Minutiae-based Matching State Model for Combinations in Fingerprint Matching System

Xi Cheng, Sergey Tulyakov and Venu Govindaraju
Center for Unified Biometrics and Sensors
University at Buffalo, NY, USA
xicheng,tulyakov,govind@buffalo.edu

Abstract

In this paper we investigate the question of combining multi-sample matching results obtained during repeated attempts of fingerprint based authentication. In order to utilize the information corresponding to multiple input templates in a most efficient way, we propose a minutiae-based matching state model which uses relationship between test templates and enrolled template. The principle of this algorithm is that matching parameters, i.e the sets of matched minutiae, between these templates should be consistent in genuine matchings. Experiments are performed on FVC2002 fingerprint databases. Result shows that the system utilizing the proposed matching state model is able to outperform the original system with raw matching scores. Likelihood ratio and multilayer perceptron are used as combination methods.

1. Introduction

Generally, it is believed that the performance of biometric systems can be improved by fusing multiple sources of biometric modalities. The idea is that the great diversity of different modalities could lead to the enhancement of classification accuracy [12]. Basically, different modalities are considered independently, and, for instance, there is no correlation between one person's face and fingerprints. But for unimodal systems with multiple templates, there is correspondence between samples or features, for example, fingerprint templates captured by two sensors at the same time should be consistent to each other. This paper investigates such correlation between matching templates and uses it to improve performance.

Fingerprint systems are widely used because of its high uniqueness and permanence. The process of fingerprint authentication is to match test template T_t to enrolled one T_e to determine if they are the same. But non-linear distortion might make two templates from the same finger to be different. In the case of bad matching, user might be asked to provide another attempt where fusion is needed in this case.

The successful fusion algorithm considered in situation of multiple samples should take into account the measures of consistency for biometric data obtained from different attempts. These measures can be derived if the details of the matching algorithms are available. For example, the earlier method of face representation used for face recognition consists of a set of pre-defined landmark points [5]. Thus the face recognition taking advantage of multiple cameras or video frames, typically attempts to reconcile the models of each camera or frame by constructing a generic model representation [14, 15].

In this paper, we consider the consistency of minutiae points in enrolled and test fingerprint templates. During genuine matching attempts, minutiae of the test fingerprints contributing to matching scores most probably have correct pairings with minutiae of the enrolled template, and, as a consequence, minutiae of two test fingerprints are paired between themselves as well. In contrast, when two impostor test fingerprints are presented to the matcher, the sets of matched minutiae are possibly more randomly paired, and there are less correspondences between matched minutiae belonging to two test fingerprints. If such hypothesis is true, then the auxiliary information in the form of numbers of corresponding pairs of matched minutiae in two test fingerprints, should be useful to improve the discrimination between genuine and impostor matches. In our experiments, we will be combining such information with raw matching scores to make a better authentication decision in a fingerprint verification system.

2. Previous Work

Previous work in multi-sample fusion use either feature level or score level fusion. Ryu et al. [8] proposed an approach to generate a *super-template* by incorporating only the highly credible minutiae points based on multiple fingerprint images. A successive Bayesian estimation ap-

978-0-7695-4990-3/13 $26.00 © 2013 IEEE
DOI 10.1109/CVPRW.2013.21

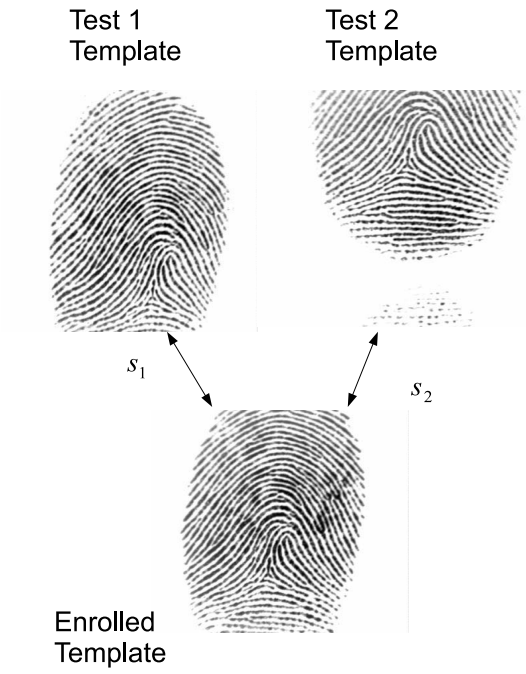


Figure 1. Matching scenario of our system.

