Constructing SVM Multiple Tree for Face Membership Authentication

Shaoning Pang

Knowledge Engineering & Discover Research Institute
Auckland University of Technology
Private Bag 92006, Auckland 1020, New Zealand
snpang@aut.ac.nz

Abstract. In membership authentication problem that has a complicated and mixed data distribution, the authentication accuracy obtained from using one classifier is not sufficient despite its powerful classification ability. To overcome this limitation, an support vector machine (SVM) multiple tree is developed in this paper according to a "divide and conquer" strategy. It is demonstrated that the proposed method shows a good membership authentication performance, as well as the strong robustness to the variations of group membership, as compared with the SVM ensemble method [1]. Specifically, the proposed method shows a better improvement in authentication performance as the group size increases larger.

1 Introduction

Membership authentication problem can be depicted as follows, consider a certain human group G with N members, which is the universal set. If there exists an arbitrary subgroup M such that $M \subset G$ and $|M| < N/2$, then it is a membership group, and the remaining people $\overline{M} = G - M$ is a non-membership group. Thus, membership authentication problem is to distinguish the membership class M from the non-membership class $\overline{M}$ in the human group.

Unlike most works on face recognition that tried to identify the identity of the given face image, I proposed a concept of dynamic membership authentication [1] that attempts to authenticate an individual's membership without revealing the individual's identity and without restricting the group size and/or the members of the group, implemented the concept using an SVM ensemble method.

One problem of SVM ensemble method is that the correct classification rate for the membership is not good as to be expected, as the size of membership group is bigger than 45 (16.6% percentage of total group). This is due to a complicated mixed data distribution among the membership and non-membership face images, as it is very difficult to discriminate such complicated mixed data in terms of only one classifier even its classification performance is powerful.

To solve this problem, a new membership authentication method of SVM multiple tree is developed in terms of a "divide and conquer" strategy, where

D. Zhang and A.K. Jain (Eds.): ICBA 2004, LNCS 3072, pp. 37–43, 2004.
© Springer-Verlag Berlin Heidelberg 2004

the whole data is divided into several subgroups by an iterative membership-based data splitting and authenticate the membership in each subspace by SVM classification. Consequently, a considerable improvement is obtained in robustness to the size changes in the membership group.

2 SVM Multiple Tree

The SVM multiple tree is constructed by a divide and conquer approach. Mathematically, the proposed membership authentication method can be formulated as follows.

$$F(\mathbf{x}) = \begin{cases} 1 \quad if \ f_{g_i}(x) = 1, \mathbf{x} \in g_i \ i = 1..L \\ -1 \ if \ f_{g_i}(x) = -1, \mathbf{x} \in \bar{g}_i \end{cases} \tag{1}$$

where the total group (G) is divided into subgroups $\{g_1, g_2, \cdots, g_L\}$, and each subgroup g_i belongs to membership class or nonmembership class. f_{g_i} is a subgroup membership classifier working on g_i. Hence, the whole membership authentication system $F(\mathbf{x})$ consists of numbers of subgroup membership classifiers, each input face $\mathbf{x}$ is first judged to be the member of a certain subgroup, then the class of $\mathbf{x}$ is determined by the label of this subgroup.

2.1 Tree Growing

Similar to decision tree, the glowing of SVM tree is determined by a succession of splits that partition the training data into disjoint subsets. Starting from the root node that contains all training data, a membership-based PCA data splitting is performed to partition the data into numbers of disjoint subsets. These subsets are represented by the same number of child nodes originating from the root nodes, and the same splitting method is applied to each child node. This recursive procedure terminates when the subdivided clusters have only either membership or nonmembership training data.

Basically, two procedures are performed at each node in the above tree generation. First, the membership-based data splitting performs a 'soft' separation of membership because it splits the data into disjoint subsets. Next, a multiclass SVM classifier is trained by the result of 'soft' classification and can be thought of as performing 'hard' decision of membership. Consequently, with the continuing of data splitting, a subspace hierarchy is built up, and a SVM multiple tree is constructed thereafter, where each terminal node of the tree is associated with a label of membership or nonmembership. Algorithm 1 shows the procedure of constructing the SVM multiple tree that includes the membership-based clustering.

