Abstract

This paper presents a novel method to authenticate an individual’s membership in a group without revealing the individual’s identity and without restricting how the member of the group may be changed. It has the ability to authenticate membership and is robust to cope with the variations of both the group size and the group member of membership.

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, members need not be distinguished from one another. Most existing research that authenticates membership in a group do so by identifying an individual[1-3], 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 unwieldy: whenever individuals are added or changed in the group, existing system performance will fluctuate with the variation of membership in the group.

This paper focuses on the problem of face authentication of membership in dynamic groups, in which we achieve general membership recognition by dynamic face authentication. This new method enable us to extend the face authentication to dynamic groups in which not only a trusted part may add and remove members of the group, but the whole group can be varied as well.

2 Membership Authentication

Membership authentication is to distinguish a certain group of face images, which are membership faces, from the remaining non-membership face images. The problem can be equal to a binary classification, to differentiate between a member and a non-member. The differences are that both the size and the member of group are dynamically changeable, and the size of membership group usually is smaller than the size of non-membership group.

Fig.1 is the illustration of a dynamic membership group. Where the membership group \( G \) is a subgroup of the universal human group \( I \), and its complemental set \( I - G \) is the non-membership group. The dashed line circles in Fig. 1 identify other membership group examples, which indicate that either the size or the member of the membership group is changeable. The membership authentication problem can be depicted as: Given a certain human group \( I \) with \( N \) members, which is the universal people set. If there exists a arbitrary subgroup \( G = \{g_i\}_{i=1}^k \) such that \( G \subset I \) and \( |G| < N/2 \), then it is membership group, and the nonmember group is \( I - G \). Thus the membership authentication problem can be depicted by Eq.(1), which is a typical binary classification problem.

\[
f(x) = \begin{cases} 
1 & \text{if } x \in G \\
-1 & \text{otherwise}
\end{cases}
\]
A direct solution of Eq.(1) is to identify each input face as one of the individual members in the group as Eq.(2).

\[
f(x) = \begin{cases} 
1 & \text{if } x = x_j, x_j \in G, j \in \{1, |G|\} \\
-1 & \text{otherwise}
\end{cases}
\] (2)

Our solution is Eq.(3), where membership and non-membership are used as a form of feature fusion, then either specific members or nonmembers can be regarded as one of the individual members in the group as face fusing, LDA feature scattering, and SVM ensemble classification. Individual steps are detailed in the subsections below and shown schematically in Fig. 2.

\[
\begin{align*}
G & = \text{Gabor feature extraction, PCA membership} \\
& \text{face fusing, LDA feature scattering, and SVM ensemble} \\
& \text{classification.}
\end{align*}
\]

Individual steps are detailed in the subsections below and shown schematically in Fig. 2.

\[
\begin{align*}
\text{Data Set} & \rightarrow \text{Gabor + PCA + LDA} \\
& \rightarrow \text{Membership} \\
& \rightarrow \text{Non-Membership} \\
& \rightarrow \text{SVM} \\
& \rightarrow \text{SVM Ensemble} \\
& \rightarrow \text{Membership} \\
& \rightarrow \text{Non-Membership}
\end{align*}
\]

\text{Figure 2. Membership authentication algorithm}

3 Valid Facial Feature Processing for Classification

3.1 Gabor Wavelet Feature

Gabor wavelet feature has been widely used both in face recognition and fingerprint authentication[3]. A 2D Gabor function is a Gaussian modulated by sinusoidal. It is a nonorthogonal wavelet, and can be specified by the frequency of the sinusoid 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 \( \times \) 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 Fusing by PCA

Theoretically, all the group member faces can be abstractly fused to one face, which is equal to “membership face,” which can be thought of as a set of eigenfaces together characterized the variation of between all the group member face images. The computation of eigenface is based on principal component analysis (PCA)[2], which finds the optimal basis for representation of the training face space 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 set is defined by \( \bar{\phi} = \frac{1}{M} \sum_{n=1}^{M} I_n \). Each face differs from the average by the vector \( \phi_n = I_n - \bar{\phi} \). The set of very large vectors is then subject to principal component analysis to identify a set of \( M \) orthonormal vectors \( u_n \) and their associated eigenvalues, which best describes the distribution of the data. The vectors \( u_n \) are the eigenvectors of the covariance matrix:

\[
Q = \frac{1}{M} \sum_{n=1}^{M} \phi_n \phi_n^T = AA^T
\] (7)

By[5], \( u_i \) can be computed as:

\[
u_i = \sum_{k=1}^{M} \nu_{ik} \phi_k
\] (8)

Where \( \nu_{ik} \) are the eigenvectors of the matrix \( A_i A_i^T, i = 1, 2, \ldots, M \). Then the eigenfaces are then chosen as the \( M' \) vectors \( u_{k}, k = 1, 2, \ldots, M' \) that correspond to the largest \( M' \) eigenvalues of the matrix \( A_i A_i^T \). Fig. 3 is the illustration of membership face with \( M' = 10 \). Consequently, a new input face image can
be transformed into its eigenface components by operation $w_k = u_k^T(T - \varphi)$, where $k = 1, 2, ..., M'$ and the weights form a feature vector $F = [w_1, w_2, ..., w_{M'}]$ that describes the contribution of each eigenface in representing the input image.

