Appeared in Proc. of 4th Int'l Conference on Audio- and Video-Based Person Authentication (AVBPA), LNCS 2688, pp. 335-342, Guildford, UK, June 9-11, 2003.

Biometric Template Selection: A Case Study in Fingerprints

Anil Jain, Umut Uludag and Arun Ross

Michigan State University, East Lansing, MI, USA 48824
{jain, uludagum, rossarun}@cse.msu.edu

Abstract. A biometric authentication system operates by acquiring biometric data from a user and comparing it against the template data stored in a database in order to identify a person or to verify a claimed identity. Most systems store multiple templates per user to account for variations in a person's biometric data. In this paper we propose two techniques to automatically select prototype fingerprint templates for a finger from a given set of fingerprint impressions. The first method, called DEND, performs clustering in order to choose a template set that best represents the intra-class variations, while the second method, called MDIST, selects templates that have maximum similarity with the rest of the impressions and, therefore, represent typical measurements of biometric data. Matching results on a database of 50 different fingers, with 100 impressions per finger, indicate that a systematic template selection procedure as presented here results in better performance than random template selection.

1 Introduction

A biometric authentication system uses the physiological (fingerprints, face, hand geometry, iris) and/or behavioral traits (voice, signature, keystroke dynamics) of an individual to identify a person or to verify a claimed identity [1]. A typical biometric system operates in two distinct stages: the enrollment stage and the authentication stage. During enrollment, a user's (the enrollee) biometric data (e.g., fingerprints) is acquired and processed to extract a feature set (e.g., minutiae points) that is stored in the database. The stored feature set, labeled with the user's identity, is referred to as a template. In order to account for variations in the biometric data of a user, multiple templates corresponding to each user may be stored. During authentication, a user's biometric data is once again acquired and processed, and the extracted feature set is matched against the template(s) stored in the database in order to identify a previously enrolled individual or to validate a claimed identity. The matching accuracy of a biometrics-based authentication system relies on the *stability* (permanence) of the biometric data associated with an individual over time. In reality, however, the biometric data acquired from an individual is susceptible to changes introduced due to improper interaction with the sensor (e.g., partial fingerprints, change in pose

during face-image acquisition), modifications in sensor characteristics (e.g., optical vs. solid-state fingerprint sensor), variations in environmental factors (e.g., dry weather resulting in faint fingerprints) and temporary alterations in the biometric trait itself (e.g., cuts/scars on fingerprints). In other words, the biometric measurements tend to have a large intra-class variability. Thus, it is possible for the stored template data to be significantly different from those obtained during authentication (Figure 1), resulting in an inferior performance (higher false rejects) of the biometric system.

(a) (b)

Fig. 1. Variations in fingerprints: Two impressions of a fingerprint acquired at different time instances exhibiting partial overlap.

In order to account for the above variations, multiple templates, that best represent the variability associated with a user's biometric data, should be stored in the database. For example, one could store multiple impressions pertaining to different portions of a user's fingerprint in order to deal with the problem of partially overlapping fingerprints. Similarly, a user's face image acquired from multiple viewpoints may be stored in order to account for variations in a person's pose. There is a tradeoff between the number of templates, and the storage and computational overheads introduced by multiple templates. For an efficient functioning of a biometric system, this selection of templates should be done automatically. However, there is limited literature dealing with the problem of automatic template selection in a biometric system. We propose techniques to automatically select the templates in order to account for variations observed in a user's biometric data as well as to adequately represent typical data values. Although we consider a fingerprint-based biometric system as our test-bed, the techniques presented in this paper may be applied to other types of biometric traits (such as face and hand geometry) as well.

2 Template Selection

The problem of template selection with regard to fingerprints may be posed as follows: Given a set of N fingerprint images corresponding to a single finger, select K templates that 'best' represent the variability as well as the typicality observed in the N images, $K < N$. Currently, we assume that the value of K

is predetermined. This systematic selection of templates is expected to result in a better performance of a fingerprint matching system compared to a random selection of K templates out of the N images.

It is important to note that template selection is different from template update. The term template update is used to refer to one of the following situations: (i) Template aging: Certain biometric traits of an individual vary with age. The hand geometry of a child, for example, changes rapidly during the initial years of growth. To account for such changes, old templates have to be regularly replaced with newer ones. The old templates are said to undergo aging. (ii) Template improvement: A previously existing template may be modified to include information obtained at a more recent time instance. For example, minutiae points may be added to, or deleted/modified from the template of a fingerprint, based on information observed in recently acquired impressions [2–4]. As another example, Liu et al. [5] update the eigenspace in a face recognition system via decay parameters that control the influence of old and new training samples of face images. Thus, template selection refers to the process by which prototype templates are chosen from a given set of samples, whereas template update refers to the process by which existing templates are either replaced or modified. We propose the following two methods for template selection:

Method 1 (DEND): In this method, the N fingerprint impressions corresponding to a user are grouped into K clusters, such that impressions within a cluster are more similar than impressions from different clusters. Then for each cluster, a prototype (representative) impression that typifies the members of that cluster is chosen, resulting in K template impressions.

