Fingerprint Matching with Registration Pattern Inspection*

Hong Chen, Jie Tian, and Xin Yang

Biometrics Research Group, Institute of Automation, Chinese Academy of Science
PO Box 2728, Beijing 100080, China
tian@doctor.com
jie.tian@fingerpass.net.cn

Abstract. The *"registration pattern"* between two fingerprints is the optimal registration of each part of one fingerprint with respect to the other fingerprint. *Registration patterns* generated from imposter's matching attempts are different from those patterns from genuine matching attempts, although they may share some similarities in the aspect of minutiae. In this paper, we present an algorithm that utilizes minutiae, associate ridges and orientation fields to determine the *registration pattern* between two fingerprints and match them. The proposed matching scheme has two stages. An offline, training stage, derives a *genuine registration pattern base* from a set of genuine matching attempts. Then, an online matching stage registers the two fingerprints and determines the *registration pattern*. Only if the pattern makes a genuine one, a further fine matching is conducted. The *genuine registration pattern base* was derived using a set of fingerprints extracted from the NIST Special Database 24. The algorithm has been tested on the second FVC2002 database. Experimental results demonstrate the performance of the proposed algorithm.

1 Introduction

Great improvement has been achieved in the development of on-line fingerprint sensing techniques and automatic fingerprint recognition algorithms. However, there are still many challenging problems exist. One challenge is how to reliably and adequately extract and record a fingerprint's feature in a convenient way for matching. Another challenging problem is matching of non-linear distorted fingerprints. The distortion consisted of two parts. The acquisition of a fingerprint is a 3D-2D warping process. Next time the fingerprint captured with a different contact center will result in a different warping mode. The other possible that will introduce distortion to

* This paper is supported by the National Science Fund for Distinguished Young Scholars of China under Grant No. 60225008, the Prophasic Project of National Grand Fundamental Research 973 Program of China under Grant No. 2002CCA03900, the National Natural Science Foundation of China under Grant No. 79990580.

J. Kittler and M.S. Nixon (Eds.): AVBPA 2003, LNCS 2688, pp. 327-334, 2003.

fingerprint is the non-orthogonal pressure people exert on the sensor. How to cope with these non-linear distortions in the matching algorithm is a real challenge.

Most automatic fingerprint verification systems are based on minutiae matching since the most reliable feature for fingerprint matching is minutiae. There are three major drawbacks with these methods. I.) Imperfection in the minutiae extract algorithm or the strong noise in the image may introduce false minutiae or miss genuine minutiae. II.) Rich information the ridge/valley structure for discrimination is not used by these methods. III.) In order to allow those greatly distorted fingerprint to be recognized, these methods have to use a large bounding box and consequently sacrifice the accuracy of the system. Jain *et al.* [3, 4] proposed a novel filterbank-based fingerprint feature representation method well handle the first two drawbacks. Fan *et al.* [11] used a set of geometric masks to record part of the rich information of the ridge structure. And Tian *et al.* [13] utilized both the minutiae and part of the associate ridges. However, these methods do not solve the problem of distortions.

Recently, some methods were presented that explicitly deal with the problem of the non-linear distortion in fingerprint images and the matching of such images. Ratha *et al.* [8] proposed a method to measure the forces and torques on the scanner directly with the aid of specialized hardware. And Dorai *et al.* [9] proposed a method to detect and estimate distortion occurring in fingerprint videos. But these methods do no help when images are already collected. Maio and Maltoni *et al.* [5] proposed a plastic distortion model to "describe how fingerprint images are deformed when the user improperly places his/her finger on the sensor plate". This model helps to understand this process. However, due to the insufficiency and uncertainty of information, it is very difficult to automatically and reliably estimate the parameter in that model. Senior *et al.* [7] proposed a method to convert a distorted fingerprint image into an equally spaced fingerprint before matching and improved the matching accuracy. However, if the compression or traction force is parallel to the local ridge orientation, the inter-ridge space will not change and this method cannot detect it. And the method cannot handle the distortion introduced by different contact center. Bazen *et al.* [6] used a thin-plate spline model to describe the non-linear distortions between the two sets of possible matching minutiae pairs. By normalizing the input fingerprint with respect to the template, this method is able to perform a very tight minutiae matching and thus improve the performance. However, the TPS model focuses on smoothly interpolating images over scattered data. When applied this model to fingerprint recognition, it can make two fingerprints, no matter they come from the same finger or not, more similar to each other. Using a series of triangular with relatively small local deformation, while accumulated to huge global distortion, Kovács-Vajna [12] proposed a fingerprint verification method, which is able to cope with the strong deformation of fingerprint images. However, triangles with small deformation may make to an odd global deformation pattern, which is infeasible for genuine matching attempt but allows some possible for imposter's matching.

