Face Authentication for Access Control based on SVM using Class Characteristics

SeHun Lim, Sanghoon Kim, Sun-Tae Chung, and Seongwon Cho

Abstract—Face authentication for access control is a face membership authentication which passes the person of the incoming face if he turns out to be one of an enrolled person based on face recognition or rejects if not. Face membership authentication belongs to the two class classification problem where SVM(Support Vector Machine) has been successfully applied and shows better performance compared to the conventional threshold-based classification. However, most of previous SVMs have been trained using image feature vectors extracted from face images of each class member(enrolled class/unenrolled class) so that they are not robust to variations in illuminations, poses, and facial expressions and much affected by changes in member configuration of the enrolled class

In this paper, we propose an effective face membership authentication method based on SVM using class discriminating features which represent an incoming face image's associability with each class distinctively. These class discriminating features are weakly related with image features so that they are less affected by variations in illuminations, poses and facial expression.

Through experiments, it is shown that the proposed face membership authentication method performs better than the threshold rule-based or the conventional SVM-based authentication methods and is relatively less affected by changes in member size and membership.

Keywords—Face Authentication, Access control, member ship authentication, SVM.

I. INTRODUCTION

FOR safer society, interests in constructing a reliable access control system based on personal identification have been increasing [1]. Biometric based identification is more reliable than token based system (card, key, and etc.), and face recognition among biometric identification systems are natural and does not have less negative responses in using from peoples, and thus much more research efforts have been pouring into this area among biometric areas [2,3].

Face recognition used for access control is face membership authentication. Face membership authentication system accepts an incoming person if he is determined to be a member (enrolled person) based on face recognition, and rejects him if not. Previously, face membership authentication systems usually adopt a threshold decision rule. That is, a face membership authentication system determines acceptance or rejection of an incoming face by checking whether the

SeHun Lim, Sanghoon Kim and Sun-Tae Chung are with School of Electronic Engineering, Soongsil University, Seoul, Korea (e-mail: cst@ssu.ac.kr).

Seongwon Cho is with A.I. Lab., Hongik University, Seoul, Korea.

correlation between the incoming face image and one of face images in the enrolled face database exceeds the given threshold.

However, variations due to different environments in illuminations, poses, facial expressions, and aging are so great that the correlation between two images of the same person under different environments can be smaller than that between two images of the different persons [4]. Therefore, the threshold rule-based decision has a fundamental limitation in lowering FRR(False Rejection Ratio) and FAR(False Acceptance Ratio). Threshold rule is a linear method like PCA and LDA. Through past decade's researches in face recognition, it has been clarified that linear methods are inadequate to represent nonlinear variations like illuminations, poses and facial expressions in real face images.

Support Vector Machine (SVM) has been proved as a successful nonlinear classifier [5] since it has been introduced by Vapnik and his coworkers [6], and thus has attracted much attention in face recognition [7,8]. Since face authentication is two class (member or nonmember) classification where SVM has shown a good performance, SVM has been applied for face membership authentication [9,10]. Surely, if SVM is well trained, then the face membership authentication method based on SVM shows superior performance to that based on threshold rule [9,10].

Most of the previous researches utilizing SVM in face recognition trains and tests SVM using image feature vectors extracted from each face image like pixel intensity, eigenfaces, Fisherfaces, Haar-like features, and Gabor feature vectors.

It is well known that there are no image feature vectors in face recognition which are invariant with respect to illuminations, or poses, or facial expression. That is, all image feature vectors are affected by the variations in illuminations, poses, and facial expressions. Therefore, one cannot find feature vectors which can separate member face images from nonmember face images well. When SVM is trained about classification between member class and nonmember class by using image feature vectors, the trained SVM may have many drawbacks in classifying an incoming face. First, the trained SVM reflects the statistics of image feature vectors of training member set and nonmember set. The feature vectors of the incoming face may have more correlation with those of the wrong class due to variations in illuminations, or poses, or facial expression, and the trained SVM may misclassify the incoming face image. Secondly, nonmember class is much larger than member class, but nonmember face images used in

training are much less than nonmember face images not used in training. Thus, trained SVM may not represent nonmember class well as much as it represents member class. Thirdly, access control system allows membership change. If membership changes (drops or joins), the previously trained SVM may not represent membership class and non membership class well and needs to be trained again. All these drawbacks are mainly due to the fact that SVM is trained using image feature vectors which cannot identify class or class member distinctively.

