Binary Discriminant Analysis for Face Template Protection

Yicheng Feng

Abstract

Biometric cryptosystem (BC) is a very secure approach for template protection because the stored template is encrypted. The key issues in BC approach include (i) limited capability in handling intra-class variations and (ii) binary input is required. To overcome these problems, this paper adopts the concept of discriminative analysis and develops a new binary discriminant analysis (BDA) method to convert a real-valued template to a binary template. Experimental results on CMU-PIE and FRGC face databases show that the proposed BDA method outperforms existing template binarization schemes.

1 Introduction

Biometrics is a reliable, robust and convenient way for person authentication [5, 3]. With the growing use of biometrics, there is a rising concern about the security and privacy of the stored biometric templates. Biometric cryptosystem [4] is a very secure approach for template protection because the output is encrypted, but suffers from two major limitations. First, this approach requires binary input while most of the templates are real-valued. Therefore, a template binarization step is required. Second, the capability for handling the intra-class variations is limited. In turn, the recognition accuracy may not be satisfied.

To fulfill the binary input requirement, some binarization schemes [8, 9, 10, 11, 12, 13, 14, 15] have been proposed in the last few years. We roughly categorize these schemes into two approaches, namely local and global. Local binarization methods consider each component x_r of the input real-valued template $\mathbf{x} = (x_1, x_2 \dots x_l)$ (feature vector) independently. For each x_r, a function f_r is applied to extract a bit b_r (or maybe several bits) from x_r ($b_r = f_r(x_r)$). The advantages of local approach are simple and low complexity but, it will distort the original data distribution. In turn, the system performance will be degraded. Global binarization methods consider template as a whole. A series of functions $f_1, f_2 \dots f_n$ are constructed to extract bits $b_1, b_2 \dots b_n$ from template $\mathbf{x}$. That is, $b_r = f_r(\mathbf{x})$. The advantage of this approach is that the binary templates could preserve the original real-valued template data distribution and discriminability, Therefore, the recognition performance of global methods, normally, outperform local methods. However, existing methods are either designed only for authentication system [10] or fingerprint biometric [11].

To overcome the limitations on existing binarization algorithms, this paper proposes a new binary discriminant analysis method to convert a real-valued template to binary template while the discriminability is maximized. The proposed method follows the global template approach and can be used for both authentication and identification. The idea of the proposed method is inspired by the linear discriminant function (LDF) for classification process. When applying in our context, each linear discriminant function divides the biometric template space into two subspaces and each subspace is then represented by a bit (either "1" or "0") as illustrated in Figure 1(a). Therefore, when more linear discriminant functions are used, the space will be divided into a number of subspaces. Each subspace can then be represented by a binary bit string. In turn, all templates within a subspace will have the same binary representation as illustrated in Figure 2. So the problem is how to determine the "optimal" set of linear discriminative functions. Details are discussed in next section.

2 Binary Discriminant Analysis

The rationale of our binary discriminant analysis algorithm is illustrated in Figure 2. We would like to find the binarization function f from the training data with class label information. In BC approach, the bio-cryptographic algorithms, such as fuzzy commitment scheme [6] and fuzzy vault scheme [7], could only handle a small image variations. Feng $etal.$ [10] have suggested that, ideally, all real-valued templates in the same class should be mapped to the same point in binary space. In practice, it is hard to achieve and therefore, we hope that all real-valued templates should be mapped to the same point in binary space as much as possible. However, it is very hard, if not impossible, to solve the multi-class optimization problem in binary space. Instead, we propose a new idea to tentatively fix the training class data center, called ideal centroids, and BCH code [1] is employed. In doing so, the "optimal" binary function can