Therefore, for an input face, its membership can be predicted in the above SVM decision tree. First, a new data $\mathbf{x}$ is feed to root node SVM tester $T_1(\mathbf{x})$ in the SVM tree. Depending the result of a decision made by an internal node SVM test $T_i(\mathbf{x})$, the tree will branch to one of the node's children. This procedure is repeated until a terminal node is reached and a membership label is then assigned to the given input face. This procedure is depicted as Algorithm 2.

Algorithm 1: SVM multiple tree construction.
Function SVMTree_Build (A training set X) {
 if (X contains the same membership) {
  Mark the end of a branch in SVM tree T;
  return;}
 Multiple_Membership-based_Splitting(X;$X_1, ..., X_q$);
  /*Divide X into disjoint subsets $X_1, ..., X_q$ */
 Append_node(T_i);
 Train_SVM_Classifier(X);
 for($j = 1; j < q; j++$) {SVMTree_Build(X_j);}
}

Algorithm 2: Authentication by SVM multiple tree.
Function SVMTree_Test (SVM multiple tree T, Input face $\mathbf{x}$) {
 current=1; /* set current node is root of T */
 while ($T_{current}$ is an inside node) {
   SVM_Test_$T_{current}(\mathbf{x})$;
   next = Search_next_node($T_{current}$);
   current = next;
  /* set next node as current node*/
   }
 return $T_{current}(\mathbf{x})$;
}

2.2 Data Splitting

In PCA, membership can be represented as a set of eigenfaces together characterized the variation of between all the group member face images. So are the non-group member faces. Thus the training set can be partitioned by a data splitting procedure with the membership eigenfaces and nonmembership eigenfaces as reference centers.

The computation of the eigenface is based on principal component analysis, which finds the optimal basis for representation of the training data space in the mean squared error sense[2]. Let the training set $I = \{\mathbf{x}_1, x_2, x_3, ..., x_M\}$ of N-dimensional face feature vectors. The mean, μ, and the covariance matrix,$\mathbf{\Sigma}$, of the data are given by:

$$\mu = \frac{1}{M}\sum_{m=1}^{M}\mathbf{x}_m \tag{2}$$

$$\mathbf{\Sigma} = \frac{1}{M}\sum_{m=1}^{M}[\mathbf{x}_m - \mu][\mathbf{x}_m - \mu]^T = \mathbf{U}\mathbf{U}^T. \tag{3}$$

Where $\mathbf{\Sigma}$ is an $N \times N$ symmetric matrix. This matrix characterizes the scatter of the data set. A none-zero vector $\mathbf{u}_k$ for which

$$\mathbf{\Sigma}\mathbf{u}_k = \lambda_k\mathbf{u}_k \tag{4}$$

is a principal component of the face feature space from I. This is often referred as eigenface[2]. Its weight is λ_k, which represents the contribution of this component in the original space. If $\lambda_1, \lambda_2, ..., \lambda_K$ are the K largest weight, then $\mathbf{U} = [\mathbf{u}_1 \mathbf{u}_2 ... \mathbf{u}_k]$ are the representative eigenfaces of data set I.

In membership authentication, the group members can be divided into membership and non-membership group members as $G = M \cup \bar{M}$. Applying the above eigenface technique Eq. (2) - Eq. (4) to M and $\bar{M}$ respectively, two representative eigenface sets are obtained as the membership eignefaces $\mathbf{U}_M = [\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_K]$ and the non-membership eigenfaces $\mathbf{U}_{\bar{M}} = [\bar{\mathbf{u}}_1, \bar{\mathbf{u}}_2, \cdots, \bar{\mathbf{u}}_L]$. They characterize the "membership-face" and "nonmembership-face" respectively.

For splitting the data following above steps, lets identify the two partitioned groups as an $c \times n$ binary matrix $\mathbf{V}$, where the element v_{ij} is 1 if the jth data point $\mathbf{x}_j$ belongs to group i, otherwise 0. Once cluster centers $\mathbf{U}_M$ and $\mathbf{U}_{\bar{M}}$ are fixed, then the data splitting based on membership can be performed as follows:

$$v_{ij} = \begin{cases} 1 \; if \; Min_{i=1}^{K} \mathbf{x} \cdot \mathbf{u}_i \leq Min_{j=1}^{L} \mathbf{x} \cdot \bar{\mathbf{u}}_j \\ 0 \; otherwise \end{cases} \tag{5}$$

Where $\mathbf{x} \cdot \mathbf{u}_i$ is the distance projected onto the membership eigenfaces ($\mathbf{U}_M$), and $\mathbf{x} \cdot \bar{\mathbf{u}}_j$ is the distance projected onto the non-membership eigenfaces ($\mathbf{U}_{\bar{M}}$). Thus, with the growing of the splitting, members and non-members are always driven into a separated subspace. Until arrive the terminal node, member and non-member can be clearly distinguished and clustered in many subgroups.