In this paper, we introduce a novel fingerprint verification algorithm based on the determination and inspection of the *registration pattern (RP)* between two fingerprints. The algorithm first coarsely aligns two fingerprints. Then determines the *possible RP* by optimally registered each part of the two fingerprints. Next, inspects the *possible RP* with a *genuine RP space*. If the *RP* makes a genuine one, a further fine matching is conducted. This paper is organized as follows. First, the feature representation and extraction method is introduced. Next, the matching algorithm is explained. Experimental result of the algorithm is given in Section 4. Section 5 contains the summary and discussion.

2 Feature Representation and Extraction

For an input fingerprint image, we use the method described in [1,2] to estimate the local orientation field *O*, enhance the image and get the thinned ridge map *T*. The thinned ridge map was post-processed using the method described in [14]. And then detect the minutiae set *M*. For each m_i belongs to *M*, we trace the associate ridges in *T* and record some sample points *P* with constant intervals. The minutia set and the sample points on the associate ridge provide information for both alignment and discrimination. The orientation field provides very good global information of a fingerprint. We choose these features to represent a fingerprint: *F=(M,P,O)*. An example of the feature set of a live-scan fingerprint is provided in Figure 1.

(a) input image (b) orientation field (c) ridge map

Fig. 1. Feature set of a live-scan fingerprint image. In some regions where minutiae are very sparse, the sample points on the associate ridges provide additional information for registration and discrimination

3 The Matching Algorithm

The matching algorithm has two stages. The offline, training stage presented in Section 3.3, derives a *genuine RP base* from a set of genuine matching attempts. The online matching stage is consisted of four sub-stages. First, the coarse registration presented in Section 3.1 aligns two fingerprints and finds the possible correspondence between the two feature sets. Second, the *RP* determination presented in Section 3.2 registers each portion of the fingerprint optimally and thus determinates the *RP*. Third, the *RP* inspection presented in Section 3.4 defines a *genuine RP space* and verifies whether a *possible RP* makes a genuine one. Fourth, the fine matching stage decides the correspondence of the two feature sets and gives a matching score.

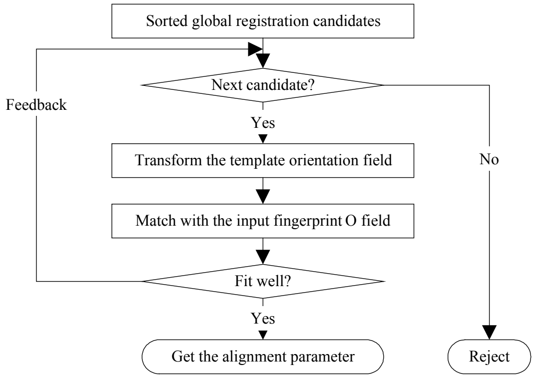

Fig. 2. Flowchart of the coarse registration with feedback

3.1 Coarse Global Registration with Feedback

The task of the coarse global registration is to align the two fingerprints and find the possible corresponding point pairs between the two feature sets. We revised the registration method described in [10] and introduce an *orientation field matching degree* feedback mechanism to improve the robustness of global alignment.

To estimate the registration parameter, we use the minutiae set to construct the local structure set: $\{Fl_1, Fl_2, \ldots, Fl_n\}$. Each local structure in the input fingerprint is compared with each local structure in the template fingerprint. Each comparison generates a registration parameter and a similarity score:

$$MFl_{p,q} = (Fl_p^t, Fl_q^i, (dx, dy, rot), s_{p,q}), \tag{1}$$

where the definition of the similarity score s_{pq} is the same with [11]. These comparisons give a possible correspondence list of feature points in two sets:

$$L_{corr} = \{(p_a^t, p_b^i, MFl_{p,q}) \mid p_a^t \in Fl_p^t, p_b^i \in Fl_q^i\}. \tag{2}$$

We cluster those registration parameters in $\{MFl_{p,q}\}$ into several candidate groups. Parameters in each group are averaged to generate a candidate global registration parameter. And the summation of similarity scores in each group becomes the power of each candidate registration parameter.

The candidate parameters are sorted by their power and verified one by one using the orientation field information to choose the best global registration parameter. Figure 2 shows the flowchart of this procedure.

3.2 Registration Pattern Determination

The next step is the determination of the *RP* that optimally registers each part of the two fingerprints. We take the input image as *"standard image"*, and register the template fingerprint, “a distorted image”, with respect to the standard one.