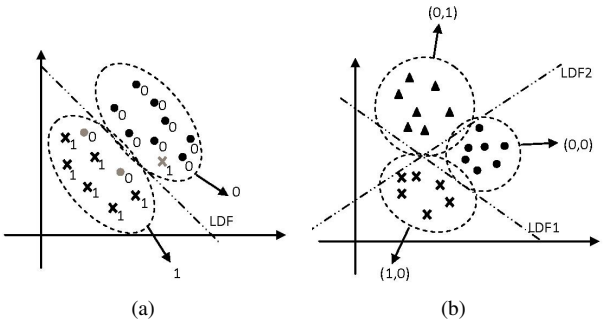

Figure 1. Linear discriminant functions for binarization. (a) Single LDF for binarization. The bits assigned to each point are the ideal labels. And the LDF labels the two subspaces to 0 and 1 respectively. (b) Multi LDF for binarization.

be determined using iterative gradient decent method.

In this section, we will first discuss how to make use of linear discriminant function for the binarization of real-valued template. After that, we will report our method in finding the "optimal" discriminant functions. Finally, we will provide the complete algorithm for the enrollment and query stages.

2.1 Linear Discriminant Function for Binarization

Assume there are c classes $\Omega_1, \Omega_2 \dots \Omega_c$ in a database. Each class Ω_i contains p training samples $\mathbf{x}_{ij}$ ($i = 1, 2 \dots c$,$j = 1, 2 \dots p$). We want to find a binarization function $f(\cdot)$, such that the between-class variance V_B is maximized and within-class variance V_W is minimized in binary space.

While the straightforward method is to find f using a multi-class optimization method, it does not work because the output is in binary space. Instead, this paper proposes to employ the linear discriminant function, which is a popular way in classification. As Figure 1(a) shows, the linear discriminant function draws a hyperplane to divide the data space into two subspaces and therefore separates the two classes. To find the optimal linear discriminant function, each sample will be labeled with a label "0" or "1" according to its class number.

For multi-class problem, obviously one discriminant function is not sufficient thus multiple discriminant functions are applied (as Figure 1(b) illustrates). Assume n discriminant functions

$$g_s(\mathbf{x}_{ij}) = (\mathbf{w}_s^{\mathbf{T}}\mathbf{x}_{ij}) + t_s \quad (s = 1, 2 \dots n)$$

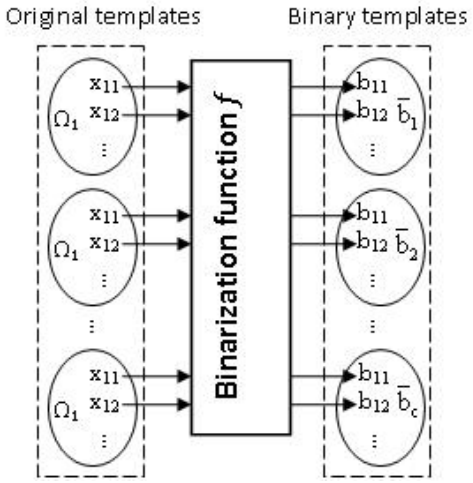

Figure 2. Rationale of the proposed algorithm.

are constructed. These functions are rewritten as the generalized form and the binarization can be written as follows:

$$b_s(\mathbf{x}_{ij}) = \begin{cases} 1 & : \quad \mathbf{u}_s^{\mathbf{T}}\mathbf{y}_{ij} > 0 \\ 0 & : \quad \mathbf{u}_s^{\mathbf{T}}\mathbf{y}_{ij} \leq 0 \end{cases} \qquad (s = 1, 2 \dots n) \quad (1)$$

where $\mathbf{u}_s^{\mathbf{T}} = [\mathbf{w}_s^{\mathbf{T}} : t_s]$ and $\mathbf{y}_{ij}^{\mathbf{T}} = [\mathbf{x}_{ij}^{\mathbf{T}} : 1]$. And

$$\mathbf{b}_{ij} = (b_1(\mathbf{x}_{ij}), b_2(\mathbf{x}_{ij}) \dots b_n(\mathbf{x}_{ij})) \quad (2)$$

Denote $\mathbf{U}$ as the matrix with columns $\mathbf{u}_s$. Next we need to construct the class centroids $\bar{\mathbf{b}}_i$ ($i = 1, 2 \dots c$), and then find binarization function f with minimized V_W.

