Jan. 2005, Vol.20, No.1, pp.70–76 J. Comput. Sci. & Technol.

Online Palmprint Identification System for Civil Applications

David Zhang[1], Guang-Ming Lu[2], Adams Wai-Kin Kong[1,3], and Michael Wong[1]

[1] *Biometrics Research Centre, Department of Computing, The Hong Kong Polytechnic University, Kowloon Hong Kong Special Administrative Region, P.R. China*

[2] *Biocomputing Research Lab, School of Computer Science and Engineering, Harbin Institute of Technology Harbin 150001, P.R. China*

[3] *Department of Systems Design Engineering, University of Waterloo, Ontario, N2L 3G1 Canada*

E-mail: {csdzhang, csglu, cswkkong, csmkwong}@comp.polyu.edu.hk; Luguangm@hit.edu.cn

Received May 21, 2004; revised July 30, 2004.

Abstract In this paper, a novel biometric identification system is presented to identify a person's identity by his/her palmprint. In contrast to existing palmprint systems for criminal applications, the proposed system targets at the civil applications, which require identifying a person in a large database with high accuracy in real-time. The system is constituted by four major components: *User Interface Module, Acquisition Module, Recognition Module* and *External Module*. More than 7,000 palmprint images have been collected to test the performance of the system. The system can identify 400 palms with a low false acceptance rate, 0.02%, and a high genuine acceptance rate, 98.83%. For verification, the system can operate at a false acceptance rate, 0.017% and a false rejection rate, 0.86%. The execution time for the whole process including image collection, preprocessing, feature extraction and matching is less than 1 second.

Keywords palmprint identification, biometrics, personal authentication

1 Introduction

Biometrics involves identifying an individual based on his/her physiological or behavioral characteristics. Many parts of our body and various behaviors are embedded such information for personal identification. In fact, using biometrics for person authentication is not new, which has been implemented over thousands years, numerous research efforts have been put on this subject resulting in developing various techniques related to signal acquisition, feature extraction, matching and classification. Most importantly, various biometric systems including, fingerprint, iris, hand geometry, voice and face recognition systems have been deployed for various applications[1]. According to the International Biometric Group (IBG, New York), the market for biometric technologies will nearly double in size this year alone. Among all biometrics, hand-based biometrics, including hand geometry and fingerprint are the most popular biometrics gaining 60% market share in 2003[2].

The proposed palmprint system is also a hand-based biometric technology. Palmprint is concerned with the inner surface of a hand and looks at line patterns and surface shape. A palm is covered with the same kind of skin as the fingertips and it is larger than a fingertip in size. Therefore, it is quite natural to think of using palmprint to recognize a person, like fingerprint, hand geometry and hand vein[3−6]. Because of the rich features including texture, principal lines and wrinkles on palmprints, we believe that they contain enough stable and distinctive information for separating an individual from a large population. We also expect that palmprints are robust to the noise because of the large surface area.

There have been some companies, including NEC and PRINTRAK, which have developed several palmprint systems for criminal applications[7,8]. On the basis of fingerprint technology, their systems exploit high resolution palmprint images to extract the detailed features like minutiae for matching the latent prints. Such approach is not suitable for developing a palmprint authentication system for civil applications, which requires a fast, accurate and reliable method for the personal identification. Based on our previous research work[9], we develop a novel palmprint authentication system to fulfill such requirements.

The rest of the paper is organized as follows. The system framework is shown in Section 2. The recognition engine is described in Section 3. Experimental results of verification, identification, robustness, and computation time are provided in Section 4. Finally, conclusion is given in Section 5.

2 System Framework

The proposed palmprint authentication system has four major components: they are *User Interface Module*, *Acquisition Module*, *Recognition Module* and *External Module*. Fig.1 shows the breakdown of each module of the palmprint authentication system. Fig.2 shows the palmprint authentication system installed at Biometric Research Center, Department of Computing, The Hong Kong Polytechnic University. The functions of each component are listed below:

*Regular Paper

This research is partially supported by the UGC/CRC fund from the Hong Kong SAR Government and the central fund from The Hong Kong Polytechnic University.

A) *User Interface Module* provides an interface between the system and users for the smooth authentication operation. We designed a flat platen surface for the palm acquisition (Fig.2). It is crucial to develop a good user interface such that users are happy to use the device.

