Automated Personal Authentication Using Both Palmprints

Xiangqian Wu[1], Kuanquan Wang[1], and David Zhang[2]

[1] School of Computer Science and Technology,
Harbin Institute of Technology (HIT), Harbin 150001, China
{xqwu, wangkq}@hit.edu.cn
[2] Biometric Research Centre, Department of Computing,
Hong Kong Polytechnic University, Kowloon, Hong Kong
csdzhang@comp.polyu.edu.hk

Abstract. To satisfy personal interests, different entertainment computing should be performed for different people (called personal entertainment computing). For personal entertainment computing, the personal identity should be first automatically authenticated. This paper proposes a novel approach for automated personal authentication by using both palmprints. The experimental results show that the fusion of the information of both palmprints can dramatically improve the authentication accuracy.

1 Introduction

The different people have different interests. To meet personal interests, different entertainment computing should be performed for different people (called personal entertainment computing). For example, the cyber pets should act different to meet different interests and the robots should provide different services to different people. To conduct personal entertainment computing, the personal identity should be first automatically authenticated. The palmprint is a relatively new biometric feature used for automated personal authentication [1–5]. Many algorithms have been developed for palmprint recognition in the last several years [4–6]. All of these algorithms only use sole palmprint of each person for authorization and the accuracies are not high enough to meet some applications. To improve the accuracy, this paper uses both palmprints of each person for authentication. In the following sections, the preprocessing technique described in [5] is used to crop the central part of the image, which is 128×128, for analysis.

2 Feature Extraction and Matching

Let I denote a palmprint image and G_σ denote a 2D Gaussian filter with the variance σ. The palmprint is first filtered by G_σ as below:

$$I_f = I * G_\theta \tag{1}$$

where $*$ is the convolution operator.

Then the difference of I_f in the horizontal direction is computed as following:

$$D = I_f * b \tag{2}$$

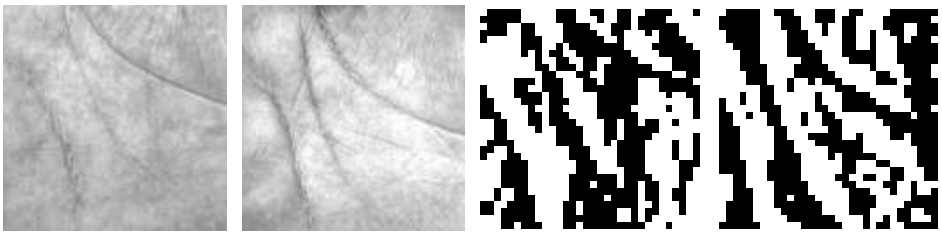
$$b = [-1, 1] \tag{3}$$

where $*$ is the convolution operator.

Finally, the palmprint is encoded according to the sign of each pixel of D:

$$C(i,j) = \begin{cases} 1, & \text{if } D(i,j) > 0; \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

C is called DiffCode of the palmprint I. The size of the preprocessed palmprint is 128×128. Extra experiments shows that the image with 32×32 is enough for the DiffCode extraction and matching. Therefore, before compute the DiffCode, we resize the image from 128×128 to 32×32. Hence the size of the DiffCode is 32×32. Fig. 1 shows some examples of DiffCode.



(a) (b) (c) (d)

Fig. 1. Some examples of DiffCodes. (a), (b) are the original palmprint and (c),(d) are their DiffCodes.

The matching score of two DiffCodes C_1 and C_2 is then defined as below:

$$S(C_1, C_2) = 1 - \frac{\sum_{i=1}^{32} \sum_{j=1}^{32} (C_1(i,j) \otimes C_2(i,j))}{32 \times 32} \tag{5}$$

Actually, $S(C_1, C_2)$ is the percentage of the places where C_1 and C_2 have the same values. Obviously, $S(C_1, C_2)$ is between 0 and 1 and the larger the matching score, the greater the similarity between C_1 and C_2. The matching score of a perfect match is 1. Because of imperfect preprocessing, there may still be a little translation between the palmprints captured from the same palm at different times. To overcome this problem, we vertically and horizontally translate C_1 a few points to get the translated C_1^T , and then, at each translated position, compute the matching score between C_1^T and C_2. Finally, the final matching score is taken to be the maximum matching score of all the translated positions.