2.2 Gradient Descent Algorithm for Multi-class Binarization

To enhance the discriminability of the extracted binary templates, the reference binary templates should have large distances between each other to gain large V_B, and this paper adopts $[n, k, d]$ BCH codes. Such codes have length n, dimension k and minimum distance d between each other. Then any codewords from the BCH codes can be chosen as class centroid $\bar{\mathbf{b}}_i$ and they have a minimum distance d. With large d, the separation between each class will be large, i.e. large between-class variance V_B.

With the class centroid, we employ the gradient descent algorithm ([16]) which has been used to find the optimal linear discriminant function for two-class problem. Here, we will extend to multiple classes.

In traditional gradient descent algorithm, the perceptron criterion function is constructed as follows

$$J(\mathbf{u}) = \sum_{\mathbf{y}_{ij} \in \Phi} |\mathbf{u}^{\mathbf{T}}\mathbf{y}_{ij}| \quad (3)$$

where Φ is the misclassified set of $\mathbf{y}_{ij}$. While it is proved that the gradient descent algorithm will converge and $J(\mathbf{u})$

will reach 0 if the two classes are well separated, in many practical applications, this may not happen. The iteration will turn over again and again when $J(\mathbf{u})$ is small. The value $J(\mathbf{u})$ and corresponding $\mathbf{u}$ are then selected as the optimal value. In multi-class problem, the criteria function is constructed as follows.

$$J(\mathbf{U}) = \sum_{\mathbf{y}_{ij} \in \Phi} \sum_{\mathbf{u}_s \in \Psi \mathbf{y}_{ij}} |\mathbf{u}_s^{\mathbf{T}} \mathbf{y}_{ij}| \tag{4}$$

where Φ indicates the misclassified set templates $\mathbf{y}_{ij}$ and $\Psi(\mathbf{y}_{ij})$ indicates the set of $\mathbf{u}_s$ which convert $\mathbf{y}_{ij}$ to bit which is different from its class centroid. Denote q as the number of iterations. Then

$$\mathbf{U}(q+1) = \mathbf{U}(q) - \eta(q) \frac{\partial J(\mathbf{U}(q))}{\partial \mathbf{U}} \tag{5}$$

From Equation (4), we have

$$\frac{\partial J(\mathbf{U})}{\partial \mathbf{U}} = \sum_{\mathbf{y}_{ij} \in \Phi} \frac{\partial \sum_{\mathbf{u}_s \in \Psi(\mathbf{y}_{ij})} |\mathbf{u}_s^{\mathbf{T}} \mathbf{y}_{ij}|}{\partial \mathbf{U}}. \tag{6}$$

Since

$$\frac{\partial |\mathbf{u}_s^{\mathbf{T}} \mathbf{y}_{ij}|}{\partial \mathbf{u}_s} = sign(\mathbf{u}_s^{\mathbf{T}} \mathbf{y}_{ij}) \mathbf{y}_{ij} \tag{7}$$

where $sign(\cdot)$ denotes the sign of the argument, therefore,

$$\frac{\partial \sum_{\mathbf{u}_s \in \Psi(\mathbf{y}_{ij})} |\mathbf{u}_s^{\mathbf{T}} \mathbf{y}_{ij}|}{\partial \mathbf{U}} = \sum_{\mathbf{u}_s \in \Psi(\mathbf{y}_{ij})} \mathbf{Y}_s. \tag{8}$$

where $\mathbf{Y}_s = [0:0:0 \ldots 0 : sign(\mathbf{u}_s^{\mathbf{T}} \mathbf{y}_{ij}) \mathbf{y}_{ij} : 0 \ldots 0]$ is the matrix with same dimension as $\mathbf{U}$, all columns except the s^{th} column are zero. Substitute Equation (8) into (6) and substitute (6) into (5), we have

$$\mathbf{U}(q+1) = \mathbf{U}(q) - \eta(q) \sum_{\mathbf{y}_{ij} \in \Phi} \sum_{\mathbf{u}_s \in \Psi(\mathbf{y}_{ij})} \mathbf{Y}_s(q) \tag{9}$$

And $\eta(q)$ is determined experimentally. Therefore, in each iteration, Equation (9) is used to update $\mathbf{U}$ and to find the optimal solution of our binarization process.