2.3 Multiclass SVM Classification

Support vector machine is a new and promising classification and regression technique proposed by Vapnik and his group at AT&T Bell laboratories[3]. For the multi-class classification, SVM can be extended in the following two ways. One method is called the "one-against-all" method, where we have as many SVMs as the number of classes. The ith SVM is trained from the training samples, where some examples contained in the ith class have "+1" labels, and other examples contained in the other classes have "-1" labels. Then, the decision function is

$$f(\boldsymbol{x}) = sign(\underset{j \in 1,2,\ldots,C}{Max}((\boldsymbol{w}^j)^T \cdot \varphi(\boldsymbol{x}_j) + b_j)), \tag{6}$$

where C is the number of the classes. Another method is called the one-against-one method[15]. When the number of classes is C, this method constructs $\frac{C(C-1)}{2}$ SVM classifiers. The ijth SVM is trained from the training samples where some examples contained in the ith class have "+1" labels and other examples contained in the jth class have "-1" labels. The class decision in this type of multiclass classifier can be performed in the following two ways. The first decision is based on the "Max Wins" voting strategy, in which $\frac{C(C-1)}{2}$ binary SVM classifiers will vote for each class, and the winner class is the class with the maximum number of votes. The second method uses the tournament match, which reduces the classification time to a log scale.

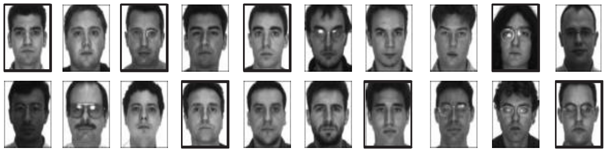

Fig. 1. Examples of face dataset for membership authentication

3 Experiments and Discussions

3.1 SVM Multiple Tree Construction

The proposed membership authentication technique has been implemented on the same face dataset as in [1]. For the construction of membership face group which are divided into a training and test set, a certain number of persons equal to the membership group are selected among 271 persons as group members, and the remaining persons are non-members. Particularly, to ensure the membership group meaningful, the size of membership group size is set to be less than the size of non-membership group, and the percentage of the group member over total persons to be within 40%. Fig. 1 are some examples of our face dataset for membership authentication, where persons in frame are assigned as member, and the remaining persons are nonmembers.

Algorithm 1 is applied to construct the SVM multiple tree for membership authentication. Fig. 2 illustrates a SVM-classification multiple tree for 10 member membership authentication that was implemented in the experiment. Each internal node of the tree identifies a multi-class SVM classifier, which is represented as as an ellipse with a label of a_b, where a is level of the node in the tree, and b is the number of brother node in the same level. The terminal node is represented as a circle or a filled circle, which denotes the class, membership or non-membership, respectively.

3.2 Comparison Experiments

The proposed method has been compared with the face recognition method and the SVM ensemble method on the membership authentication of two big group-size membership datasets, whose group sizes are 50 and 60 respectively, which are greater than the limitation of SVM ensemble method. The used face-identification method is embedded HMM with the 2nd-order block-specfic eigenvectors[4], which was reported, had the best recognition performance on the above face database. The SVM ensemble method is the previous work on dynamic membership authentication[1]. Table 1 shows the contrast statistical results, where SVM ensemble method is denoted as Proposed method I, and the proposed multiple SVM classification tree method as Proposed method II. Note that in Table 1, the proposed SVM classification tree provides a good ability of membership recognition, as well as a good system stability on these two

