A Novel Personal Authentication System Using Palmprint Technology

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

[1] Biometric Research Centre, Department of Computing,
The Hong Kong Polytechnic University, Kowloon, Hong Kong
{csdzhang, csmkwong}@comp.polyu.edu.hk
http://www.comp.polyu.edu.hk/~biometrics
[2] Biocomputing Research Lab,
School of Computer Science and Engineering,
Harbin Institute of Technology, Harbin, China
Luguangm@hit.edu.cn
[3] Electrical and Computer Engineering,
University of Waterloo, Ontario, Canada N2L 3G1
adamskong@ieee.org

Abstract. In recent times, an increasing, worldwide effort has been devoted to the development of automatic personal identification systems that can be effective in a wide variety of security contexts. Palmprints have a number of unique advantages: they are rich in features such as principal lines, wrinkles, and textures and these provide stable and distinctive information sufficient for separating an individual from a large population. In this paper, we present a novel biometric authentication system to identify a person's identity by his/her palmprint. Being a robust and reliable system, it was tested by more than 8,000 palmprint images with very low false acceptance rate (0.02%), and a relative high genuine acceptance rate (98.83%). The whole authentication process is less than 1 second. Finally, some possible applications are discussed which could be benefited by using palmprint technology.

1 Introduction

Personal authentication plays a critical role in our society. e-Commerce applications such as e-Banking or security applications such as building entrance demand fast, real time, and accurate personal identification. Knowledge-based approaches use "something that you know" (such as passwords and personal identification numbers [1]) for personal identification; token-based approaches, on the other hand, use "something that you have" (such as passports or credit cards) for the same purpose. Tokens (e.g. credit cards) are time consuming and expensive to replace. These approaches are not based on any inherent attribute of an individual in the identification process made them unable to differentiate between an authorized person and an impostor who fraudulently acquires the "token" or "knowledge" of the authorized person. This is why biometrics identification or verification system started to be more focused in the recent years. Various biometric systems including, fingerprint, iris, hand geometry, voice and face recognition systems have been deployed for various applications [1].

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

S.K. Pal et al. (Eds.): PReMI 2005, LNCS 3776, pp. 147 – 156, 2005.

larger than a fingertip in size. Therefore, it is quite natural to think of using palmprint to recognize a person, which receives a high user acceptance rate, similar to that of the fingerprint, hand geometry and hand vein [2-5]. Because of the rich features including texture, principal lines and wrinkles on palmprints, they contain enough stable and distinctive information for separating an individual from a large population.

There have been some companies, including NEC and PRINTRAK, which have developed several palmprint systems for criminal applications [6-7]. 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 [8-9], we develop a novel palmprint authentication system to fulfill such requirements.

The rest of the paper is organized as follows. The system design and analysis is shown in Section 2. The recognition module is described in Section 3. Experimental results of verification, identification, and robustness are provided in Section 4. Some possible applications of personal authentication using palmprints are revealed in Section 5, and finally conclusions are given in Section 6.

2 System Design and Analysis

2.1 System Design

The schematic diagram of the proposed system is shown in Fig. 1. There is a user interface for the input of the palm. Inside our system, there are various components including a flat platen surface, lighting unit, CCD camera, A/D converter, processing

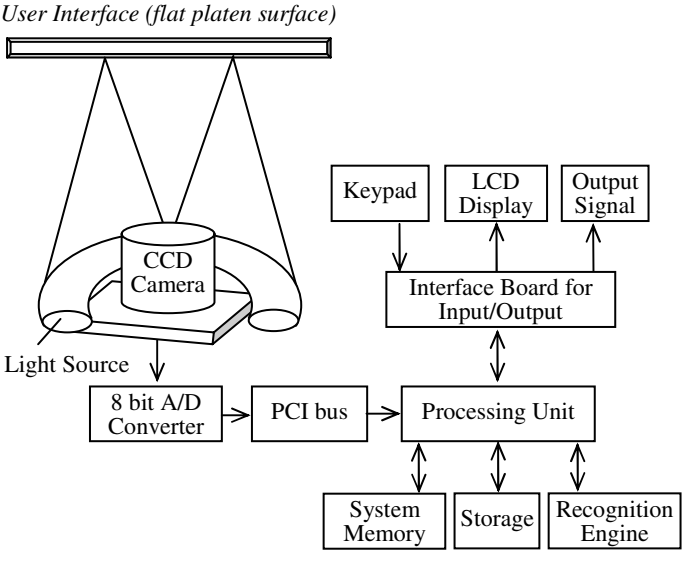


Fig. 1. The schematic diagram of the palmprint authentication system

unit, memory, storage, keypad, LCD display, output signal and recognition engine. The ring light source is designed to provide white light source of high intensity, and it can increase the contrast of the palmprint features from the uneven palm skin surfaces. The optical components (CCD camera and light source) are fabricated in a controlled environment in order to minimize the effects of ambient light. When the signal is generated by the CCD, it is digitized by an 8-bit A/D converter and then the digitized data is transferred to the processor through the PCI bus. The palmprint image is stored in the storage of the system. An interface board is designed to communicate the user with the system through a keypad and a LCD display unit. Recognition engine is the core part of our system which performs personal identification. The output signal is sent when a correct match is obtained.

