & \text{if } \mathbf{x} \in M, \\ -1 & \text{otherwise.} \end{cases} \tag{1}$$

A direct solution of Eq. (1) is to identify each input face as one of the individual members in the group, as Eq. (2).

$$f(x) = \begin{cases} 1 & \text{if } x = x_j,\ x_j \in M,\ j \in (1, |M|), \\ -1 & \text{otherwise.} \end{cases} \tag{2}$$

This identification-based method involves a multi-class classification procedure, which make it lose the adaptive capability for the dynamic membership authentication. Furthermore, as the whole members of the dynamic group increases, the off-line computation time for membership authentication becomes huge, because most multi-class classifiers work as the combination of binary classifier, such as multiclass SVM is a one-to-one/one-to-all exhaustive ransacking combination of binary SVM classifier.

To overcome this problem, we modify the membership authentication procedure into Eq. (3), where *fusion* function that consists of three sequential operations: Gabor filtering, principal component analysis (PCA), and linear discriminant analysis (LDA). It compresses all the member and all the non-member into membership faces and non-membership faces respectively. Consequently, a people is assigned into the membership or the non-membership group depends on the spacial distance from the people to the membership or non-membership model. That is one binary class classification procedure.

$$f(\mathbf{x}) = \begin{cases} 1 & \text{if } \mathbf{x} \mapsto \text{Model}_M(\text{fusion}(M)), \\ -1 & \text{if } \mathbf{x} \mapsto \text{Model}_{\overline{M}}(\text{fusion}(\overline{M})), \end{cases} \tag{3}$$

where $\mapsto$ implies "near to the model", and $\text{Model}_M(\cdot)$ and $\text{Model}_{\overline{M}}(\cdot)$ denote the classifier models of the membership and the non-membership model, respectively.

The following is a summary of the steps of the dynamic membership authentication algorithm, which consists of Gabor feature extraction, PCA membership face fusing, LDA feature scattering, and SVM ensemble classification. Individual steps are detailed in the subsections below and shown schematically in Fig. 2.

## 3. Effective facial encoding for good classification

### 3.1. Gabor wavelet feature

Gabor wavelet feature has been widely used both in the face recognition and the fingerprint authentication (Moghaddam and Yang, 2000; Jain et al., 1999). A 2D Gabor function is a Gaussian modulated by a sinusoid. It is a non-orthogonal wavelet and it can be specified by the frequency of the sinusoid $\omega = 2\pi f$ and the standard deviations of Gaussian $\sigma_x$ and $\sigma_y$.

$$g(x,y:f,\theta)=\exp\left(-\frac{1}{2}\left(\frac{x'^2}{\sigma_x^2}+\frac{y'^2}{\sigma_y^2}\right)\cos(2\pi f x')\right), \tag{4}$$

$$\begin{aligned} x' &= x\sin\theta + y\cos\theta,\\ y' &= x\cos\theta - y\sin\theta, \end{aligned} \tag{5}$$

where $f$ is the frequency of the sinusoidal plane wave along the direction $\theta$ from the $x$-axis, $\sigma_x$ and $\sigma_y$ specify the Gaussian envelope along $x$- and $y$-axes, respectively, which determine the bandwidth of the Gabor filter. For our experiment data (8 bits gray facial image, with the size of 46 × 56), 20 spatial frequencies are used, with $f=\pi/2^i$, $(i=1,\ldots,5)$ and $\theta=k\pi/4$, $(k=1,\ldots,4)$.

### 3.2. Face fusion by principal component analysis

According to PCA theory, all face images of the members or non-members can be compressed into a set of holistic faces, which are represented by a set of eigenfaces, which together characterize the variations among all face images in the groups. We call them "membership face" or "non-membership face".