proach was applied to a sequence of templates to determine the highly likely true minutiae. The experimental results showed that more impressions of the same fingerprint are used, the better accuracy will be achieved. Jain et al. [6] defined spatial relationship between two input templates using a modified iterative closest point algorithm to compute a transformation matrix. Better performance can be achieved by extracting augmented minutiae sets after test templates are mosaicked. All these methods utilize only positive examples to improve representation of multiple enrolled templates.

Feature level fusion or creation of composite template can be used in other modalities. For example, a set of signatures can be used to construct a template as a trained HMM in handwritten signature verification system [11]. In face recognition system, the sequence of video frames can be used to generate a more precise model of the face [9].

Contrary to feature level fusion, score level fusion provides us a way to fuse templates without detail of matching algorithms. Previous work of fingerprint and face biometric systems have employed score level fusion in multi-sample scenario. Uludag et al. [13] proposed a similarity score-based approach to select and to fuse multiple templates for each enrollee in order to improve the performance of a fingerprint authentication system. Verification was done based on the mean (or minimum) of the similarity scores of the query with the templates of the claimed identity. Chellappa et al. [3] generated a sequence of matching scores by matching each frame extracted from a clip of video to an enrolled face template of the person. Conditional entropy which captures the evolving uncertainty of the identity variable given observations is updated to combine matching scores. In [4] we used the score between test templates in addition to raw matching scores. Such score could indicate either the quality of the test templates or the diversity between them. The presented fusion algorithm is relatively heuristic but seems to be efficient since only one more score should be generated.

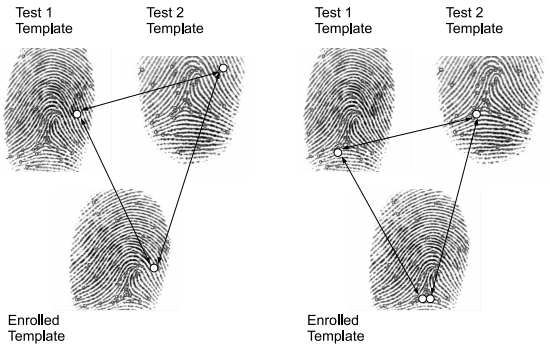
Our method in this paper considers an indeterminate approach using matching scores and parameters of obtained matches. Instead of attempting to build a composite model as in the previous methods or just using matching scores, we propose to derive the matching state model information which represents the multi-sample matching scenario. This is some additional information which describes parameters of the found match, and we use this information along with raw matching scores. Our conjecture is that this approach will be more successful in situations, where one of the samples makes error in multi-sample matching.

In contrast to typical feature level and score level fusion algorithms, current approach attempts to fuse the auxiliary information obtained during matching. In this regard it is somewhat similar to the multi-view face fusion methods [14, 15], which reconstruct the position of the face with respect to different camera views and check the consistency of the transformation from one face view to another. It seems that such idea has not yet been applied to fingerprint matchers.

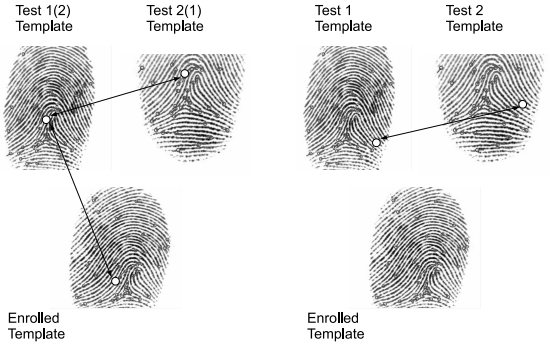
3. Minutiae-based Matching State Model

We consider the matching scenario shown in Fig. 1 having one enrolled template T_e and two test templates T_{t1} and T_{t2}. One verification attempt has two matching scores between the enrolled template and two test templates - s_1 and s_2. Genuine verification attempt is the case where enrolled and test templates are from the same finger, that is, s_1 and s_2 are both genuine scores. The case of impostor attempt is generated by assuming both test templates from one finger and enrolled one from another finger, in this case, s_1 and s_2 are both impostor scores.