2.3 Procedure of the proposed BDA algorithm

This section summarizes the proposed binary discriminant analysis algorithm.

Enrollment:

1. Choose suitable $[n, k, d]$ BCH codes. Randomly choose c codewords from the BCH codes as reference bit templates $\bar{\mathbf{b}}_i$.
2. Randomly initialize $\mathbf{U}(1)$ and convert the original templates $\mathbf{x}_{ij}$ into bit template $\mathbf{b}_{ij}$ with Equation (1) and (2). Set iteration number $q = 1$.

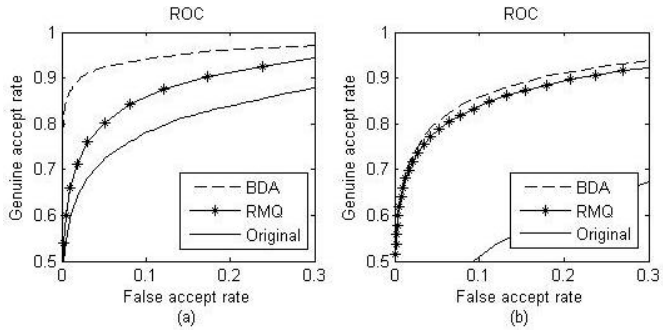

Figure 3. ROC curves for (a) CMU PIE database, (b) FRGC database.

3. While $q < q_{end}$,
   (a) Compute $J(\mathbf{U}(q))$ with Equation (4).
   (b) Do identification with $\mathbf{b}_{ij}$ as query and $\bar{\mathbf{b}}_i$ as reference. Store the misclassified binary templates to set Φ.
   (c) Update $\mathbf{U}(q)$ to $\mathbf{U}(q+1)$ with Equation (9).
   (d) Update $\mathbf{b}_{ij}$ with $\mathbf{U}(q+1)$ and $q = q + 1$.

The total iteration time q_{end} is determined experimentally. We choose the $\mathbf{U}(q)$ with minimum $J(\mathbf{U}(q))$ in the last few steps as the optimal U.

Query:

1. A query template $\mathbf{x}'_{i'j'}$ is presented to the system.
2. Generate a binary template $\mathbf{b}'_{i'j'}$ from $\mathbf{x}'_{i'j'}$ with Equation (1) and (2).
3. Perform identification: compare $\mathbf{b}'_{i'j'}$ with each reference binary template $\bar{\mathbf{b}}_i$, and classify the query to class Ω_{i_0} if $\bar{\mathbf{b}}_{i_0}$ is closet to $\mathbf{b}'_{i'j'}$.

3 Experimental Results

Two popular and public domain databases, namely CMU PIE [17] and FRGC [18], are employed in our experiments. The parameters are shown in Table 1, where c is the number of classes in the database, m denotes the number of images per class and p is the number of images per class used for training.

In all experiments, face region is manually extracted and aligned. Fisherface [2] is used to extract the facial feature vector which is considered as the original face template. We choose codewords from the $[511, 76, 171]$ BCH codes and determine the reference binary templates, which has sufficient between-class variance ($d = 171$) and sufficient security level ($k = 76$). Random Multi-space Quantization

(RMQ) algorithm [9] is used for comparison. The extracted RMQ binary templates have the same length as the original templates. We test our proposed algorithm in both identification and authentication systems.