The computation of eigenfaces is based on the PCA, which finds the optimal directions for the best representation of the training face images in the mean squared error sense. Let the training set of face images be $I_1, I_2, I_3, \ldots, I_M$. The average face of the training face image data set is defined by $\varphi=(1/M)\sum_{i=1}^{M} I_i$. Each face differs from the average by the vector $\phi_i = I_i - \varphi$. The set of very large vectors is then subject to PCA to identify a set of $M$ orthonormal vectors $\boldsymbol{u}_i$ $(i=1,2,\ldots,M)$ and their associated eigenvalues, which describes the distribution of the data very well. The vectors $\boldsymbol{u}_i$ are the eigenvectors of the covariance matrix as

$$Q=\frac{1}{M}\sum_{i=1}^{M}\phi_i\phi_i^{\mathrm{T}}=\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}. \tag{6}$$

By Skurichina and Duin (1996), $\boldsymbol{u}_i$ can be computed as

$$\boldsymbol{u}_i=\sum_{k=1}^{M} v_k\phi_k, \tag{7}$$

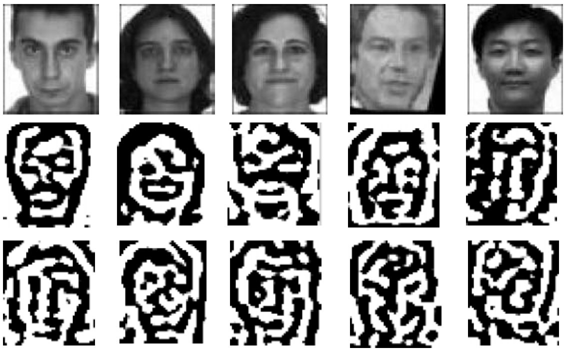

Fig. 3. Ten dominant eigenfaces of Gabor-filtered features of the membership face images.

where $v_k$ are the eigenvectors of the matrix $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$, $i=1,2,\ldots,M$. Then, the eigenfaces are chosen as the $M'$ $(\ll M)$ vectors $\boldsymbol{u}_k$ $(k=1,2,\ldots,M')$ that correspond to the largest $M'$ eigenvalues of the matrix $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$. Fig. 3 illustrates the first 10 eigenfaces of the Gabor-filtered features of five face images included in the membership group.

Next, a new input face image can be transformed into its eigenface features by operation $\boldsymbol{w}_k = \boldsymbol{u}_k^t(I-\varphi)$, where $k=1,2,\ldots,M'$ and the weights form a feature vector $F=[\boldsymbol{w}_1,\boldsymbol{w}_2,\ldots,\boldsymbol{w}_{M'}]$ that describes the contribution of each eigenface in representing the input image.

### 3.3. Feature scattering by linear discriminant analysis

After fusing both members and non-members to their primary components, we have investigated the distribution of two classes (member and non-member) in Gabor eigenfeature space. The distribution looks like Fig. 4(a), in which we noticed that feature vectors of members and non-members are mixed together, so it is difficult for the lower-order non-linear classifier to distinguish them. To overcome this difficulty, we turn to another data transformation technique, LDA (Kak and Martinez, 2001).

LDA seeks a single projection that can optimally separate the two-labelled clusters in the distribution space, and make them have a minimum within-cluster distance and a maximum between-cluster distance. Thus, the ratio of the

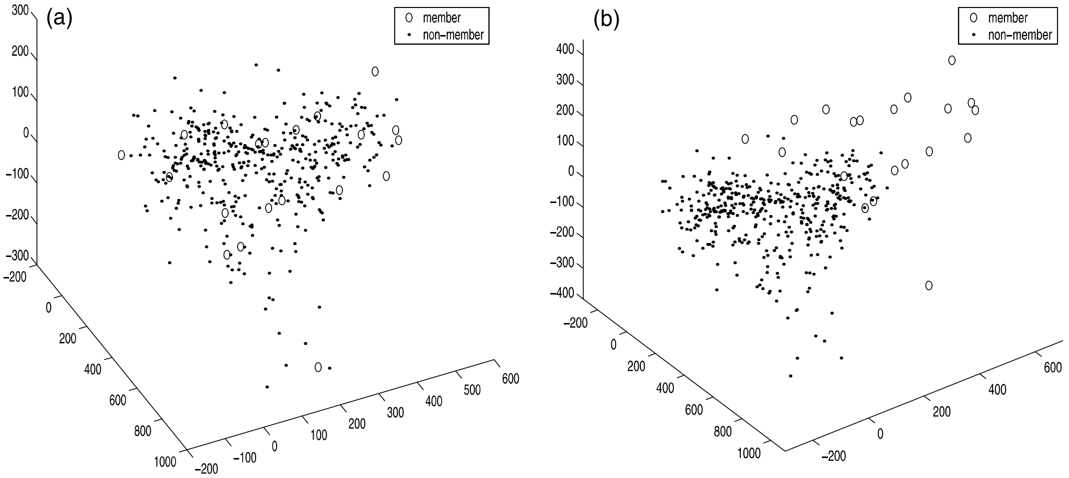

Fig. 4. An illustration of feature transformation by LDA (the left: feature space before LDA and the right: feature space after LDA).