With standard template representation consisting of a set of minutiae points from fingerprints, matching algorithm can output which minutiae points are matched in each template. Since in both genuine and impostor matchings two test templates are from the same finger, Fig. 2 shows four cases based on matched minutiae in two test templates. Minutiae in test templates are represented to be m_{t1}

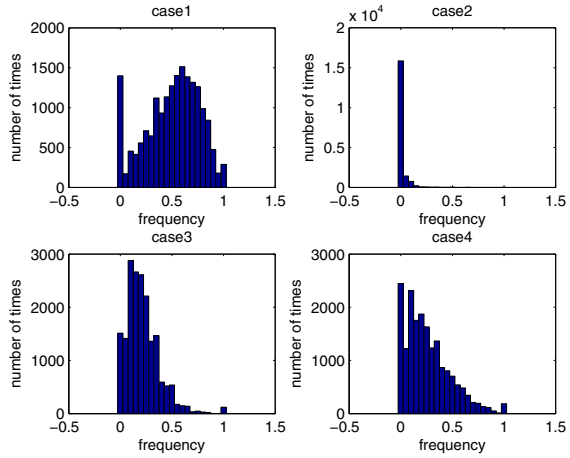


(a) Case 1 (b) Case 2

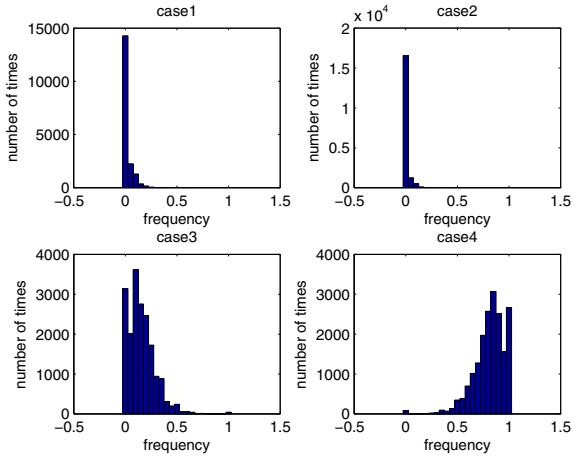


(c) Case 3 (d) Case 4

Figure 2. Four cases based on matched minutiae correspondences for two test and one enrolled fingerprint templates.



(a) Genuine DB1



(b) Impostor DB1

Figure 3. Histogram of frequency for each case in genuine and impostor matchings of DB1

and m_{t2}, and minutiae in the enrolled template to be m_e. Fig. 2(a) is the case where m_{t1}, m_{t2} and m_e are matched to each other. This is the case which happens a lot in genuine matching where all templates are from the same finger. Fig. 2(b) shows the case in which m_{t1} and m_{t2} are matched, but respective matched minutiae are different in the enrolled template. Fig. 2(c) means no matching between m_e and m_{t2}(or m_{t1}) though both of them are matched to one minutiae in another test template. Fig. 2(d) shows the fourth case where no matching between m_e and m_{t1}(or m_{t2}) when m_{t1} matches to m_{t2}. Impostor matchings always contain many such cases since test and enrolled templates are from different fingers. These are the only four possible cases when m_{t1} matches to m_{t2}. Our hypothesis is that the first case indicates the correspondence between matching two test fingerprints to one enrolled fingerprint, and the other cases indicate the disagreement between matches. If we denote the number of matched minutiae pairs for two test templates as $num\_matched(m_{t1}, m_{t2})$, the number of each case as num_case_i $1 \leq i \leq 4$, the frequency of each case in each matching triplet is defined as:

$$freq_i = \frac{num\_case_i}{num\_matched(m_{t1}, m_{t2})} \quad (1)$$

where i= 1,2,3 and 4 and summation of frequencies equals to 1. We want to use the frequencies of each case along with the matching scores s_1 and s_2 in Fig. 1 to make better authentication decisions. According to our hypothesis, the frequency of first case should have a positive effect on the combined matching score, and frequencies of other cases should have a negative effect.