3.3 Feature scattering by LDA

In the above fused feature space, to reduce the classification difficulty, we also used linear discriminant analysis (LDA)\[5\]. LDA seeks a single projection that can optimally separate the two labelled clusters in the distribution space, and gives them a minimum within-cluster distance and a maximum between-cluster distance. Thus the ratio of the between class scatter to the within class scatter, $J(w)$ is maximized.

$$J(w) = \frac{w^T S_B w}{w^T S_w w}$$  \hspace{1cm} (9)

Where,

$$S_w = \sum_{i=-1}^{1} \sum_{x \in F_i} (x - m_t)(x - m_t)^T$$ \hspace{1cm} (10)

$$S_B = (m_1 - m_2)(m_1 - m_2)^T$$ \hspace{1cm} (11)

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

$$\frac{\partial J(w)}{\partial w} = 0$$ \hspace{1cm} (12)

4 Membership Authentication by SVM Ensembles

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 a type of cross-validation optimization of single SVM, and should have a more stable classification performance than other models, which we proved in [4].

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. In addition, another strategy is the majority-voting rule that chooses the classification made by more than the 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

$$C^n_k p^k (1 - p)^{N-k}$$ \hspace{1cm} (13)

Thus, the possibility of the majority scheme will be given as below,

$$\sum_{k>N/2}^N C^n_k p^k (1 - p)^{N-k}$$ \hspace{1cm} (14)

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

Based on the modeling of face authentication of membership in Section 3, 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 is to seek the best answer from all the SVM judgments. This will keep the classification performance of the system more stable. Therefore, we deal with classification as a two-layer SVM ensemble. The first layer SVMs are for membership and non-membership SVM modeling, and the second layer is a decision support mechanism (DSM) based on the plurality strategy.

5 Experiment

We have implemented the proposed membership authentication technique on the Matlab platform. In our experiments, 1,355 face images of 271 persons (5 face images per person) are taken. Each image has the size of 56 x 46. First, 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 don’t need to remove the hair information. But for a robust face membership authentication system, face images are usually cropped to keep only the main facial regions, since the hairstyle can change in appearance easily, which will inevitably affect the result of our face authentication. To construct the membership group, and divide the training and test data set. We randomly select a certain number of persons equal to the group size of member among 271 persons for the group member. The remaining persons are considered as the non-group member. The percentage of the group members over total persons can be changed freely within a 40% range.

Next, we perform Gabor feature extraction, valid facial feature processing for classification, and SVM ensembles with polynomial kernel [5], which we discussed in above sections respectively, then test the algorithm with 5 different sizes of membership group. For the case of each membership group size, we carry out 10 times test with different group member. The average
performance of our system simulation are listed in Table 1.

As we have seen in this table, the proposed dynamic membership authentication method provides us with a very good performance on non-membership authentication: The average false-positive error is 0.003. In fact, such a near zero non-membership misclassification rate is very important for a security system, because it is dangerous to take people without membership. On the other hand, it seems that the results of membership authentication of the system are not good as the best expectation. For some small group-size cases such as 5 members and 10 member cases, the authentication error rate approaches half percent. But we can regard it as reasonable, because for small group sizes, 5 pictures for each member are not enough for the valid training of each SVM. Fortunately, as shown in Table 1, with the increase of the group size, the membership authentication error is dropping down.

Table 1. The experimental results of membership authentication

<table>
<thead>
<tr>
<th>Size</th>
<th>Ratio</th>
<th>M. error/Nm</th>
<th>NM error/Nnm</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>98.56%</td>
<td>5/10</td>
<td>1/430</td>
</tr>
<tr>
<td>10</td>
<td>97.98%</td>
<td>8/20</td>
<td>0/424</td>
</tr>
<tr>
<td>20</td>
<td>98.23%</td>
<td>8/40</td>
<td>0/419</td>
</tr>
<tr>
<td>30</td>
<td>98.87%</td>
<td>5/60</td>
<td>0/410</td>
</tr>
<tr>
<td>40</td>
<td>96.93%</td>
<td>14/100</td>
<td>2/383</td>
</tr>
</tbody>
</table>

In order to test the algorithm stability under the variation of the members in a specific group size, we randomly select 10 different groups, in which each group consists of five different persons. We applied the proposed authentication method to each group independently. The correct authentication rate is almost constant in the range of from 97% to 98.5%. 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 ranged from 5 to 95 persons with the step size of 5 persons, and represent the trend of correct authentication rate using B-spline interpolation. Fig. 4 shows the authentication performance. From the figure, we note that the proposed authentication method has a good ability to recognize non-membership, and that membership authentication entails a majority part of the misclassification.

6 Conclusion

In this paper, we proposed a dynamic membership authentication method. Unlike other face recognition works, the proposed method can authenticate membership without recognizing the individual identities of face images. The problem with the method is that the correct classification rate for membership is highly degraded when the size of members is small (less than 20), due to the limited training data set. Nevertheless, the simulation results show that the authentication performance of our method can keep stable for the member group with a size of less than 45 persons. It is also very robust to variation of the members in the membership group.

References