between class scatter to the within class scatter, $J(\boldsymbol{w})$ is maximized.

$$J(\boldsymbol{w}) = \frac{\boldsymbol{w}^{\mathrm{T}} S_B \boldsymbol{w}}{\boldsymbol{w}^{\mathrm{T}} S_w \boldsymbol{w}}, \tag{8}$$

where

$$S_w = \sum_{i=-1}^{1} \sum_{x \in F_i} (\boldsymbol{x} - \boldsymbol{m}_i)(\boldsymbol{x} - \boldsymbol{m}_i)^{\mathrm{T}}, \tag{9}$$

$$S_B = (\boldsymbol{m}_1 - \boldsymbol{m}_2)(\boldsymbol{m}_1 - \boldsymbol{m}_2)^{\mathrm{T}}. \tag{10}$$

The optimal value of $w$ can be obtained by solving the following equation:

$$\frac{\partial J(\boldsymbol{w})}{\partial \boldsymbol{w}} = 0. \tag{11}$$

With the projection matrix $\boldsymbol{w}$, the eigenfeatures in Fig. 4(a) can be optimally redistributed as Fig. 4(b), which is easier to classify into two classes.

## 4. Membership authentication by support vector machine ensembles

### 4.1. Support vector machine

The SVM is a new and promising classification and regression technique proposed by Vapnik and his group at AT&T Bell Laboratories (Cortes and Vapnik, 1995). Recent theoretical research work has solved the existing difficulty of using SVM in practical applications (Joachims, 1999; Platt, 1999). By now, it has been successfully applied in many areas, such as face detection, handwriting digital character recognition, data mining, etc.

In theory, SVM classification can be traced back to the classical structural risk minimization approach, which fixes the classification decision function by minimizing the classification risk as follows:

$$R = \frac{1}{l} \sum_{i=1}^{l} |f(\boldsymbol{x}_i) - y_i|, \tag{12}$$

where $f$ is the classification decision function. For SVM, the linearly separable problem can be treated as the classical classification decision function as

$$f_{w,b} = \mathrm{sign}(\boldsymbol{w} \cdot \boldsymbol{x} + b). \tag{13}$$

However, the SVM is trying to fix the optimal separating hyperplane by constructing the maximum margin between different classes as

$$\min : \tfrac{1}{2}\boldsymbol{w}^{\mathrm{T}}\boldsymbol{w},$$

$$y_i(w \cdot \boldsymbol{x}_i + b) \geqslant 1. \tag{14}$$

For a linearly non-separable case, the above formula can be extended by introducing a new set of variables $\{\xi_i | i = 1, 2, \ldots, l\}$ as the measurement of violation of the constraints (Cortes and Vapnik, 1995) as follows:

$$\min : \frac{1}{2}\boldsymbol{w}^{\mathrm{T}}\boldsymbol{w} + C\left(\sum_{i=1}^{l}\xi_i\right)^k,$$

$$y_i(\boldsymbol{w}^{\mathrm{T}}\varphi(\boldsymbol{x}_i) + b) \geqslant 1 - \xi_i, \tag{15}$$

where parameter $C$ and $k$ are used to penalize variables $\xi_i$, $\varphi(\cdot)$ is a non-linear function which maps the input space into a higher dimensional space. Minimizing the first term in Eq. (15) amounts to minimizing the VC-dimension of the learning machine, minimizing the second term in Eq. (15) controls the empirical risk. Therefore, in order to solve problem Eq. (15), this method needs to construct a set of functions, and implement classical risk minimization on the function set. Here, a Lagrangian method is used to solve the above problem. Then Eq. (15) can be written as

$$\max : F(\Lambda) = \Lambda \cdot \mathbf{1} - \tfrac{1}{2}\Lambda \cdot D\Lambda,$$

$$\Lambda \cdot y = 0; \quad \Lambda \leqslant C; \quad \Lambda > 0. \tag{16}$$

where $\Lambda = (\lambda_1, \ldots, \lambda_l)$, $D = y_i y_j \boldsymbol{x}_i \cdot \boldsymbol{x}_j$ for binary classification and the decision function Eq. (13) can be re-written as

$$f(\boldsymbol{x}) = \mathrm{sgn}\left(\sum_{i=1}^{l} y_i \lambda_i^* (\boldsymbol{x} \cdot \boldsymbol{x}_i) + b^*\right). \tag{17}$$