4. Combination Methods

FVC2002 has four databases DB1, DB2, DB3 and DB4 where each one was captured by different sensors. Each

database has 110 different persons with 8 different images for the same finger of the person [1]. The genuine matching case is generated by assuming one of eight images for the same finger to be enrolled and other two to be tested. For each person, there are 168 such matching variations and totally it's $168 * 110 = 18480$. On the other hand, the impostor matching case is generated by matching one image from one person as the enrolled template and two test templates from another person. The number of impostor matchings is selected as the same as the number of genuine matchings.

Fig. 3 shows the histogram of frequencies for genuine and impostor matchings in DB1. Since DB2, DB3 and DB4 have the similar scenarios, we omit figures for them. As you can see the genuine matching in Fig. 3(a), distribution of frequencies for case 1 is near 1 and most of the frequencies for case 4 are near 0. This is actually expected because in genuine matching, most of minutiae in each of three templates can be matched to each other. On the other hand, impostor matching in Fig. 3(b) says, most of frequencies for case1 are near 0 but most of them for case 4 are near 1. This is also true because impostor matching means test templates from the same finger but enrolled one from another. Most of time, when two minutiae in each test template are matched, both of them might not be matched to any minutiae in enrolled template. So case 4 is dominant in impostor matchings. But for case 2 or case 3, the distributions of frequencies are comparable to the respective cases in genuine and impostor matchings. So it's not clear if case 2 and case 3 are useful to discriminate genuine and impostor matchings. Information from case 1 and case 4 is useful to make such decision, since if frequency of case 1 is closer to 1, it's more probably to be a genuine matching. On the other hand, if frequency of case 4 is closer to 1, it is more likely to be an impostor matching. In this paper, we only use the frequencies for case 1 and case 4 in the matching state model.

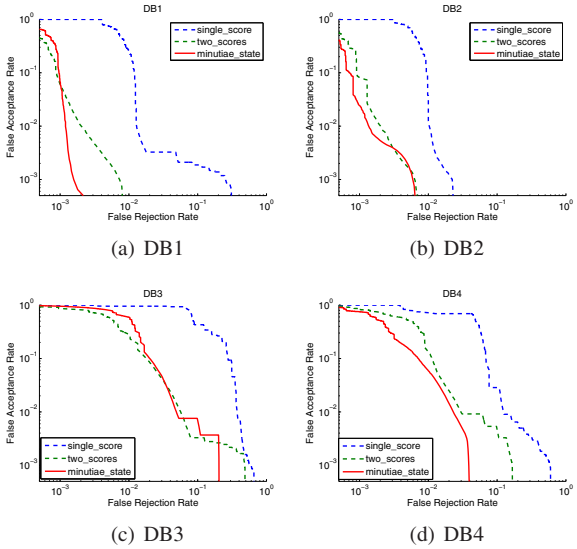
The first experiment on measuring the effect of minutiae-based model on classifying genuine and impostor matching attempts is likelihood ratio - the optimal method in verification biometric systems [10]. For the system using raw matching scores, the likelihood ratio is:

$$S = \frac{p_{gen}(s_1, s_2)}{p_{imp}(s_1, s_2)} \tag{2}$$

where $p_{gen}(s_1, s_2)$ is the probability density of genuine scores s_1 and s_2, and $p_{imp}(s_1, s_2)$ is the probability density of impostor scores. Likelihood ratio assigns the combined score a value of ratio between genuine and impostor score densities.

To use frequencies for case 1 and case 4, four dimensional probability densities are constructed in likelihood ratio:

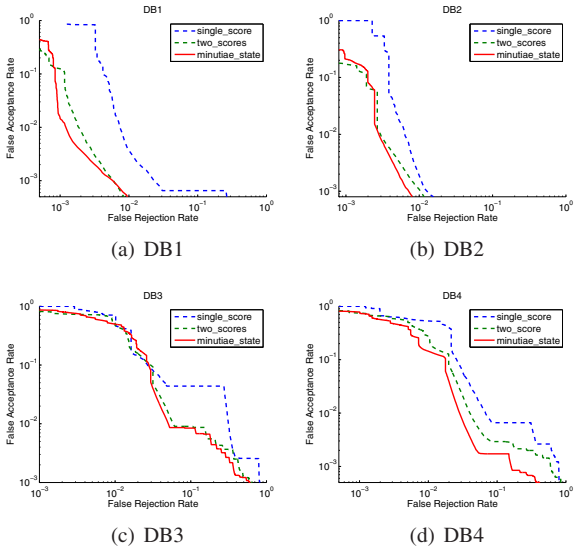
$$S = \frac{p_{gen}(s_1, s_2, freq_1, freq_4)}{p_{imp}(s_1, s_2, freq_1, freq_4)} \tag{3}$$