To perform clustering, it is required to compute the (dis)similarity between fingerprint impressions. This measure of (dis)similarity is obtained by matching the minutiae point sets of the fingerprint impressions. Our matching algorithm is based on an elastic string matching technique that outputs a distance score indicating the dissimilarity of the minutiae sets being compared [6]. Since our representation of the N fingerprint impressions is in the form of a $N \times N$ dissimilarity matrix instead of a $N \times d$ pattern matrix (d is the number of features), we use hierarchical clustering [7]. In particular, we use an agglomerative complete link clustering algorithm. The output of this algorithm is a dendrogram which is a binary tree, where each terminal node corresponds to a fingerprint impression, and the intermediate nodes indicate the formation of clusters (see Figure 2).

The template set T, $|T| = K$, is selected as follows:

1. Step 1: Generate the $N \times N$ dissimilarity matrix, M, where entry (i, j), $i, j \in \{1, 2, \ldots N\}$ is the distance score between impressions i and j.
2. Step 2: Apply the complete link clustering algorithm on M, and generate the dendogram, D. Use the dendogram D to identify K clusters.
3. Step 3: In each of the clusters identified in step 2, select a fingerprint impression whose average distance from the rest of the impressions in the cluster is minimum. If a cluster has only 2 impressions, choose any one of the two impressions at random.

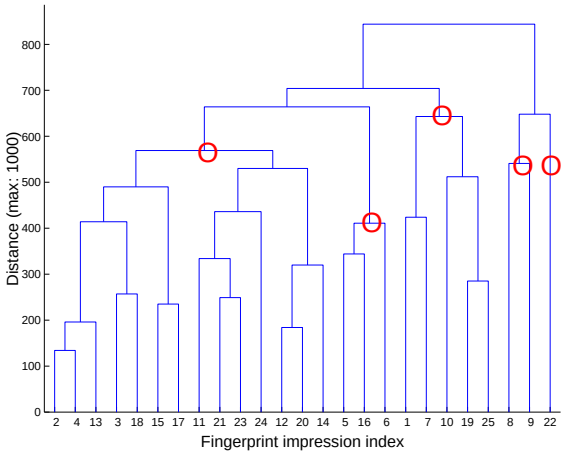


Fig. 2. Dendrogram generated using the 25 fingerprint impressions of one finger. The circles on the subtrees indicate impressions enclosed by the clusters for $K = 5$.

4. Step 4: The impressions selected in step 3 constitute the template set T.

We refer to the above algorithm as DEND since it uses the dendrogram to choose the representative templates.

Method 2 (MDIST): The second method sorts the fingerprint impressions based on their *average* distance score with other impressions, and selects those impressions that correspond to the K smallest average distance scores. Here, the rationale is to select templates that exhibit maximum similarity with the other impressions and, hence, represent typical data measurements. We refer to this method as MDIST since templates are chosen using a minimimum distance criteria. Thus, for every user:

1. Step 1: Find the pair-wise distance score between the N impressions.
2. Step 2: For the j^{th} impression, compute its average distance score, d_j, with respect to the other $(N-1)$impressions.
3. Step 3: Choose K impressions that have the smallest average distance scores. These constitute the template set T.

The choice for the value of K is application dependent. Larger K values would mean storing more templates per user, and this may not be feasible in systems with limited storage capacities. Moreover during authentication, matching a query (input) image with a large number of templates per user would be computationally demanding. Smaller K values, on the other hand, may not sufficiently capture the intra-class variability nor the typicality of the impressions, leading to inferior matching performance. Therefore, a reasonable value of K, that takes into account the aforementioned factors, has to be specified.