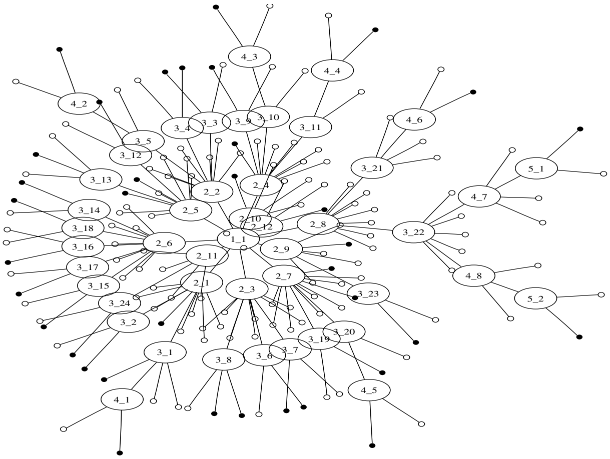

Fig. 2. An SVM multiple tree for 10 member membership authentication

Table 1. The comparison result of authentication error between two different authentication methods

	Proposed method I		Proposed method II		Identification-based method
Group Size	50	60	50	60	
Ex1(que:1,reg:2,3,4,5)	4.1%	5.8%	3.4%	3.7%	0.6%
Ex2(que:2,reg:1,3,4,5)	2.8%	11.5%	4.1%	4.8%	2.9%
Ex3(que:3,reg:1,2,4,5)	9.2%	3.7%	3.7%	4.1%	0.6%
Ex4(que:4,reg:1,2,3,5)	3.1%	13.3%	4.1%	4.8%	5.0%
Ex5(que:5,reg:1,2,3,4)	10.5%	23.7%	3.7%	4.1%	18.0%
Average	5.9%	11.6%	3.8%	4.3%	5.4%
Variance	130.0e-005	610.0e-005	0.9e-005	2.4e-005	530.0e-005

big group-size membership datasets. while the performance of SVM ensemble come to deteriorate. The correct rate becomes junior to face identification-based method, and the variance also jumps to the same grade as face identification method.

3.3 Stability Test

In the stability test of the proposed authentication method under the condition of different membership group sizes. The proposed authentication method is compared with the SVM ensemble method with different membership group sizes ranging from 5 to 95 persons with a step size of 5 persons. Fig. 3 shows the comparison result of the number of mis-authentications between two authentication methods, where two pieces of curve illustrate the stability of the

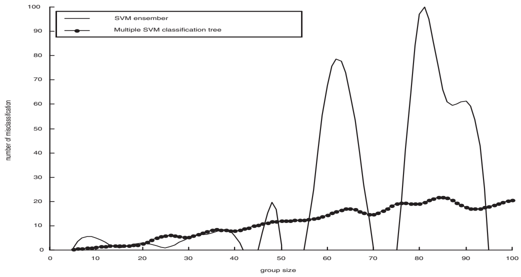

Fig. 3. Stability test under different group size

two methods under different membership group size, respectively. As can be seen, the proposed authentication method shows a good stability because it still shows a small number of mis-authentication as the membership group size grows greater than 45, and its curve fluctuates very slightly and smoothly. While the SVM ensemble-based method loses such stability, some mutation appears in the latter half part of its curve, which implies that the performance of system is out of control. It is evident that the proposed membership authentication method has a much better salability under the change of membership group size than the SVM ensemble method.

4 Conclusions

This paper presents a new membership authentication method by face classification using SVM multiple tree, in which the size of membership group and the members in the membership group can be changed dynamically. The experimental results show that the proposed SVM classification tree-based method not only keeps the good properties that the SVM ensemble method has, such as a good authentication accuracy and the robustness to the change of members, but also has a considerable improvement on the stability under the change of membership group size.

References

[1] S. N. Pang, D. Kim, and S. Y. Bang, “Membership authentication in the dynamic group by face classification using SVM ensemble,” Pattern Recognition Letters, Vol. 24, pp. 215-225, 2003. 37, 41

[2] Pentland, A., Turk,M. (1999) Eigenfaces for Recognition Journal of Cognitive Neuroscience, 3(1):71-86. 39, 40

[3] V. Vapnik. Estimation of dependences based on empirical data. Springer-Verlag, 1982. 40

[4] Min-Sub Kim, Daijin Kim, Sung Yang Bang, Sang-Youn Lee, Young-Sik Choi(2002) Face Recognition Descriptor Using the Embedded HMM with the 2nd-order Block-specific Eigenvectors ISO/IEC JTC1/SC21/WG11/M7997, Jeju, March 2002. 41