3 Score Fusion

Denote x_1 and x_2 as the scores obtained from the left palmprints matching and right palmprints matching between two persons, respectively. To obtain the final matching score x, we fuse these two scores by following simple strategies, which need not any prior knowledge or training.

S_1: Maximum Strategy:

$$x = \max(x_1, x_2) \tag{6}$$

S_2: Minimum Strategy:

$$x = \min(x_1, x_2) \tag{7}$$

S_3: Product Strategy:

$$x = \sqrt{x_1 x_2} \tag{8}$$

S_4: Sum Strategy:

$$x = \frac{x_1 + x_2}{2} \tag{9}$$

4 Experimental Results And Analysis

We employed the PolyU Palmprint Database [7] to test our approach. This database contains 7752 grayscale images captured from 386 different palms by a CCD-based device. From this database, we can get 3701 pairs (right and left) of palmprints captured from 193 different persons to test the approach.

4.1 Difference Between Left and Right Palmprints

To fuse the features of both palmprint, we should investigate the difference between them. If the palmprints from the right and left hands of same persons are very similar, the fusion cannot improve the performance much. To investigate this, two types of matching are conducted on the database: 1) Each palmprint is matched against all of the palmprints from different persons; 2) Each left palmprint is matched against the right palmprints of the same person. The score distributions of these two types of matchings are plotted in Fig. 2. This figure shows that the difference between the right and left palmprints of the same persons is close to that of the palmprints from different persons. Hence, the left and right palmprints of the same person are independent. So they can be fused to improve the authentication accuracy.

4.2 Accuracy Tests

To evaluate the accuracies of the different fusion strategies, each pair of palmprints in the database is matched with the other pairs. The ROC curve of each strategy is plotted in Fig. 3 and the EER of them are listed in Table 1. This figure and table also demonstrate that each fusion strategy can improve the authentication accuracy. The Sum and Product strategies are the best ones, which can decrease the EER from about 0.2% (left palmprints) or 0.3% (right palmprints) to 0.03%.

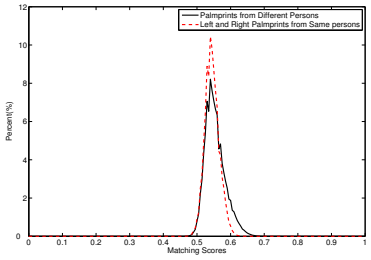


Fig. 2. The matching score distributions

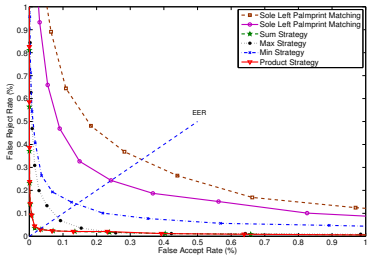


Fig. 3. ROC curves of different strategies

Table 1. EER of different strategies

Strategy	Sole Left Palmprint	Sole Right Palmprint	Sum	Maximum	Minimum	Product
EER	0.326%	0.243%	0.0319%	0.080%	0.137%	0.0313%

5 Conclusions

For conducting personal entertainment computing, this paper authenticates people automatically using palmprints of both hand, which can dramatically improve the authentication accuracy.

Acknowledgements

This work is partially supported by the NSFC (No. 60441005), the Key-Project of the 11th-Five-Year Plan of Educational Science of Hei Longjiang Province, China (No. HZG160), the Science and Technology Project of the Education Department of Hei Longjiang Province (No. 11523026) and the Development Program for Outstanding Young Teachers in Harbin Institute of Technology.

References

1. Zhang, D.: Palmprint Authentication. Kluwer Academic Publishers (2004)
2. Wu, X., Zhang, D., Wang, K.: Palmprint Recognition. China: Scientific Publishers (2006)
3. Duta, N., Jain, A., Mardia, K.: Matching of palmprint. Pattern Recognition Letters **23** (2001) 477–485
4. Han, C., Chen, H., Lin, C., Fan, K.: Personal authentication using palm-print features. Pattern Recognition **36** (2003) 371–381
5. Zhang, D., Kong, W., You, J., Wong, M.: Online palmprint identification. IEEE Transactions on Pattern Analysis and Machine Intelligence **25** (2003) 1041–1050
6. Wu, X., Wang, K., Zhang, D.: Palm-line extraction and matching for personal authentication. IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans **36** (2006) 978–987
7. PolyU Palmprint Palmprint Database. (http://www.comp.polyu.edu.hk/∼biometrics/)