### 4.2. The support vector machine ensemble

The basic concept of SVM ensemble is to model a given input pattern by obtaining a classification from a group of SVMs and using a consensus scheme to decide the collective classification by vote. Thus, the ensemble of SVM is actually a type of cross-validation optimization of single SVM, and should have a more stable classification performance than other models, which we demonstrated in (Pang et al., 2001).

An ensemble of independently trained SVMs can make a collective classification in several ways. The most powerful voting rule appears to be a plurality in which the collective decision is the classification reached by more SVMs than any other. Besides, another strategy is the majority-voting rule that chooses the classification made by more than half of SVMs.

Suppose all SVMs arrive at the correct classification with a certain likelihood $1 - p$, the chances of seeing exactly $k$ errors among $N$ copies of the SVM is then

$$C_n^k p^k (1 - p)^{N-k}. \tag{18}$$

Thus, the possibility of the plurality scheme will be given as

$$\sum_{k>N/2}^{N} C_n^k p^k (1 - p)^{N-k}. \tag{19}$$

As long as $p$ is less than 0.5, and all the SVMs are independent, then the more SVMs will be used, and the lower the possibility of error by a plurality decision rule.

Based on the modelling of face authentication of membership in Section 2, a new input face image can be automatically identified by either the membership SVM classifier or the non-membership SVM classifier. However, for the SVM ensemble, the last output is given out by a decision support mechanism that seeks the best answer from all the SVM judgments. This will keep the classification performance of the system more stable. Therefore, we deal with the classification as a two-layer SVM ensemble, as shown in Fig. 5. The first layer SVMs are for membership and non-membership SVM modelling, and the second layer is a decision support machine based on the plurality strategy.

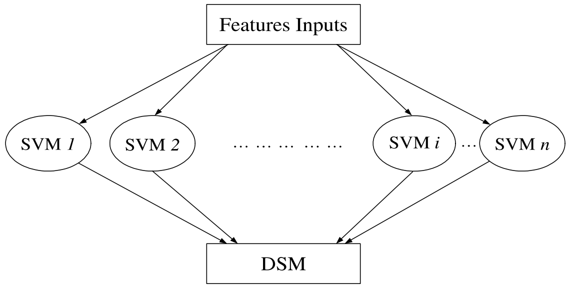

Fig. 5. A structure of SVM ensemble model.

## 5. Experiment results and discussion

We have implemented the proposed membership authentication technique on the Matlab platform. In our experiments, 1355 face images of 271 persons (five face images per person) are taken. Each image has the size of $56 \times 46$. The images are selected from AR (Purdue), AT&T, Yale, UMIST, University of Berne, and some face images obtained from MPEG-7 news videos (Kim et al., 2002). For all experiments, four images for a person are registered by training the SVM ensemble and one remaining image of the person is applied to the trained SVM ensemble for testing the authentication performance.

In order to remove the effect due to the illumination, each image is normalized to have a constant mean and variance. Because the changes of the hairstyle are rather little in our experimental data, we do not need to remove the hair information. But face images are cropped to keep only the main facial region for a robust face membership authentication system. Before we apply the proposed authentication method to the face images, we construct the face images for the membership group which are divided into a training and test set.

1. Randomly select a certain number of persons equal to the membership group size among 271 persons and assign them to the group member. The remaining persons are considered as non-group members.
2. Divide the membership group into training and test face images with the same sizes. Also, divide the non-member group in the same way. The percentage of the group member over total persons can be changed freely within 40%.

Then, we perform the Gabor feature extraction, valid facial feature extraction such as PCA and LDA, and face classification based on the SVM ensembles with polynomial kernel (Joachims, 1999), which we have discussed in above sections respectively. We test the proposed membership authentication over five different sizes of membership group. For the case of each membership group size, we carry out 10 trials with different group members. Fig. 6 illustrates a typical example of selecting 10 different groups, in which each group consists of five different persons.