Therefore, one needs to train SVM using class discriminating features which are relatively less affected by variations in illuminations, poses, facial expressions, and etc. and can discriminate classes distinctively and separate membership class from non membership class, well. Since such class discriminating features characterize classes, not each class member faces, they are free from membership change, and is relatively less affected by change in class membership configuration, and also robust to variations of illuminations, poses, and facial expressions. This kind of thoughts can be found in [11] which adopts dynamic similarity features in face recognition. But [11] uses LDA classifier, and moreover did not exploit the concept of class characteristics fully.

In this paper, we propose an efficient face membership authentication method based on SVM using class discriminating features. Through experimental experiences, we first observe some class discriminating features which can discriminate each class (member class and nonmember class) distinctively, and thus can separate each other. Then, we train SVM with such class discriminating features. Through experiments, it is shown that our proposed face membership authentication method performs better than previous SVM-based methods or threshold-based methods, and robust to change in membership configuration.

The rest of the paper is organized as follows. Section 2 explains some technical background for this paper, and Section 3 first explains our class discriminating features, and then proposes a new face membership authentication method based on SVM using class characteristics. Section 4 describes experiment results, and the conclusion is presented in Section 5.

II. BACKGROUND

A. SVM (Support Vector Machine)

SVM (Support Vector Machine) introduced by Vapnik and his coworkers [6] has been proved as a useful technique for data classification [5]. In this paper, we utilize LIBSVM library implementation of SVM algorithm [12]. Introduction of SVM here is mainly based on LIBSVM document [12].

Viewing the input data as two sets of vectors in an *n*-dimensional space, an SVM will construct a separating hyperplane in that space, one which maximizes the margin between the two data sets. To calculate the margin, one constructs two parallel hyperplanes, one on each side of the separating one, which are pushed up against the two data sets. Intuitively, a good separation is achieved by the hyperplane that

has the largest distance to the neighboring data points of both classes. The original optimal hyperplane algorithm proposed by Vladimir Vapnik was a linear classifier, later SVM is generalized to be non-linear classifiers by applying the kernel trick.

In machine learning, the kernel trick is a method for using a linear classifier algorithm to solve a non-linear problem by mapping the original non-linear observations into a higher-dimensional space, where the linear classifier is subsequently used; this makes a linear classification in the new space equivalent to non-linear classification in the original space.

We now explain C-SVC(C-Support Vector Classification) formulation of SVM which is used in this paper.

Given training vectors $x_i \in R^n, i = 1, \cdots, l$, in two classes, and a vector $y \in R^l$ such that $y_i = \{1, -1\}$, C-SVC [13] solves the following primal problem:

$$\min_{w,b,\xi} \frac{1}{2} w^T w + C \sum_{i=1}^{l} \xi_i \qquad (1)$$

$$\text{subject to } y_i(w^T \phi(x_i) + b) \geq 1 - \xi_i,$$

$$\xi_i \geq 0, i = 1, \cdots, l$$

Its dual formulation is as follows

$$\min_{\alpha} \frac{1}{2} \alpha^T Q \alpha - e^T \alpha \qquad (2)$$

$$\text{subject to } y^T \alpha = 0,$$

$$0 \leq \alpha_i \leq C, \ i = 1, \cdots, l$$

where e is the vector of all ones, $C > 0$ is the upper bound, Q is an l by l positive semi-definite matrix, $Q_{ij} \equiv y_i y_j K(x_i, x_j)$, and $K(x_i, x_j) \equiv \phi(x_i)^T \phi(x_j)$ is the kernel. Here training vectors x_i are mapped into a higher (maybe infinite) dimensional space by the function ϕ.

If $\alpha = (\alpha_1, \alpha_2, ..., \alpha_l)$ satisfying (2) is found, then $w^T \phi(x) = \sum \alpha_i y_i K(x_i, x)$, and $b = y_k - w^T \phi(x_k)$ for any x_k such that $\alpha_k \neq 0$.