(a) DB1 (b) DB2

(c) DB3 (d) DB4

Figure 4. Likelihood Ratio



(a) DB1 (b) DB2

(c) DB3 (d) DB4

Figure 5. Multilayer Perceptron

Since the approximation of densities of genuine and impostor scores could have a negative impact for likelihood ratio method, we verify the results with the combination method utilizing multilayer perceptron to compare the use of raw matching scores and the minutiae-based matching state model. The used perceptron has two hidden layers with eight nodes in the first hidden layer and nine nodes in the second hidden layer. The input layer for system with raw scores contains two nodes with each for one score. The input layer for matching state model has four nodes for two matching scores, $freq_1$ and $freq_4$. The output layer for both situations has one node with expected 0 for impostor matching and 1 for genuine matching.

5. Experiment

We use the minutiae-based fingerprint matching system proposed in [7] to get matching scores and corresponding matched minutiae points of two templates. The system used minutiae points as well as secondary features which incorporate relative distance of minutiae, radial angle of minutiae, and minutia orientations in each fingerprint. Instead of using $n^2/(size_1 + size_2)$ or $2 * n/(size_1 + size_2)$ (where $size_1$ and $size2$ are the numbers of minutiae in each print, and n is the number of matched minutiae) to compute the similarity scores, they utilized number of minutiae points on overlapping areas and average feature distances to calculate reliable scores. Matching process was converted to a minimum cost flow problem which gave an efficient way to get optimal matching.

For both likelihood ratio and multilayer perceptron, we use bootstrap technique [2]. In each step of bootstrap, twenty five persons are randomly selected for training, other twenty five persons for validation, and remaining sixty persons for testing.

Results for likelihood ratio and multilayer perceptron are shown in Fig. 4 and Fig. 5. The curve notated 'single_score' is the ROC for utilization of only one template. The curve notated 'two_scores'is for two matching scores fusion as in Eq. 2. The curve for minutiae-based matching state model is notated as 'minutiae-based'. As it was expected, the performance of fusion two scores is much better than using one score. The minutiae-base matching state model improved the performance further. The equal error rates (EER) are shown in Table 1 and Table 2 with mean and standard derivation from one hundred bootstrap steps. Since the purpose of this paper is to compare fusion two scores with and without minutiae-based model, the EER for single score is not shown here. Result show that using minutiae-based matching state model in both likelihood ratio and multilayer perceptron performs better than just using raw matching scores.

The additional computational complexity compared to system using raw scores can be acceptable, since matching pairs are generated at the time of score calculation. The only additional time is to compare the three matched minutiae sets to get frequencies for each case in Fig. 2.

6. Conclusions

In this paper, we have proposed a minutiae-based matching state model in multi-sample fingerprint systems. In minutiae-based fingerprint systems, scores are generated by using matched minutiae in two matching fingerprints. In the case of multiple input samples, the minutiae matched in test templates and the enrolled template should be consistent. We have analyzed four cases where test templates are from the same finger and concluded that the first case in Fig. 2(a) and the fourth case in Fig. 2(d) might useful to improve the performance in addition to raw matching scores.

EER(%)	two scores	matching state model
db1	0.349 ± 0.058	0.145 ± 0.040
db2	0.344 ± 0.071	0.329 ± 0.041
db3	3.300 ± 0.380	3.057 ± 0.247
db4	2.044 ± 0.248	1.803 ± 0.227

Table 1. Equal error rate for FVC2002 datasets using likelihood ratio

EER(%)	two scores	matching state model
db1	0.254 ± 0.074	0.197 ± 0.059
db2	0.233 ± 0.099	0.227 ± 0.097
db3	2.998 ± 0.620	2.770 ± 0.568
db4	2.079 ± 0.283	1.56 ± 0.324

Table 2. Equal error rate for FVC2002 datasets using multilayer perceptron

We have used both likelihood ratio and multilayer perceptron based on FVC2002 dataset. Experimental results show that utilization of proposed minutiae-based matching state model can get better performance than using only raw matching scores.