The classification results of the proposed membership authentication method are listed in Table 1. Here, we consider two different types of authentication error, such as ‘‘true-negative error’’ and ‘‘false-positive error’’, where the former means that members are identified as non-members and the latter means non-members are identified as members, respectively. As we have seen in Table 1, the proposed membership authentication method provides a very good performance on non-membership authentication in that the average false-positive error is about 0.003. In fact, such a near zero false-positive misclassification error rate is very important for a security system, because it is dangerous to treat some non-members as members. On the other hand, it seems that true-negative misclassification error of the proposed authentication method is not good as the expectation, especially for the cases of small group-size,

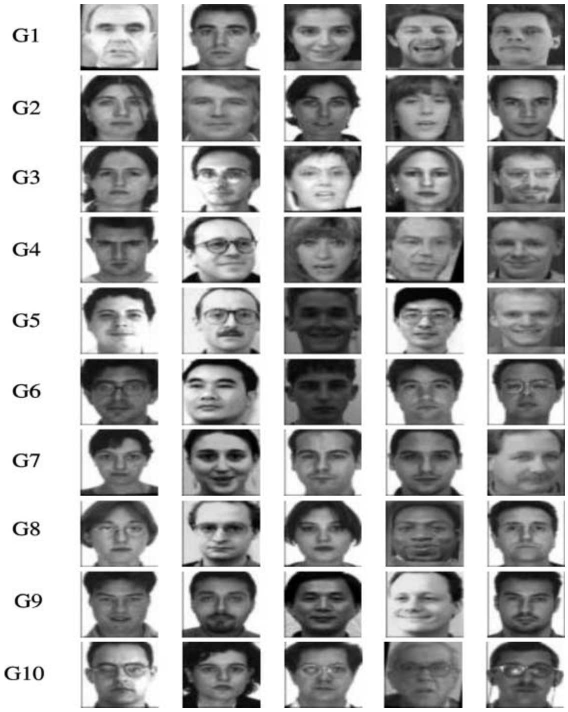

Fig. 6. Ten different membership groups with five members per each group.

Table 1
The classification results of the proposed membership authentication

| Group size | Correct rate (%) | True-negative error (%) | False-positive error (%) |
|---|---|---|---|
| 10 | 97.78 (= 265/271) | 1.85 (= 5/271) | 0.37 (= 1/271) |
| 20 | 98.52 (= 267/271) | 1.48 (= 4/271) | 0.00 (= 0/271) |
| 30 | 98.15 (= 266/271) | 1.85 (= 5/271) | 0.00 (= 0/271) |
| 40 | 96.68 (= 262/271) | 2.58 (= 7/271) | 0.74 (= 2/271) |

Table 2
The comparison result of authentication error between two different authentication methods

| Group size | Proposed method (%) | | | | Identification-based method (%) |
|---|---|---|---|---|---|
| | 10 | 20 | 30 | 40 | |
| Ex1(que:1,reg:2,3,4,5) | 1.1 | 1.1 | 1.5 | 2.6 | 0.6 |
| Ex2(que:2,reg:1,3,4,5) | 1.1 | 1.8 | 1.5 | 2.9 | 2.9 |
| Ex3(que:3,reg:1,2,4,5) | 2.9 | 1.5 | 1.8 | 2.9 | 0.6 |
| Ex4(que:4,reg:1,2,3,5) | 2.9 | 1.1 | 2.2 | 3.7 | 5.0 |
| Ex5(que:5,reg:1,2,3,4) | 2.9 | 1.8 | 2.2 | 4.4 | 18.0 |
| Average | 2.2 | 1.5 | 1.8 | 3.3 | 5.4 |
| Variance | 10.1e−005 | 1.4e−005 | 1.3e−005 | 5.5e−005 | 530.0e−005 |

such as 5 or 10 member cases, where the authentication error rate are near to half percent. But we can regard it as reasonable, because for small group sizes, five pictures for each member are not enough for the valid training of each SVM. Fortunately, as shown in Table 1, the true-negative misclassification error for the membership authentication drops down as the size of the membership group increases.