B) *Acquisition Module* is the channel for the palmprints to be acquired for the further processing.

C) *Recognition Module* is the key part of our system, which will determine whether a user is authenticated. It consists of image pre-processing, feature extraction, template creation, database updating, and matching. Then it gives an identification/verification result.

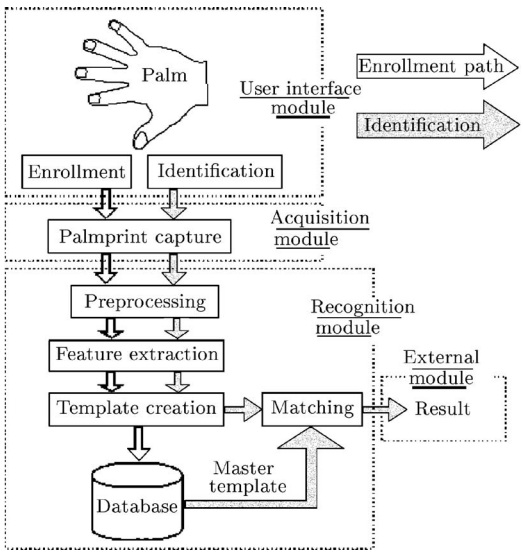

Fig.1. Breakdown of each module of the palmprint authentication system.

Fig.2. Palmprint authentication system installed at Biometrics Research Center, The Hong Kong Polytechnic University.

D) *External Module* receives the signal come from the recognition module, to allow some operations to be performed, or denied the operations requested. This module actually is an interfacing component, which may be connected to another hardware components or software components. Our system presents an external interface for physical door access control or an employee attendance system.

Since the design philosophy and implementation of the user interface module and the acquisition module have been described in [9], and the external interface is an application dependent component. In this paper, we are not intended to discuss them further, and we will concentrate on the discussion about the recognition module in detail.

3 Recognition Engine

After the palmprint images are captured by the Acquisition Module, they are fed into the recognition engine for palmprint authentication. The recognition engine is the key part of the palmprint authentication system, which consists of the stages of: image preprocessing, feature extraction, and matching.

3.1 Image Preprocessing

When capturing a palmprint, the position, direction and stretching degree may vary from time to time. As a result, even the palmprints from the same palm could have a little rotation and translation. Also the sizes of palms are different from one another. So, the preprocessing algorithm is used to align different palmprints and extract the corresponding central part for feature extraction[10]. In our palmprint system, both the rotation and translation are constrained to some extent by the capture device panel, which can locate the palms by several pegs. Then the preprocessing algorithm can locate the coordination system of the palmprints quickly by the following five steps.

Step 1. Use a threshold to convert the original grayscale image into a binary image, then using a low-pass filter to smooth the binary image.

Step 2. Trace the boundary of the holes $H1$ and $H2$ between those fingers.

Step 3. Compute the tangent of the holes $H1$ and $H2$. $T1$ and $T2$ are the tangent points of $H1$ and $H2$, respectively.

Step 4. Align $T1$ and $T2$ to determine the Y-axis of the palmprint coordination system and making a line passing through the midpoint of the two points ($T1$ and $T2$), which is perpendicular to this Y-axis to determine the origin of the system.

Step 5. Extract a sub-image of a fixed size based on the coordinate system (see Fig.3). The sub-image is located at a certain area of the palmprint image for feature extraction.

3.2 Feature Extraction

The feature extraction technique implemented on the proposed palmprint system is modified from [9], where single circular zero DC Gabor filter is applied to the preprocessed palmprint images and the phase information is coded as feature vector called PalmCode. The modified technique exploited four circular zero DC Gabor filters

with the following general formula

$$G_D = \frac{1}{2\pi\sigma^2}\exp\left\{-\frac{1}{2}\left[\frac{(x'-x_o)^2}{\sigma^2}+\frac{(y'-y_0)^2}{\sigma^2}\right]\right\} \cdot\{\exp(i2\pi\omega x')-\exp(-2\pi^2\omega^2\sigma^2)\}, \quad (1)$$

where $x' = x\cos\theta + y\sin\theta$ and $y' = -x\sin\theta + y\cos\theta$; (x_0, y_0) is the center of the function in the spatial domain of the function; ω is the frequency of the sinusoidal plane wave along the orientation, θ; σ is the standard deviations of the circular Gaussian function; θ is the direction of the filter. The four Gabor filters share the same parameters, σ and ω, only different in θ. The corresponding values of θ are 0, $\pi/4$, $\pi/2$ and $3\pi/4$.