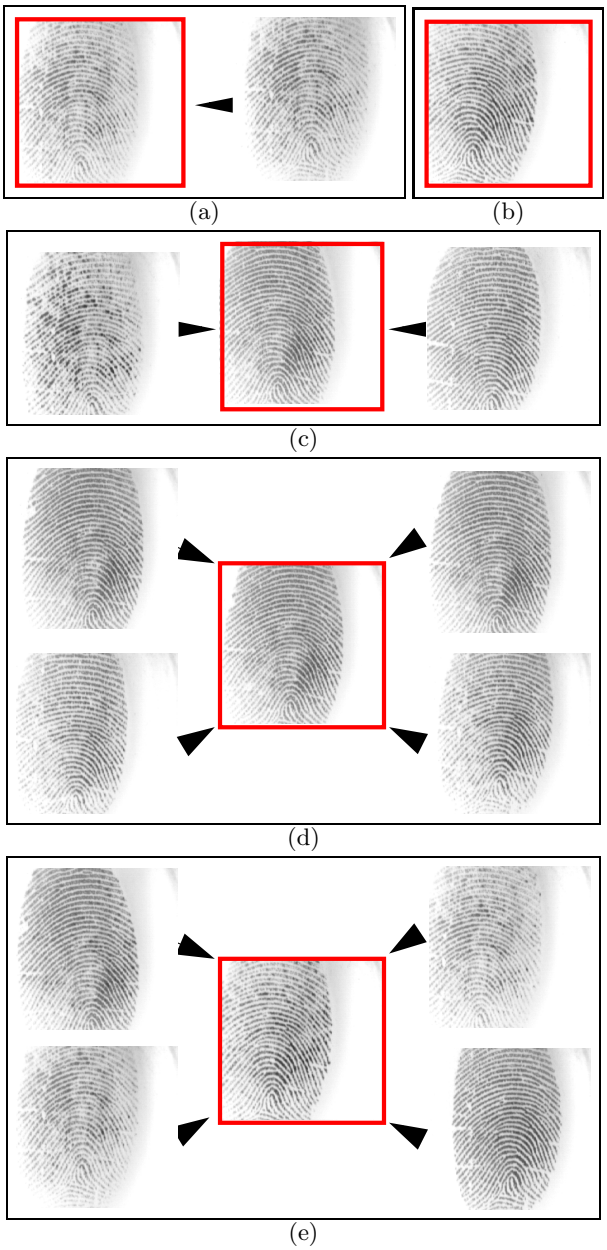


Fig. 3. The cluster membership ($K = 5$) for the dendrogram shown in Figure 2. At most 5 members are indicated for each cluster. The prototype template in each cluster is marked with a thick border. Note that the cluster in (b) has only one member.

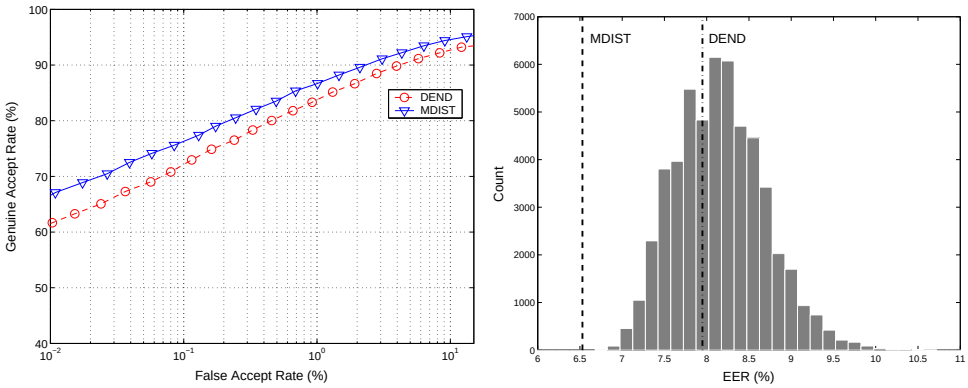
Fig. 4. The prototype templates of a finger selected using the MDIST algorithm.

3 Experimental Results

In order to study the effect of automatic template selection on fingerprint matching, we need to have several impressions per finger (~ 25). Standard fingerprint databases (e.g., FVC 2002 [8]) do not contain a large number of impressions per finger. Therefore, we collected 100 impressions each of 50 different fingers (10 fingers each of 5 different individuals) in our laboratory using the Identix BioTouch USB 200 optical sensor (255×256 images, 380 dpi). The data was acquired over a period of two months with no more than 5 impressions of a finger per day. The 100 impressions of each finger were partitioned into two sets: template selection was done using the first 25 impressions, and the matching performance of the selected templates was tested using the remaining 75 impressions (test set).

Figure 2 shows the dendrogram obtained using the 25 fingerprint impressions of one finger. On setting $K = 5$, the resulting clusters and their prototypes as computed using the DEND algorithm are shown in Figure 3; some clusters are seen to have only one member, suggesting the possible existence of outliers. The various prototypes are observed to have different regions of overlap with respect to the extracted minutiae points. The prototypes, for the same finger, computed using the MDIST algorithm are shown in Figure 4.