Table 2 shows the comparison results of authentication performance between the proposed membership authentication method and the identification-based authentication method in terms of authentication error defined by the sum of true-negative error and false-positive error. Here, the latter authentication method is based on the face recognition method using the embedded hidden markov model (HMM) with the 2nd-order block-specific eigenvectors, whose detailed description can be found in (Kim et al., 2002). Among five images of each person, four images are chosen for training the SVM and one remaining image for testing the authentication performance. We take a fivefold cross validation technique such that all images in the database were included in the testing set. Here, Ex1(que:1,reg:2,3,4,5) means, for each person, four images labelled as '2', '3', '4', and '5' are used for registering the SVM and the remaining image labelled as '1' is used for testing the identification. From this table, we note that (1) our proposed authentication method is superior to the identification-based authentication method in all different number of group sizes since the authentication error of the proposed method in the case of group size with 40 members [1] is 3.3% while the authentication error of the identification-based authentication method is 5.4%, (2) among four different group sizes, the case of the group size with 20 members shows the best authentication performance, and (3) our proposed authentication method is more stable than the identification-based authentication method in all different number of group sizes since the variance of authentication errors of the proposed authentication method (=4.6e−005 in average) is much smaller than that of the identification-based authentication method (=530.0e−005). The last result is particularly significant in the case of dynamic membership

[1] In fact, this is the worst case.

authentication problem whose size of group members are often changing dynamically.

In order to test the stability of the proposed authentication method under the variation of the members in a specific group size, we randomly select 10 different groups per each group size. We applied the proposed authentication method to each group independently. Fig. 7 shows that the authentication performance of our proposed method is very stable because the correct authentication rate is almost constant in the range of from 97% to 98.5% without regard to the variations of members in the group with the same group size.

Another stability analysis concerns the authentication performance of under the variation of the size of members in the membership group. We test the proposed authentication algorithm with the different sizes of membership group ranging from 5 to 95 persons with the step size of five persons, and represent the trend of correct authentication rate using linear interpolation. Fig. 8 shows the authentication performance in terms of the number of misclassifications in the case of membership and non-membership authentication. From the figure, we note that the proposed authentication method has a good ability to recognize

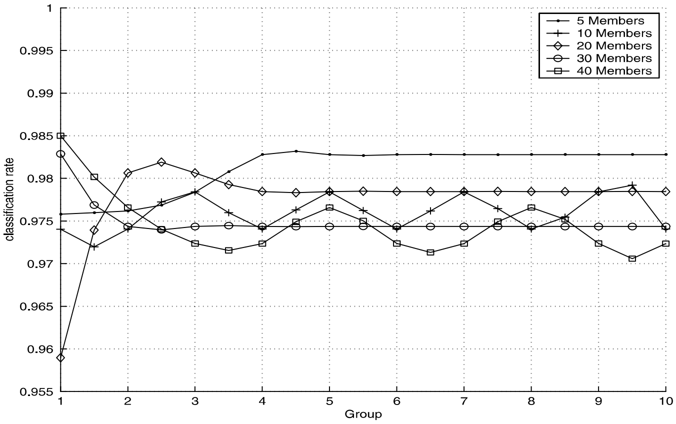

Fig. 7. Stability test under different members.

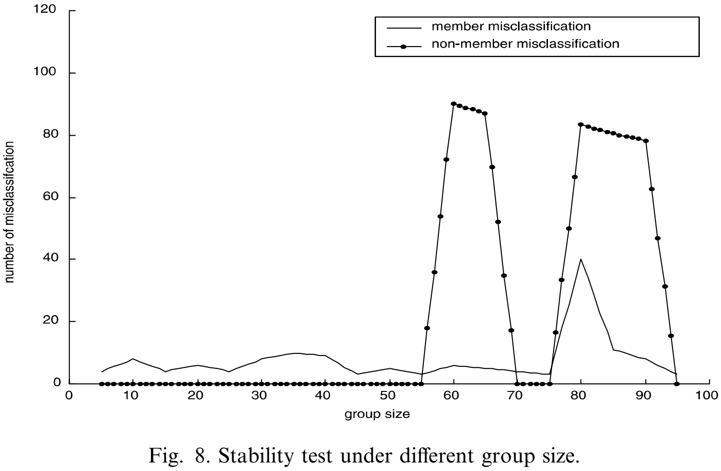

Fig. 8. Stability test under different group size.

non-membership, and the membership authentication takes a majority part of the misclassification.

In addition, we also note that, PCA projects the membership face features and non-membership into two eigenface-dominant spaces. With the increment of membership group size, the primary components and their dominant spaces become similar, thus it will certainly result in a larger classification difficulty, which makes the authentication performance in Fig. 8 become very unstable. Especially when using linear kernel in SVM, large misclassification errors are possible.