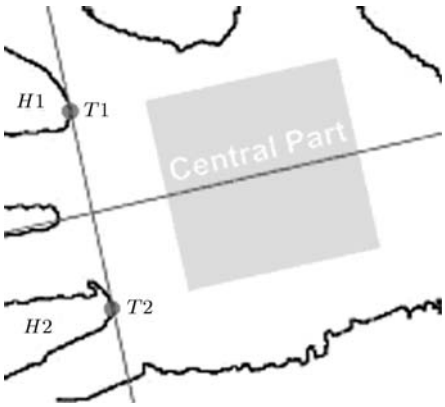

Fig.3. Major steps on palmprint preprocessing: $H1$ and $H2$ are boundary of the holes between the two fingers, where $T1$ and $T2$ are the tangent point of $H1$ and $H2$, respectively. The central box is the sub-image of a palm.

In the previous approach, only the phase information is exploited but the magnitude information is totally neglected. The proposed method is to use the magnitude to be a fusion condition to combine different PalmCodes generated by the four Gabor filters. Mathematically, the implementation has the following steps.

1) The four Gabor filters are applied to the preprocessed palmprint image, I described as $G_j * I$, where G_j $(j = 1, 2, 3, 4)$ is the circular zero DC Gabor filter and "$*$" represents an operator of convolution.

2) The square of the magnitudes of the sample point is obtained by $M_j(x, y) = G_j(x, y) * I \times \overline{G_j(x, y) * I}$, where "$-$" represents complex conjugate.

3) According to the fusion rule, $k = \arg\max_j(M_j(x, y))$, the phase information at point (x, y) is coded as the following

$$h_r = 1 \text{ if } \mathrm{Re}[G_k * I] \geqslant 0 \quad (2)$$

$$h_r = 0 \text{ if } \mathrm{Re}[G_k * I] < 0 \quad (3)$$

$$h_i = 1 \text{ if } \mathrm{Im}[G_k * I] \geqslant 0 \quad (4)$$

$$h_i = 0 \text{ if } \mathrm{Im}[G_k * I] < 0. \quad (5)$$

This coding method is named as Fusion Code, which is represented by a set of bits. Our experiments show that the Fusion Code is more stable and efficient for palmprint authentication.

3.3 Feature Matching

The feature matching determines the degree of similarity between two templates — the identification template and the master template. In this paper, the normalized hamming distance is implemented for comparing two Fusion Codes. The normalized hamming distance is represented by

$$D_o = \Big[\sum_{i=1}^{N}\sum_{j=1}^{N} P_M(i,j)\cap Q_M(i,j)\cap ((P_R(i,j)\otimes Q_R(i,j) + P_I(i,j)\otimes Q_I(i,j)))\Big]\cdot \Big[2\sum_{i=1}^{N}\sum_{j=1}^{N} P_M(i,j)\cap Q_M(i,j)\Big]^{-1}, \quad (6)$$

where $P_R(Q_R)$, $P_I(Q_I)$ and $P_M(Q_M)$ are the real part, imaginary part and mask of the Fusion Code $P(Q)$, respectively; $\otimes$ and $\cap$ are Boolean operators, XOR and AND, respectively[9]. The ranges of normalized hamming distances are between zero and one. Zero represents perfect matching. Because of the imperfect preprocessing, one of the Fusion Code is vertically and horizontal translated to match the other again. The ranges of the vertical and the horizontal translations are defined from -2 to 2. The minimum D_0 value obtained from the translated matching is considered to be the final matching score.