In order to assess the matching performance of the proposed techniques (for $K = 5$), we match every image in the test set (50 fingers, 75 impressions per finger) against the selected templates (5 per finger). When a test image is matched with the template set of a finger, 5 different distance scores are obtained. The mimimum of these scores is reported as the final matching score. Thus, we obtain $187,500$ matching scores ($75 \times 50 \times 50$) using the selected template sets. Figure 5(a) shows the ROC (Receiver Operating Characteristic) curves representing the matching performance of the template sets selected using both the algorithms. The Equal Error Rates (EER) of DEND and MDIST are observed to be 7.95% and 6.53%, respectively. Now, for the 50 fingers, there are a total of $\binom{25}{5}^{50} - 1$ *non-selected* template sets. It is computationally prohibitive to generate the matching scores and the ROC curves corresponding to all these permutations. Therefore, we chose $53,130$ permutations (assuming that the impression indices in the template set of all the 50 fingers is the same) and computed their EER. The histogram of EER values is shown in Figure 5(b). In this histogram,



(a) (b)

Fig. 5. (a) The ROC curves for the DEND and MDIST algorithms. (b) The EER histogram for the non-selected sets.

the vertical dashed lines indicate the EER values corresponding to the DEND and MDIST algorithms. The percentage of non-selected template sets that have a lower EER than the template sets selected with the proposed methods is 37.7% and 0%, for DEND and MDIST, respectively, thereby suggesting that systematic template selection is better than random selection.

The table in Figure 6(a) lists the impressions that were selected as templates for one finger using the DEND and MDIST algorithms at different K values. The impression index indicates the acquisition time of the impressions - a lower index referring to an earlier time instance. We see that there is no direct relationship between an impression index and its choice as a template. This result suggests that template selection is a necessary step prior to matching. Figure 6(b) shows the EER of the proposed selection methods at different values of K.

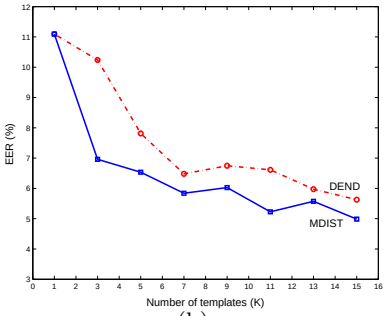
4 Discussion and Future Work

A systematic procedure for template selection is critical to the performance of a biometric system. Based on our experiments, we observe that the MDIST algorithm for template selection results in a better matching performance than DEND. This may be attributed to the fact that MDIST chooses a template set that typifies those candidate impressions that are similar and occur frequently. However, the DEND method captures the variations associated with the fingerprint impressions. We also observe that systematic template selection results in a better performance than random selection of templates.

The template selection mechanism has to be applied periodically, and in an incremental fashion, as more and more biometric samples of an individual are acquired after repeated use of the system. Currently, we are working on employing the template selection techniques to *update* the template set of a user

K	DEND	MDIST
1	2	2
3	4,8,25	2,4,13
5	4,5,9,22,25	2,3,4,12,13
7	2,5,7,9,19,22,23	2,3,4,12,13,21,23
9	2,5,7,8,9,19,20,22,23	2,3,4,12,13,20,21,23,25

(a)



(b)

Fig. 6. (a) The selected templates for a finger using the DEND and MDIST algorithms at different K values. (b) The EER of the fingerprint matcher at different values of K.

in fingerprint systems. We are also examining ways to determine the value of K automatically. It may be necessary to store different number of templates for different users. Future work would involve testing similar techniques on face and hand biometric data.

References

1. J. L. Wayman, "Fundamentals of biometric authentication technologies," *International Journal of Image and Graphics*, vol. 1, no. 1, pp. 93–113, 2001.
2. X. Jiang and W. Ser, "Online fingerprint template improvement," *IEEE Transactions on PAMI*, vol. 24, pp. 1121–1126, August 2002.
3. K. A. Toh, W. Y. Yau, X. D. Jiang, T. P. Chen, J. Lu, and E. Lim, "Minutiae data synthesis for fingerprint identification application," in *Proc. International Conference on Image Processing (ICIP)*, vol. 3, pp. 262–265, 2001.
4. A. K. Jain and A. Ross, "Fingerprint mosaicking," in *Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, (Orlando, Florida), May 2002.
5. X. Liu, T. Chen, and S. M. Thornton, "Eigenspace updating for non-stationary process and its application to face recognition," *To appear in Pattern Recognition, Special issue on Kernel and Subspace Methods for Computer Vision*, 2003.
6. A. K. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification," *IEEE Transactions on PAMI*, vol. 19, pp. 302–314, April 1997.
7. A. K. Jain and R. C. Dubes, *Algorithms for Clustering Data*. Englewood Cliffs, New Jersey: Prentice Hall, 1988.
8. D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Fingerprint verification competition," in *Proceedings of the International Conference on Pattern Recognition (ICPR)*, (Quebec City, Canada), pp. 744–747, August 2002.