The feature set of the template fingerprint is first aligned with the input fingerprint using the global alignment parameter we get in the last step. Next, we tessellate the overlap portion of the input image into seven non-overlap hexagons with radius=R. Then, we compute the optimal alignment parameter of the template image with respect to each hexagon in the input image. The registration method is the same with that described in Section 3.1 except that: first, the searching space is greatly reduced, since the search region is restricted to the hexagon and its neighborhoods; second, sample points on the associate ridges are utilized to provide more information for registration. The possible correspondence list is extended by the possible correspondences of sampled feature points. We illustrate the orientation and type of the sample points in Figure 3.

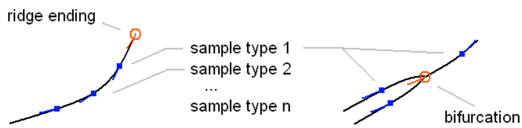

Fig. 3. Orientation and type of sample points on associate ridges

The registration parameters in a whole describe the *RP* between the two images:

$$RP = ((dx_1, dy_1, rot_1), (dx_2, dy_2, rot_2), \ldots, (dx_7, dy_7, rot_7)). \tag{3}$$

3.3 Learning Genuine Registration Patterns

Some fingerprints from different fingers may have similar flow patterns and many of their minutiae can be matched if we use a loose bounding box in order to allow the large distortion. However, when analyzed the two fingerprints in detail, we found that the *RP* was different from those from true matching.

To learn the *genuine RPs,* we used a set of distorted fingerprint images to derive a *genuine RP base (GRPB)*. This set of images was extracted from NIST Special DB24 [15]. The database contains 100 MPEG-2 compressed digital videos of live-scan fingerprint data. Users are required to place their finger on the sensor and distort their finger exaggeratedly once the finger touched the surface.

(a) template image (b) input image (c) registration pattern

Fig. 4. A *genuine RP* derived from a true matching attempt

We matched those images from same finger one to one and computed the *RPs*. These *RPs* formed our *GRPB*. In our experiment, we use seven fix-sized hexagons with R = 45 pixels. In most cases, they can cover most of the overlap portion. And the alignment parameters of these hexagons can well represent the whole *RP*. Figure 4 shows a *genuine RP* our algorithm derived from two images in NIST Special DB24.

3.4 Registration Pattern Inspection

We define the distance between two *RPs*:

$$d(RP_i, RP_j) = \sqrt[3]{\sum_k | dx_k^i - dx_k^j |^3 + | dy_k^i - dy_k^j |^3 + (R \times | rot_k^i - rot_k^j |} \quad (4)$$

.

And a genuine RP space:

$$S_{GRP} = \{RP \mid \exists RP_i \in GRPB, d(RP, RP_i) < Thr_{gspace}\} . \quad (5)$$

When we match fingerprints, each matching attempt generates a *possible RP*. If the *possible RP* belongs to S_{GRP}, a further fine matching is conducted. If not, the matching attempt is rejected. Figure 5 shows a *fake RP* our algorithm detected.

(a) template image (b) input image (c) registration pattern

Fig. 5. A *fake RP* our algorithm detected. The two fingerprints have some similarities in both minutiae and flow patterns. Inadequate contrast in the image stopped us from rejecting it in the stage of coarse global registration, though the two fingerprints in fact belong to different types

3.5 Fine Matching

This is the final matching step. From the list of possible corresponding point pairs refined in the stage of *RP* determination, each feature point in the overlap portion of the template fingerprint may have one or more corresponding feature points in the input fingerprint. The confliction of one feature point corresponding to more than one feature points can be solved by a simple rule: assign this feature point to the point which has the largest sum of similarity score with it. All the other correspondences are deleted. Then compute the matching score:

$$M = \frac{m}{\max(n_{input}, n_{template})} \times \sum s_i , \quad (6)$$

where m is the number of matching feature points, n_{input} and $n_{template}$ are the numbers of feature points in the overlap portion of the input fingerprint and template fingerprint respectively, and s_i is the similarity score in the final correspondence list.

4 Experiments and Results

We have tested our algorithm on the second FVC2002 database [16]. This database contains 880 optical 8-bit gray-scale fingerprint images (296×560 pixels), 8 prints of each of 110 fingers. The images are captured at 569 dpi. Noted that this resolution is different to the images in the NIST Special DB24, which were captured at 500dpi, we scaled the data in the *GRPB*. Each fingerprint in the test set was matched with the other fingerprints in the set. Therefore a total of $(880 \times 872)/2 = 383{,}680$ imposter's matching attempts and $(110 \times 8 \times 7)/2 = 3{,}080$ genuine matching attempts were tested. To examine the effectiveness of the *RP* inspection method, we computed matching scores of both with and without the *RP* inspection method. The ROC (Receiver Operating Characteristic) curve is shown in Figure 6. The equal error rate (EER) is observed to be ~ 0.51% and ~ 1.1% respectively.