4 Performance Evaluation

4.1 Testing Database

We collected palmprint images from 200 individuals using our palmprint capture device described in [9]. The subjects are mainly students and staff volunteers from The Hong Kong Polytechnic University. In this dataset, 134 people are male, and the age distribution of the subjects is: about 86% are younger than 30, about 3% are older than 50, and about 11% are aged between 30 and 50. In addition, we collected the palmprint images on two separate occasions. On each occasion, the subject was asked to provide about 10 images each of the left palm and the right palm. Therefore, each person provided around 40 images, resulting in a total number of 8,025 images from 400 different palms in our database. In addition, we changed the light source and adjusted the focus of the CCD camera so that the images collected on the first and second occasions could be regarded as being captured by two different palmprint devices. The average time interval between the first and second occasions was 70 days. The size of all the testing images used in the following experiments is 384×284 with 75dpi, in 256 gray levels.

4.2 Experimental Results of Verification

Verification refers to the problem of confirming or denying a claim of individuals. It is also considered as one to one matching. To obtain the verification result, two group experiments are carried out separately. In the first experiment, only one palmprint image of each palm is used for registration, while 3 palmprint images of each palm are used for registration in the second experiment. In the first experiment, each palmprint image is matched with all other palmprint images in the database. A correct matching occurs if two palmprint images are from the same palm, incorrect matching otherwise. The total number of matching is 32,119,735. Number of genuine matching is 76,565 and the rest of them are incorrect matchings. Fig.4(a) shows the probability of genuine and imposter distributions estimated by the correct and incorrect matchings. Some thresholds and corresponding false acceptance rates (FARs) and false rejection rates (FRRs) are listed in Table 1. According to Table 1, using one palmprint image for registration, the proposed system can be operated at a low false acceptance rate 0.096% and a reasonably low false rejection rate 1.05%.

Table 1. FARs and FRRs with Different Threshold Values for the Palmprints Verification Results

Threshold	Registered image=1		Registered images=3	
	FAR (%)	FRR (%)	FAR (%)	FRR (%)
0.32	0.000027	8.15	0.000012	5.12
0.34	0.00094	4.02	0.0016	2.18
0.36	0.011	1.94	0.017	0.86
0.38	0.096	1.05	0.15	0.43
0.40	0.68	0.59	1.03	0.19

In the second experiment, the testing database is divided into two databases, 1) registration database and 2) testing database. Three palmprint images of each palm collected in the first occasion are selected for the registration database. Totally, the registration database contains 1,200 palmprint images and the rest of them are for the testing database. In this verification test, each palmprint image is matched with all the palmprint images in the testing database. Therefore, each testing image produces three hamming distances for one registered palm. We take the minimum of them as the final hamming distance. For achieving statistically reliable results, this test is repeated for three times by selecting other palmprint images for the registration database. Total number of hamming distances from correct matchings and incorrect matchings are 20,475 and 8,169,525, respectively. Fig.4(b) shows the probability of genuine and imposter distributions estimated by the correct and incorrect matchings, respectively. Some threshold values along with its corresponding false acceptance and false rejection rates are also listed in Table 1. According to Table 1 and Fig.4, we can conclude that using three templates can provide better verification accuracy. In fact, using more palmprint images of the same palm during registration can provide more information to the system so that it can recognize the noise or deformed features. It is also the reason for commercial verification systems requiring more than one sample for registration.

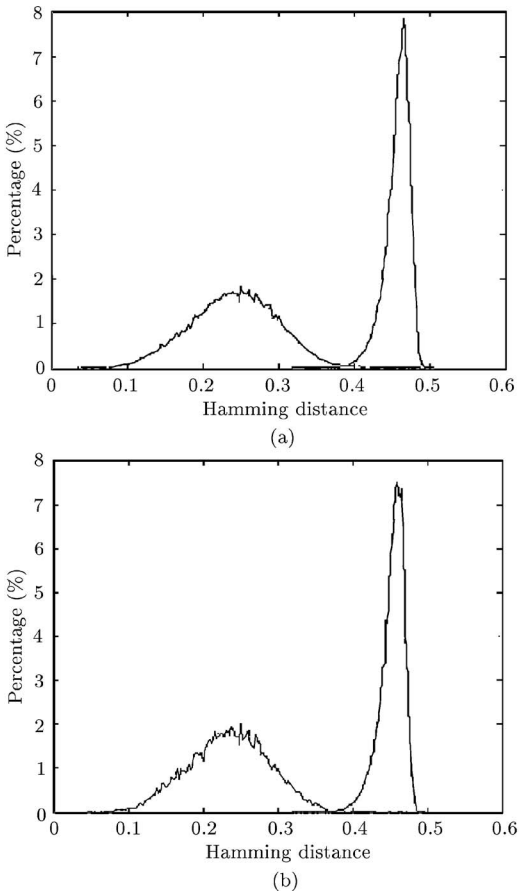

Fig.4. Verification test results. (a) and (b) show the Genuine and imposter distributions for verification tests with one and three registered images per palm, respectively.