Then, the decision function is

$$\text{sgn}\left(\sum_{i=1}^{l} y_i \alpha_i K(x_i, x) + b \right).$$

Some common kernels include,

① Polynomial (homogeneous): $K(x_i, x_j) = (x_i^T x_j)^d$

② Polynomial (inhomogeneous):

$$K(\mathrm{x}_i,\mathrm{x}_j) = (\gamma \mathrm{x}_i^{\mathrm{T}}\mathrm{x}_j + r)^d, \gamma > 0$$

③ Radial Basis Function (RBF):

$$K(\mathrm{x}_i,\mathrm{x}_j) = \exp(-\gamma \parallel \mathrm{x}_i - \mathrm{x}_j \parallel^2), \quad \gamma > 0$$

④ Sigmoid : $K(\mathrm{x}_i,\mathrm{x}_j) = \tanh(\gamma \mathrm{x}_i^{\mathrm{T}}\mathrm{x}_j + r)$

where γ, r ,and d are kernel parameters

In this paper, we use ③ Radial Basis Function as a kernel type.

B. Gabor wavelet, Gabor Jet, and Gabor Similarity

The Gabor feature vectors are reported as a best distinctive local feature for face recognition [14]. We adopt similarity between face images based on Gabor feature vectors in this paper.

The Gabor feature vectors at a point used in this paper are the ones obtained by convolving Gabor wavelet kernels with the intensity of the pixel at the point of face images.

The Gabor wavelet kernels used in this paper are as follows [15].

$$W(x,y,\theta,\lambda,\sigma) = e^{-\frac{1}{2\sigma^2}(\vec{x}\bullet\vec{x})} e^{i\vec{k}\bullet\vec{x}} \tag{3}$$

where wave vector $\vec{k}$ is given as $\vec{k} = \left(\frac{2\pi\cos\theta}{\lambda}, \frac{2\pi\sin\theta}{\lambda}\right)^t$, and θ represents wavelet direction, λ represents wave length , σ in (3) represents the size of Gaussian, and is proportional to λ . In this paper, we consider 40 Gabor wavelet kernels obtained by $\theta \in \{0, \frac{\pi}{8}, \frac{2\pi}{8}, \frac{3\pi}{8}, \frac{4\pi}{8}, \frac{5\pi}{8}, \frac{6\pi}{8}, \frac{7\pi}{8}\}$, $\lambda \in \{4, 4\sqrt{2}, 8, 8\sqrt{2}, 16\}$ and $\sigma = \lambda$ in (3). Let us denote the Gabor wavelet coefficient (Gabor feature vector) obtained by convolving j-th one among the above 40 Gabor wavelet kernels with $I(x^i,y^i)$ (intensity of image at point (x^i,y^i)) as $J_j^i(x^i,y^i)$. Then, Gabor jet $J^i(x^i,y^i)$ at a pixel point (x^i,y^i) of an image is defined to be the set $J^i = \left\{J_j^i; j=1,...,40\right\}$.

Each Gabor wavelet coefficient J_j^i can be represented as $J_j^i = a_j^i e^{i\phi_j^i}$ (magnitude a_j^i , phase ϕ_j^i).

When n Gaber jets are extracted from a face image A at the positions $\left\{(x^1,y^1),(x^2,y^2),...,(x^n,y^n)\right\}$, we call $J(A) = \left\{J^i; i=1,...,n\right\}$ as a face Gabor bunch of face image A.

In this paper, face Gabor similarity $S(J(A),J(B))$ between face A and face B is defined as a correlation between face Gabor bunch of two face images in the following way [15] where magnitude is only considered.

$$S(J(A),J(B)) \equiv \frac{1}{n}\sum_{i=1}^{n} \frac{\sum_{j=1}^{40} a_j^i(A)a_j^i(B)}{\sqrt{\sum_{j=1}^{40}\left(a_j^i(A)\right)^2 \sum_{j=1}^{40}\left(a_j^i(B)\right)^2}} \tag{4}$$

C. Face PCA Gabor Similarity

In this paper, we choose 225 points at 15×15 grid locations in 256×256 size face image (see Fig. 1) which is considered as proprietary number of feature points to represent a face image of 256×256 size.
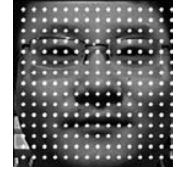