The minutiae-based matching state model can be extended to be used in scenarios where more than two test or enrolled templates are used. The cases as in Fig. 2 will be slightly modified according to that situation. In case one of more than two test templates is erroneous, it is possible to find out the erroneous one by using the matching state model accounting for frequencies of each case in each template. These will be left for our future work.

References

[1] Fingerprint verification competition. 2006. http://bias.csr.unibo.it/fvc2002/. 4

[2] R. M. Bolle, N. K. Ratha, and S. Pankanti. Error analysis of pattern recognition systems–the subsets bootstrap. *Computer Vision and Image Understanding*, 93(1):1–33, 2004. doi: DOI: 10.1016/j.cviu.2003.08.002. 5

[3] R. Chellappa, V. Kruger, and Z. Shaohua. Probabilistic recognition of human faces from video. In *Image Processing. 2002. Proceedings. 2002 International Conference on*, volume 1, pages I–41–I–44 vol.1, 2002. 2

[4] X. Cheng, S. Tulyakov, and V. Govindaraju. Multiple-sample fusion of matching scores in biometric systems. *Computer Vision and Pattern Recognition Workshops (CVPRW), 2011 IEEE Computer Society Conference on*, pages 120–125. 2

[5] T. F. Cootes, G. J. Edwards, and C. J. Taylor. Active appearance models. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 23(6):681–685, 2001. 1

[6] A. Jain and A. Ross. Fingerprint mosaicking. In *Acoustics, Speech, and Signal Processing, 1993. ICASSP-93., 1993*

IEEE International Conference on, volume 4, pages IV–IV, 2002. 2

[7] T.-Y. Jea and V. Govindaraju. A minutia-based partial fingerprint recognition system. *Pattern Recognition*, 38(10):1672–1684, 2005. 5

[8] T. Kanade, A. Jain, N. Ratha, C. Ryu, Y. Han, and H. Kim. Super-template generation using successive bayesian estimation for fingerprint enrollment. In *Audio- and Video-Based Biometric Person Authentication*, volume 3546 of *Lecture Notes in Computer Science*, pages 261–277. Springer Berlin / Heidelberg, 2005. 1

[9] L. Kuang-Chih, J. Ho, Y. Ming-Hsuan, and D. Kriegman. Video-based face recognition using probabilistic appearance manifolds. 1:I–313–I–320 vol.1, 2003. 2

[10] S. Prabhakar and A. K. Jain. Decision-level fusion in fingerprint verification. *Pattern Recognition*, 35(4):861–874, 2002. doi: DOI: 10.1016/S0031-3203(01)00103-0. 4

[11] G. Rigoll and A. Kosmala. A systematic comparison between on-line and off-line methods for signature verification with hidden markov models. In *Pattern Recognition, 1998. Proceedings. Fourteenth International Conference on*, volume 2, pages 1755–1757 vol.2, 1998. 2

[12] A. A. Ross, K. Nandakumar, and A. K. Jain. *Handbook of Multibiometrics*. International Series on Biometrics. Springer-Verlag New York, Inc., 2006. 1

[13] U. Uludag, A. Ross, and A. A. Jain. Biometric template selection and update: a case study in fingerprints. *Pattern Recognition*, 37(7):1533–1542, 2004. doi: 10.1016/j.patcog.2003.11.012. 2

[14] S. Von Duhn, Y. Lijun, K. Myung Jin, and T. Hung. Multiple-view face tracking for modeling and analysis based on non-cooperative video imagery. pages 1–8, 2007. 1, 2

[15] Y. Zhang and A. M. Martnez. A weighted probabilistic approach to face recognition from multiple images and video sequences. *Image and Vision Computing*, 24(6):626–638, 2006. doi: DOI: 10.1016/j.imavis.2005.08.004. 1, 2