4.3 Experimental Results of Identification

Identification test is a one-against-many, N comparison process. In this experiment, N is set to 400, which is the total number of different palms in our database. Same as the previous verification experiment, the palmprint database is divided into two databases, 1) registration and 2) testing databases. The registration database contains 1,200 palmprint images, three images per palm. The testing database has 6,825 palmprint images. Each palmprint image in the testing database is matched to all of the palmprint images in the registration database. Therefore, each testing image generates 3 correct and 1,197 incorrect matchings. The minimum hamming distances of correct matchings and incorrect matchings are regarded as the identification hamming distances of genuine and impostor, respectively. This experiment is also called a one-trial test since the user only provides one palmprint image in the test to make one decision. In fact, a practical biometric system collects several biometric signals to make one decision. Therefore, in this experiment, we implement one-, two-, and three-trial tests.

In the two-trial test, a pair of palmprint images in the testing database belongs to the same palm is matched to all of the palmprint images in the registration database. Each pair of the palmprint images in the two-trial test generates 6 correct and 2,394 incorrect matchings. The minimum hamming distances of correct matchings and incorrect matchings are considered as the identification hamming distances of genuine and imposter, respectively. Similarly, in the three-trial test, the identification hamming distances of genuine and imposter are obtained from 9 correct and 3,591 incorrect matchings, respectively. Each test is repeated three times by selecting other palmprints from the registration database. In each test, the number of identification hamming distances of genuine and imposter matchings both are 20,475. Fig.5 shows ROC curves of the three tests and Table 2 lists the threshold values along with its corresponding FARs and FRRs of the tests. According to Fig.5 and Table 2, more input palmprints can provide more accurate results.

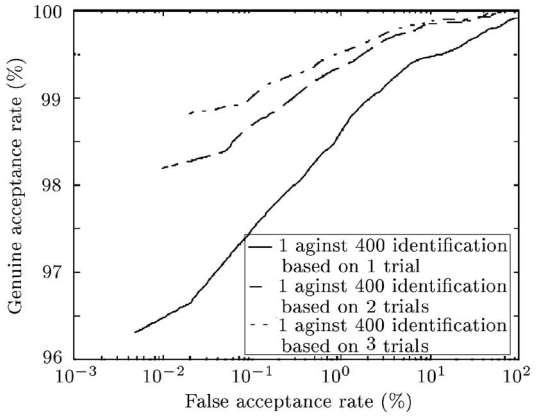

Fig.5. ROC curves for a 1-against-400 identification testing with different numbers of trials.

Table 2. FARs and FRRs with Different Threshold Values for the 1-to-400 Palmprints Identification Results

Threshold	Trial=1		Trial=2		Trial=3	
	FAR (%)	FRR (%)	FAR (%)	FRR (%)	FAR (%)	FRR (%)
0.320	0.0049	3.69	0.0098	1.80	0.020	1.17
0.325	0.0439	2.93	0.088	1.34	0.131	1.06
0.330	0.15	2.29	0.28	1.02	0.42	0.68
0.335	0.37	1.90	0.68	0.72	0.96	0.48
0.340	0.84	1.51	1.43	0.57	1.93	0.37
0.345	1.45	1.16	2.32	0.42	3.02	0.26

4.4 Computation Time

Another key issue for a civilian personal identification system is whether the system can run in real time. In other words, the system should be running as fast as possible. The proposed method is implemented using C language and Assemble language on a PC embedded Intel Pentium IV processor (1.4GHz) with 128MB memory. The execution time for image collection, image preprocessing, feature extraction and matching are listed in Table 3. The total execution time for a 1-against-400 identification, each palm with 3 templates, is less than 1 second. Users will not feel any delay when using our system.