Fig. 1 Locations of Gabor feature points

Then, total Gabor wavelet coefficients extracted from a face image are $9,000(=225 \times 40)$ which may be too large for training SVM and calculating face Gabor similarity. Thus, we apply PCA to the enrolled face images, and obtain PCA modes of 95% energy. PCA modes represent variations among enrolled face images, and large variations are usually due to variations in illuminations, poses, and facial expression, and they are represented in the first and next several largest PCA modes. Thus, we discard first 5 largest PCA modes, and take the remaining PCA mode coefficients for each face image as a face PCA Gabor bunch. Then, we define the face PCA similarity between two images as a correlation between face PCA Gabor bunch in the similar way as (4).

III. PROPOSED FACE MEMBERSHIP AUTHENTICATION METHOD

A. Class Discriminating Characteristics

As explained in Section II, similarity between two images is calculated from correlation between feature vectors of two images. Feature vectors properly extracted from face images reflect a person's identity. Thus, the similarity between two face images of the same person shows tendency to be higher than the similarity between two face images of two different persons. But, since feature vectors are obviously affected by variations of illuminations, poses, facial expression and etc., similarity between two face images of different persons can be higher than that of two face images of the same person. The similarity itself alone cannot be a good class characteristic. In order to find class discriminating features, we did the following experiment and observed the experimental results.

Experimental face image set consists of enrolled face image subset and unenrolled face image subset. Then, we calculate the similarity (face PCA Gabor similarity) between a sample face with each face image in the enrolled subset, and rank all enrolled images based on the similarity between each enrolled image and the sample face image. That is, if an enrolled face

image has the largest similarity with the sample face image among enrolled face images, then the enrolled face image is ranked as the first. Likewise, one can rank all other enrolled face images.

Through the observations in the above experiment, we found the following tendencies.

1) *If the sample face is a face of the enrolled person, many highly ranked face images come from the same person as the person of the sample face image. Thus, the count of the face images of the same person among the highly ranked face images can be a good characteristic which can discriminate between enrolled class and unenrolled class distinctively.*

2) *In the case that the person of the sample face image is an enrolled person, the difference between the similarity of the 1st ranked face image and that of the highest ranked face image among enrolled face images of different persons from the person of the 1st ranked face image is larger than that in the other case.*

3) *The similarity of the first ranked enrolled face image is higher if the person of the sample face image is an enrolled person than if not.*

Thus, we find that the following 3 characteristics can be a good class discriminating features:

① the count of the face images of the same person among the first 5 highest ranked enrolled face images about the sample (incoming) face

② The difference between the similarity of the 1st ranked enrolled face image and that of the highest ranked face image among enrolled face images of different persons

③ The similarity of the first ranked enrolled face image

B. Calculation of SVM Training Data

Train set consists of two parts: membership face image set and non membership face image set. All train set images are normalized. Normalization includes geometric normalization and illumination normalization. In geometric normalization process, size of face image is normalized into 256×256 size, eyes' coordinates are set to a fixed position and pose of face is rendered upright. Illumination normalization is done using anisotropic smoothing method [16]. For all normalized training face image, Gabor feature vectors are extracted at 225 image points located at the grid as shown in the Fig. 1.

Now, we obtain a face PCA Gabor bunch for each training image. Then, for each sample image from the training set, we calculate the face PCA Gabor similarity between the sample image and each face image in the membership set. Next, for each sample image, one computes the above three class characteristics. Since similarity between two same images is trivially perfect, it is not included in computing the three class characteristics. If the sample face image comes from membership set, the three class characteristics are used for a positive training data, and if not, they are used for a negative

training data.

C. Authentication Decision

In authentication process, we calculate three characteristics for a new incoming normalized face image and passes them into the trained SVM. If the result is positive, then we decide the person of the incoming image belongs to a membership set. If not, we decide that the person as a nonmember.

IV. EXPERIMENTS

A. Experiment Environments

In order to evaluate our proposed algorithm, we constructed two domestic face databases and used them in our experiments, one for training and one for authentication testing.

The training domestic face database consists of 415 images of 83 persons with 5 pose directions (-45°, -22.5°, 0°, +22.5°, +45°) under different illuminations. Each image is JPEG with a resolution of 640×480. Some face images of the training domestic face database are shown in Fig. 2.