## 6. Conclusions

In this paper, we proposed a membership authentication method by face classification using the SVM ensemble, in which the size of membership group and the members in the membership group can be changed dynamically. Unlikely other face recognition works, the proposed method can authenticate the membership without recognizing the individual identities of face images, and the system's authentication performance is very robust to the changes of both the size of membership group and the members of membership group.

We considered many valuable approaches for implementing the proposed membership authentication system as follows. First, each face image was Gabor-filtered using a variety of different frequencies and directions to increase the robustness to the variation of external conditions like illumination and pose. Second, many Gabor-filtered images for a person were fused into one facial image to build membership and non-membership feature space. Third, all the facial images for the member (or non-member) group were represented by a specific set of eigenfaces via a PCA technique. Fourth, the eigenfeatures obtained by the projection were transformed by LDA technique for a better classification capability. Finally, the facial features were classified by the SVM ensemble that was comprised of several independently trained SVMs for a collective decision.

However, one problem with the proposed authentication method is that the correct classification rate for the membership is highly degraded when the size of members is small (<20), due to the limited training data set. Nevertheless, simulation results show that the authentication performance of the proposed method can keep stable for the member group with a size of less than 50 persons. It is also very robust to variation of the members in the membership group.

## Acknowledgements

The authors would like to thank the Ministry of Education of Korea for its financial support toward the Electrical and Computer Engineering Division at POSTECH through its BK21 program.

## References

Cortes, C., Vapnik, V., 1995. Support vector network. Machine Learning 20, 273–297.

Gutta, S., Huang, J., Jonathon, P., Wechsler, H., 2000. Mixture of experts for classification of gender, ethnic origin, and pose of human faces. IEEE Transactions on Neural Networks 11 (4), 948–960.

Jain, A.K., Prabhakar, S., Lin, H., 1999. A multichannel approach to fingerprint classification. IEEE Transactions on Pattern Analysis and Machine Intelligence 21 (4), 348–359.

Joachims, T., 1999. Making large-scale support vector machine learning practical. In: Advances in Kernel Methods: Support Vector Machines. MIT Press, Cambridge, MA.

Kak, A.M., Martinez, A.C., 2001. PCA versus LDA. IEEE Transactions on Pattern Analysis and Machine Intelligence 23 (2), 228–233.

Kim, M., Kim, D., Bang, S., Lee, S., 2002. Face Recognition Descriptor Using the Embedded HMM with the 2nd-order Block-specific Eigenvectors. ISO/IEC JTC1/SC21/WG11/M7997, Jeju, March 2002.

Liao, R., Li, S.Z., 2000. Face recognition based on multiple facial features. In: Proceedings of Automatic Face and Gesture Recognition, pp. 239–244.

Lyons, M.J., Budynek, J., Plante, A., Akamatsu, S., 2000. Classifying facial attributes using a 2-D Gabor wavelet representation and discriminant analysis. In: Proceedings of Automatic Face and Gesture Recognition, pp. 202–207.

Moghaddam, B., Yang, M.H., 2000. Gender classification with support vector machines. In: Proceedings of Automatic Face and Gesture Recognition, pp. 306–311.

Pang, S.N., Kim, D., Bang, S.Y., 2001. Fraud detection using support vector machine ensemble. ICONIP2001, pp. 1344–1349.

Pentland, A.P., Turk, M.A., 1999. Eigenfaces for recognition. Journal of Cognitive Neuroscience 3 (1), 71–86.

Platt, J., 1999. Fast training of support vector machines using sequential minimal optimization. In: Advances in Kernel Methods: Support Vector Machines. MIT Press, Cambridge, MA.

Skurichina, M., Duin, R.P.W., 1996. Stabilizing classifiers for very small sample size. In: Proceedings of International Conference on Pattern Recognition, vol. 2, pp. 891–896.

Turk, M.A., Pentland, A.P, 1991. Face recognition using eigenfaces. In: Proceeding of Computer Vision and Pattern Recognition, pp. 586–591.

Zhujie, J.I., Yu, Y.L., 1994. Face recognition with eigenfaces. In: Proceeding of IEEE Conference on Industrial Technology, pp. 434–438.