Table 3. Execution Time of the Palmprint Authentication System

Operations	Execution time
Image collection	340ms
Preprocessing	250ms
Feature extraction	180ms
Matching	1.3μs

4.5 Robustness

As a practical biometric system, other than accuracy and speed, robustness of the system is another important issue. Here, we present three experiments to illustrate the robustness of our system. The first one is an individual's jewelry such as rings, which may influence the accuracy of some preprocessing algorithms. The second one is the noise on the palmprints, which directly affect the performance of the system. The third is the ability of identifying the identity of identical twins' palmprints.

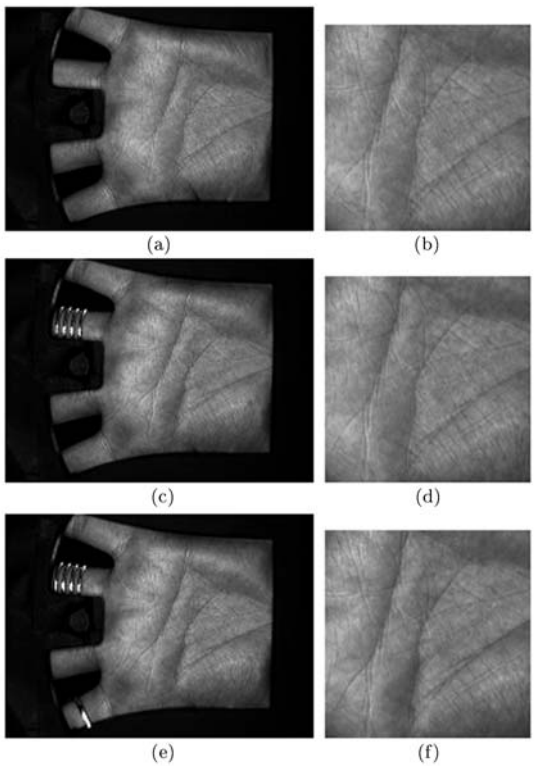

Fig.6. Palmprint images with ring on the fingers for testing the robustness of the system.

Fig.6 shows three palmprint images with and without rings on the fingers and their corresponding preprocessed sub-images. It shows that the preprocessing algorithm described in Section 3 is not affected by the rings. However, some preprocessing algorithms such as using such information may not be stable under the influence of the rings.

To verify the robustness of noise palmprints, Fig.7(a) provides a clear palmprint image and Figs.7(b)–7(f) show five palmprint images, with different texts. Their hamming distances are given in Table 4; all of them are smaller than 0.29. Comparing the hamming distances of imposter in Table 1 and Table 2, it is ensured that all the hamming distances in Table 4 are relatively small. Fig.7 and Table 4 illustrates that the proposed palmprint authentication system is very robust to the noise on the palmprint.

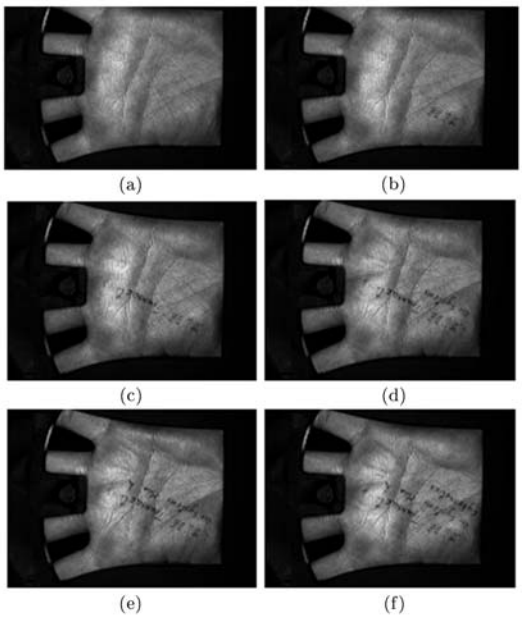

Fig.7. Palmprint images with different texts for testing the robustness of the system.