Fig. 2 Some face images of the training domestic face database

The testing domestic face database consists of 837 images of 75 persons with no restriction on illumination, pose, and facial expression. 53 of 75 persons overlap with the persons of the training face database, and the other 22 persons are totally new. Each image is JPEG with a resolution of 640×480. Some face images of the testing domestic face database are shown in Fig. 3.

Fig. 3 Some face images of the testing domestic face database

B. Experiment Results

We carried out two experiments. In the first experiment, in order to compare the proposed face membership authentication method with the threshold rule-based one and the conventional

direct SVM-based one, we calculated FRR(Fault Rejection Ratio) and FAR(Fault Acceptance Ratio).

In the first experiment, the configuration of training image set and testing image set is as follows.

TABLE I
CONFIGURATION OF TRAINING SET AND TESTING SET

		Enrolled persons' images	Unenrolled persons' images
Training set		200 (40 persons)	215 (43 persons)
Testing set	Type A	223 (23 persons)	235 (30 persons)
	Type B		369 (22 persons)

All training images come from training face database, and all testing images comes from testing face database. Unenrolled persons's images in Type A testing set consist of 235 face images of 30 persons which overlap with 43 unenrolled but trained persons while unenrolled persons' images in Type B testing set consist of 369 face images of 22 persons who are new persons not trained before. Unenrolled persons' images in Type B testing set are prepared for testing untrained and unenrolled persons.

Threshold-based face membership authentication method computes the similarity between the incoming testing image and each enrolled image, and checks whether the first rank's similarity exceeds the given threshold. The threshold is determined so as to satisfy FAR=0.85% for Type A testing set. The conventional direct SVM-based method trains SVM using face PCA Gabor bunches with FAR=0.85% for Type A testing set. The proposed method trains SVM using three class characteristics with FAR=0.85% for Type A testing set. Table II shows the results of the first experiment.

TABLE II
THE RESULT OF THE FIRST EXPERIMENT

Methods	Test set	Error rate (%)
Direct SVM	Type A	FRR 8.97, FAR 0.85
	Type B	FRR 8.97, FAR 41.73
Threshold	Type A	FRR 14.35, FAR 0.85
	Type B	FRR 14.35 , FAR 1.63
Proposed	Type A	FRR 6.73, FAR 0.85
	Type B	FRR 6.73, FAR 2.71

The results of the first experiment in Table II shows that the proposed face membership authentication method performs better than the other previous methods, especially for unenrolled face images which are used in training SVM. These results also show that the SVM used in the proposed method is less affected by change in the trained non membership class members.

In the second experiment, in order to investigate the effects of changes in membership configuration caused by join or drop on the proposed method, we tested the cases where the members is increasing or decreasing from the enrolled membership class used in the first experiment. In each case, the same SVM as the one in the first experiment is used.

Table III shows the results of the second experiment.

Types C, D, E, and F test set consist of different FRR test set and FAR test set, respectively.

TABLE III
THE RESULT OF THE SECOND EXPERIMENT

Enrolled persons' images	Test set	Error rate (%)
200 (40 persons)	Type A	FRR 6.73, FAR 0.85
	Type B	FRR 6.73, FAR 2.71
250 (50 persons)	Type C	FRR 6.84, FAR 1.03
	Type D	FRR 6.84 , FAR 2.17
150 (30 persons)	Type E	FRR 4.12, FAR 1.89
	Type F	FRR 4.12, FAR 3.25

FRR sets of Types C and D are composed of 263 face images of 29 enrolled persons in the testing face database, and FAR set of Types C is composed of 195 face images of 24 unenrolled persons in the testing face database. And, FRR sets of Types E and F are composed of 194 face images of 18 enrolled persons in the testing face database, and FAR set of Types E is composed of 264 face images of 35 unenrolled persons in the testing face database. FAR sets of Type D and F are the same as the set of the unenrolled persons' images in Type B testing set.

Experimental data in Table III shows that the performance of the proposed face membership authentication method is relatively stable for different membership classes so that the proposed method is robust to the change in membership configuration.