Table 1. The experiment settings

Database	c	m	p
CMU PIE	68	105	10
FRGC	350	40	5

The experimental results are shown in Figure 3, with symbol "Original" denotes original system without protection, "RMQ" denotes the Random Multi-sacle Quantization algorithm and "BDA" denotes the proposed Binary Discriminant Analysis algorithm. The experimental results show that the binary templates extracted by our proposed BDA algorithm have better discriminability than the original templates and the binary templates extracted from the RMQ algorithm. The genuine accept rate (GAR) with fixed false accept rate FAR=0.1 in ROC curves and rank 1 accuracy of these methods are also reported in Table 2 and 3.

Table 2. GAR (in %) for the BDA algorithm, RMQ algorithm and the original template

GAR(%)	Original	RMQ	BDA
CMU PIE	59.26	66.18	87.32
FRGC	26.28	65.15	67.02

Table 3. Rank 1 accuracy (in %) for the BDA algorithm and RMQ algorithm

Accuracy (%)	RMQ	BDA
CMU PIE	66.93	83.25
FRGC	54.50	57.71

4 Conclusions

In this paper, we have proposed a new binary discriminant analysis (BDA) scheme to convert the original face templates into binary templates. A new multiple class gradient descent algorithm is proposed for optimizing the objective function in binary space. Experimental results show that the proposed BDA algorithm handles the discriminability of the extracted binary templates well and suitable for the biometric cryptosystem approach.

References

[1] J. L. Massey, "Shift-Register Synthesis and BCH Decoding," *IEEE Trans. Inform. Theory,*, vol. 15, no. 1, pp. 122-127, January 1969.

[2] P N Belhumeur, J P Hespanha and D J Kriegman, "Eigenfaces vs. fisherfaces: Recognition using class specific linear projection", *IEEE Trans. on PAMI,* 19(7), pp. 711-720, 1997.

[3] N Ratha, J Connell and R Bolle, "Enhancing security and privacy in biometric-based authentication systems," *IBM Systems Journal,* Vol. 40. No. 3, pp. 614 - 634, 2001.

[4] A K Jain, K Nandakumar and A Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, Vol. 8, 2008.

[5] U Uludag, S Pankanti, S Prabhakar and A K Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE,* vol. 92, no. 6, pp. 948-960, 2004.

[6] A Juels, M Wattenberg, "A fuzzy commitment scheme", *Proceedings of the Sixth ACM Conf. on Comp. and Comm. Security,* pp. 28-36, 1999.

[7] A Juels and M Sudan. "A Fuzzy Vault Scheme", *IEEE International Symposium on Information Theory,* 2002.

[8] F Monrose, M Reiter, Q Li and S Wetzel, "Cryptographic Key Generation from Voice," *Proc. IEEE Symp. Security and Privacy*, pp.202-213, May 2001.

[9] A Teoh, A Goh and D. Ngo, "Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1892-1901, Dec. 2006.

[10] Y C Feng, P C Yuen and A K Jain, "A Hybrid Approach for Generating Secure and Discriminating Face Template," *IEEE Transactions on Information Forensics and Security*, in press, 2010.

[11] E C Chang and S Roy, "Robust extraction of secret bits from minutiae," *in Proceedings of 2nd International Conference on Biometrics,* pp. 750C759, 2007.

[12] A Nagar, K Nandakumar and A K Jain, "A Hybrid Biometric Cryptosystem for Securing Fingerprint Minutiae Templates," *Pattern Recognition Letters,* 2009.

[13] A Nagar, K Nandakumar and A K Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," *International Conference on Pattern Recognition,* pp. 1-4, 2008.

[14] T A M Kevenaar, G J Schrijen, M Veen, A H M Akkermans, "Face recognition with renewable and privacy preserving binary templates," *IEEE Workshop on Automatic Identification Advanced Technologies,* pp. 21-26, 2005.

[15] J P Linnartz, P Tuyls, "New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates," *Audio and Video-Based Biometric Person Authentication,* 2003.

[16] R Duda, P Hart and D Stork, "Pattern classification," 2001.

[17] http://vasc.ri.cmu.edu/idb/html/face/index.html

[18] http://www.frvt.org/FRGC/