Table 4. Hamming Distances of Fig.7

Figs.	7(b)	7(c)	7(d)	7(e)	7(f)
7(a)	0.19	0.21	0.27	0.29	0.28
7(b)		0.18	0.27	0.26	0.27
7(c)			0.27	0.28	0.28
7(d)				0.23	0.19
7(e)					0.19

A test of identical twins is regarded as an important test for biometric authentication, but not all biometrics, including face and DNA, can pass this test. However, the palmprints of identical twins have enough distinctive information to distinguish them. We collected 590 palmprint images from 30 pairs of identical twins' palms. Each of them provides around 10 images of their left palms and 10 images of their right palms. Their age range is between 6 and 45 years old. Some samples of identical twins' palmprints are shown in Fig.8. Based on this database, we match a palmprint in the twin database with his/her identical twin sibling to produce imposter matching scores, and match the samples of their own to get the genuine scores. The genuine and imposter distributions are given in Fig.9. From the figure, we can find that identical twins' palmprint can easily be separated, just like twins' fingerprints[10].

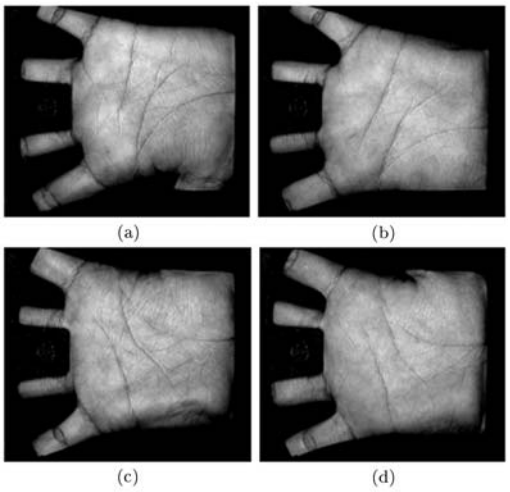

Fig.8. Identical twins' palmprints. (a), (b) are their left hands, and (c), (d) are their right hands, respectively.

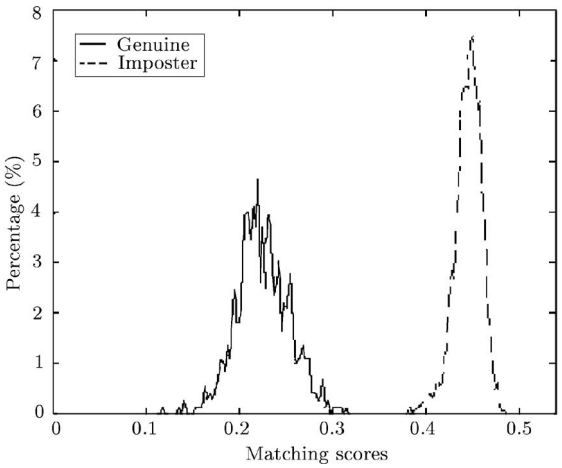

Fig.9. Genuine and imposter distributions for measuring the similarity of identical twins' palmprints.

5 Conclusion

In this paper, we have presented a novel biometric system based on the palmprint. The proposed system can accurately identify a person in real time, which is suitable for various civil applications such as access control. Experimental results show that the proposed system can identify 400 palms with a low false acceptance rate, 0.02%, and a high genuine acceptance rate, 98.83%. For verification, the system can operate at a false acceptance rate, 0.017% and a false rejection rate, 0.86%. The experimental results including accuracy, speed and robustness demonstrate that the palmprint authentication

system is comparable with other hand-based biometrics systems, such as hand geometry and fingerprint verification system[11,12] and is practical for real-world applications. The system has been installed at the Biometrics Research Center, Department of Computing, The Hong Kong Polytechnic Univ. since March 2003 for access control.

References

[1] Jain A, Bolle R, Pankanti S (eds.). Biometrics: Personal Identification in Networked Society. Boston, Mass: Kluwer Academic Publishers, 1999.

[2] International Biometric Group's Biometric Market Report 2003–2007. http://www.biometricgroup.com/reports/public/market_report.html

[3] Sanchez-Reillo R, Sanchez-Avilla C, Gonzalez-Marcos A. Biometric identification through hand geometry measurements. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2000, 22(10): 1168–1171.

[4] Im S K, Park H M, Kim Y W *et al.* An biometric identification system by extracting hand vein patterns. *Journal of the Korean Physical Society*, 2001, 38(3): 268–272.

[5] Jain A, Hong L, Bolle R. On-line fingerprint verification. *IEEE Trans. PAMI*, 1997, 19(4): 302–314.

[6] Jain A K, Ross A, Prabhakar S. An introduction to biometric recognition. *IEEE Trans. Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics*, 2004, 14(1): 4–20.