V. CONCLUSION

In this paper, we proposed a new face membership authentication method. The proposed method decides whether the person of the incoming face image is a member or not based on the SVM binary classifier using class characteristics. As opposed to the previous SVM which are usually trained using image feature vectors like pixel intensity, eigenfaces, Fisher faces, Haar like feature vectors, and Gabor feature vectors, the SVM adopted in the proposed method is trained using class characteristics which can discriminate member class from nonmember class distinctively.

Image feature vectors are affected by variations in illumination, poses, and facial expression so that the SVM trained by these image feature vectors is affected by such variations. Also, since the such trained SVM by the image feature vectors of training set images reflects the statistics of training member class images and nonmember class images, the SVM may not classify properly the incoming face image whose image features are somewhat deviated from the image features' statistics of the training images. Moreover, such SVM can be affected by changes in membership configuration caused by member joining or secession.

However, the SVM trained using class characteristics proposed in this paper reflects distinctive characteristics discriminating between member class and nonmember class so that it is robust to variations in illuminations, poses, and facial expression of individual images, and much less affected by

changes in membership configuration.

Through experiments, it was shown that the proposed face membership authentication method performs better compared to the previous threshold-based methods and the conventional SVM-based methods, and is much less affected by changes in membership.

REFERENCES

[1] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp, 2021-2040, Dec 2003.

[2] W. Zhao, R. Chellappa, J. Phillips, and A. Rosenfeld, "Face Recognition: A Literature Survey," ACM Computing Surveys, pp. 399-458, 2003.

[3] S.Z. Li and A. K. Jain, Handbook of Face Recognition, Springer, 2004

[4] Y. Adini, Y. Moses, and S. Ullman, "Face Recognition: The problem of compensating for changes in illumination direction," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 19, no. 7, pp. 721-732, July 1997.

[5] C. J. Burges, "A tutorial on Support Vector Machines for Pattern Recognition," Data *Mining and Knowledge discovery*, 2, pp.121-167, 1998.

[6] C. Cortes, and V. Vapnik, "Support vector network," *Machine Learning 20*, pp. 273–297, 1995.

[7] P.J. Phillips, "Support vector machines applied to face recognition," Adv. *Neural Inform. Process. Syst*. 11, pp. 803–809, 1998.

[8] G. Guo, S. Z. Li, and K. Chan, Face Recognition by Support Vector Machines," *4th IEEE Int'l Conf. on Automatic Face and Gesture Recognition*, pp. 196-201, 2000.

[9] S. Pang, D. Kim, S. Y. Bang, "Membership authentication in the dynamic group by face classification using SVM ensemble," *Pattern Recognition Letters*, vol. 24, no 1-3, Jan. 2003.

[10] S. Pang, D. Kim, S. Y. Bang, "Face membership authentication using SVM classification tree generated by membership-based LLE data partition," *Neural Networks, IEEE Transactions on*, vol. 16, no. 2, pp. 436-446, March 2005.

[11] Q. Liu, W. Yan, H. Lu and S. Ma, "Occlusion Robust Face Recognition with Dynamic Similarity Features," *18th IEEE Int'l Conf. Pattern Recognition (ICPR'06)*, 2006.

[12] C. Chang and C. Lin, "LIBSVM: a Library for Support Vector Machines," http://www.csie.ntu.edu.tw/~cjlin/libsvm

[13] B. E. Boser, I. Guyon, and V. Vapnik, "A training algorithm for optimal margin classifiers," *Proc. 5th Annual Workshop on Computational Learning Theory*, pp. 144-152, ACM Press, 1992.

[14] J. Zou, Q. Ji, G. Nagy, "A Comparative Study of Local Matching Approach for Face Recognition," *IEEE Trans. Image Processing*, vol. 16, No. 10, October, 2007.

[15] L. Wiskott, J. M. Fellous, N. Kuiger, and C. von der Malsburg, "Face Recognition by Elastic Bunch Graph Matching," *Pattern Analysis and Machine Intelligence*, IEEE Transactions, vol. 19, pp. 775-779, July 1997.

[16] R. Gross and V. Brajovic, "An image preprocessing algorithm for illumination invariant face recognition," *In Audio- and Video-Based Biometric Person Authentication*, vol. 2688, pp. 10-18, June, 2003.