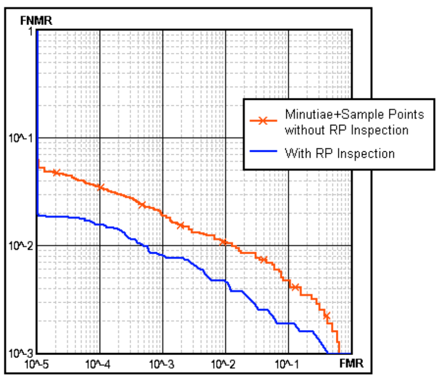

Fig. 6. ROC showing the effectiveness of the algorithm on the second FVC2002 database

5 Summary and Future Work

We have introduced a novel fingerprint verification algorithm based on the determination and inspection of the *RP* between two fingerprints. The coarse global registration with feedback is capable of aligning two fingerprints with very high accuracy and robustness. The inspection of *possible RP* successfully detected some dangerous imposter's matching attempts, which had similar flow pattern and minutiae configuration with the template images. Such cases are also the main reason for the high false matching rates (FMR) in traditional matching algorithms. Currently, a *possible RP* is inspected by one to one check with the *genuine RPs*. We are working on deriving a knowledge base from these patterns.

References

[1] A.K. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification", *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 19, no. 4, pp. 302-314, 1997.

[2] L. Hong, Y. Wan, and A. K. Jain, "Fingerprint image enhancement: algorithms and performance evaluation", *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 20, no. 8, pp.777-789, 1998.

[3] A.K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching", *IEEE Trans. on Image Processing*, vol. 9, no.5, pp. 846-859, 2000.

[4] Ross, A.K. Jain, and J. Reisman, "A hybrid fingerprint matcher", *Pattern Recognition*, 2003.

[5] R. Cappelli, D. Maio, and D. Maltoni, "Modelling plastic distortion in fingerprint images", in *Proc. ICAPR2001,* Rio de Janeiro, Mar. 2001.

[6] Asker M. Bazen and Sablih H. Gerez, "Elastic minutiae matching by means of thin-plate spline models", in *Proc. 16th ICPR*, Québec City, Canada, Aug. 2002.

[7] Senior and R. Bolle, "Improved fingerprint matching by distortion removal", *IEICE Trans. Inf. and Syst., Special issue on Biometrics*, E84-D (7): 825-831, Jul. 2001.

[8] N.K. Ratha and R.M. Bolle, "Effect of controlled acquisition on fingerprint matching", in *Proc. 14th ICPR,* Brisbane, Australia, Aug., 1998.

[9] Chitra Dorai, Nalini Ratha, and Ruud Bolle, "Detecting dynamic behavior in compressed fingerprint videos: Distortion", in *Proc. CVPR2000*, Hilton Head, SC., Jun. 2000.

[10] X. Jiang and W. Yau, "Fingerprint minutiae matching based on the local and global structures", in *Proc. 15th ICPR*, Barcelona, Spain, Sept. 2000.

[11] Kuo Chin Fan, Cheng Wen Liu, and Yuan Kai Wang, "A randomized approach with geometric constraints to fingerprint verification", *Pattern Recognition*, 33 pp. 1793-1803, 2000.

[12] Z.M. Kovács-Vajna, "A fingerprint verification system based on triangular matching and dynamic time warping", *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 22, no. 11, pp. 1266-1276, 2000.

[13] Yuliang He, Jie Tian, Xiping Luo, and Tanghui Zhang, “Image enhancement and minutia matching in fingerprint verification”, *Pattern Recognition Letter*, vol. 24/9-10, pp. 1349-1360, 2003.

[1] Xiping Luo and Jie Tian□"Knowledge based fingerprint image enhancement", in *Proc. 15th ICPR*, Barcelona, Spain, Sept. 2000.

[15] C.I. Watson, *NIST Special Database 24 Digital Video of Live-Scan Fingerprint Data*, U.S. National Institute of Standards and Technology, 1998.

[16] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, and A.K. Jain, "FVC2002: Second fingerprint verification competition", in *Proc.16th ICPR*, Québec City, Canada, Aug. 2002.