[7] NEC automatic palmprint identification system. http://www.nectech.com/afis/download/PalmprintDtsht.q. pdf

[8] Prinkrak palmprint identification system. http://www.printrakinternational.com/omnitrak.htm

[9] Zhang D, Kong W K, You J, Wong M. On-line palmprint identification. *IEEE Trans. PAMI*, 2003, 25(9): 1041–1050.

[10] Jain A K, Prabhakar S, Pankanti S. On the similarity of identical twin fingerprints. *Pattern Recognition*, 2002, 35(11): 2653–2662.

[11] Jain A K, Prabhakar S, Hong L, Pankanti S. Filterbank-based fingerprint matching. *IEEE Trans. Image Processing*, 2000, 9(5): 846–859.

[12] Sanchez-Reillo R, Sanchez-Avilla C, Gonzalez-Marcos A. Biometric identification through hand geometry measurements. *IEEE Trans. PAMI*, 2000, 22(18): 1168–1171.

David Zhang graduated in computer science from Peking University in 1974. In 1983 he received his M.Sc. degree in computer science and engineering from the Harbin Institute of Technology (HIT) and then in 1985 his Ph.D. degree from the same institution. In 1994 he received his second Ph.D. degree in electrical and computer engineering from the University of Waterloo, Ontario, Canada. Prof. Zhang is currently with The Hong Kong Polytechnic University (PolyU), where he is the Founding Director of the Biometrics Technology Centre (UGC/CRC) (www4.comp.polyu.edu.hk/~biometrics/), a body supported by the Hong Kong SAR Government. He also serves as Adjunct Professor in Tsinghua Univ., Shanghai Jiaotong Univ., Harbin Institute of Technology, and the Univ. Waterloo. Prof. Zhang's research interests include automated biometrics-based authentication, pattern recognition, and biometric technology and systems. He is the Founder and Editor-in-Chief, International Journal of Image and Graphics (IJIG); Book Editor, Kluwer International Series on Biometrics (KISB); and Associate Editor of more than ten international journals including IEEE Trans. SMC-A/SMC-C, Pattern Recognition. He is the author of more than 130 journal papers, twenty book chapters and ten books. As a principal investigator, he has since 1980 brought to fruition many biometrics projects and won numerous prizes. Prof. Zhang holds a number of patents in both USA and China and is a current Croucher Senior Research Fellow.

Guang-Ming Lu graduated from HIT in electrical engineering in 1998, where he also obtained his M.Sc. degree in control theory and control engineering in 2000. He is pursuing the Ph.D. degree in the Dept. Computer Science and Engineering of HIT since 2000. He is currently a lecturer in the Biocomputing Research Lab., School of Computer Science and Engineering, HIT. His research interests include pattern recognition, image processing, and automated biometrics technologies.

Adams Wai-Kin Kong received his B.Sc. degree in mathematics from Hong Kong Baptist Univ. with first class honors and obtained his M.Phil. degree from PolyU. Currently, he is a Ph.D. candidate at Univ. Waterloo. During his study, he received several awards and scholarships from the universities, including Scholastic Award, Tuition Scholarships for Research Postgraduate Studies and International Graduate Student Award. In 2003, based on his palmprint identification algorithm, he was selected as a finalist of young inventor awards organized by Far Eastern Economic Review, who was the only one finalist from Hong Kong. His research interest includes biometrics, pattern recognition, image processing and neural network.

Michael Wong received his M.Phil. from the Dept. Computing, PolyU in 2004. He received the B.A. (Hons.) degree in computing from PolyU in 2001 with first class honors, and was awarded The Reuter Foundation Scholarship in 2001. During his study at the Kwai Chung Technical Institutes, he received the CMA & Donors Scholarship Award and The Chiap Hua Cheng's Foundation Scholarship in 1996 and 1997, respectively. He was one of the group leaders in the Preferred Graduate Development Programme (PGDP 2000), organized by PolyU, and was awarded the Certificate of Achievement for his outstanding leadership and contributions to the PGDP 2000. In his M.Phil. study, he received a two-year Tuition Scholarship for Research Postgraduate Studies awarded by PolyU. His research interest includes biometrics, pattern recognition, and image processing.