2.2 System Framework

The proposed palmprint authentication system has four major components: *User Interface Module*, *Acquisition Module*, *Recognition Module* and *External Module*:

(a) *User Interface Module* provides an interface between the system and users for the smooth authentication operation. It is crucial to develop a good user interface so that users are pleasure to use the device. A flat platen surface is designed for palm acquisition accordingly [10].

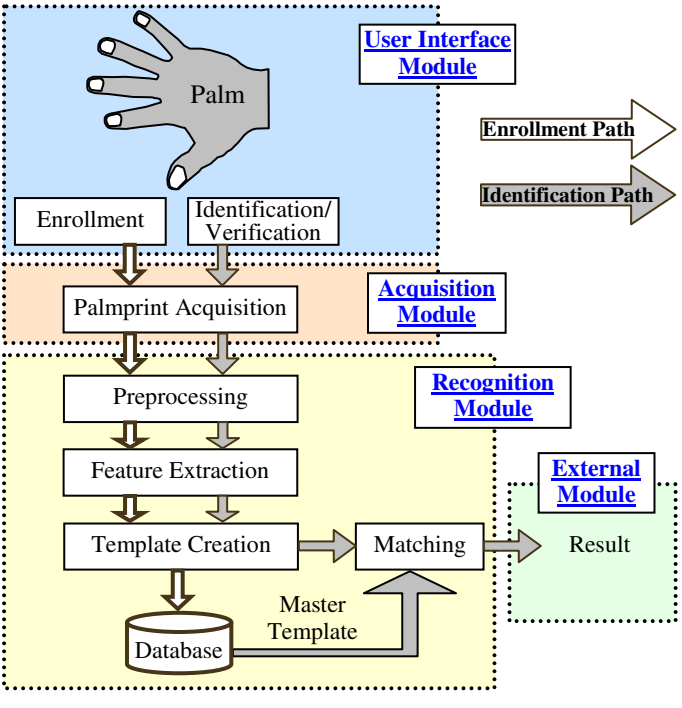


Fig. 2. The breakdown of each module of the palmprint authentication system

(b) *Acquisition Module* is the channel for the palm to be acquired for the further processing. It calls the frame grabber to transfer one frame of image to the processor, and then examines whether a hand has put on the device.
(c) *Recognition Module* is the key part of our system. It consists of image preprocessing algorithm, feature extraction algorithm, template creation, database updating, and matching of features.
(d) *External Module* receives the signal from the recognition module. This module actually is an interfacing component, which may be connected to another hardware or software components. Currently, our system uses a relay to control an electronic door lock for the physical access control.

Fig. 2 shows the details of each module of the palmprint authentication system. The design methodology and implementation of the user interface module and the acquisition module have been described in detail in [10]. The external module is an interfacing component which is application dependent. In this paper, we only concentrate on the recognition module and the performance issues of the proposed system.

3 Recognition Module

After the palmprint images are captured by the *Acquisition Module*, they are fed into the recognition module for palmprint authentication. The recognition module consists of the stages of: palmprints preprocessing, feature extraction, and matching. In the preprocessing stage, different palmprints are aligned for feature extraction. In this paper, we use the preprocessing technique described in [9].

3.1 Feature Extraction

The feature extraction technique implemented on the proposed palmprint system is modified from [9], where a 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:

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

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, π/4, π/2 and 3π/4.

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 followings:

$$\begin{aligned} h_r &= 1 \quad if \quad \mathrm{Re}[G_k * I] \geq 0 \\ h_r &= 0 \quad if \quad \mathrm{Re}[G_k * I] < 0 \\ h_i &= 1 \quad if \quad \mathrm{Im}[G_k * I] \geq 0 \\ h_i &= 0 \quad if \quad \mathrm{Im}[G_k * I] < 0 \end{aligned} \tag{2}$$

More discussion and comparisons between this method and PalmCode are given in [11].

3.2 Matching

The feature matching determines the degree of similarity between two templates – the authentication template and the master template. Since the format of Fusion Code and PalmCode are exactly the same, a normalized hamming distance implemented in PalmCode is still useful for comparing two Fusion Codes. Fusion Code is represented by a set of bits. Mathematically, the normalized hamming distance is represented by:

$$D_o = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} P_M(i,j) \cap Q_M(i,j) \cap \left((P_R(i,j) \otimes Q_R(i,j) + P_I(i,j) \otimes Q_I(i,j))\right)}{2\sum_{i=1}^{N}\sum_{j=1}^{N} P_M(i,j) \cap Q_M(i,j)} \tag{3}$$

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. The ranges of normalized hamming distances are between zero and one, where zero represents perfect matches. 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.

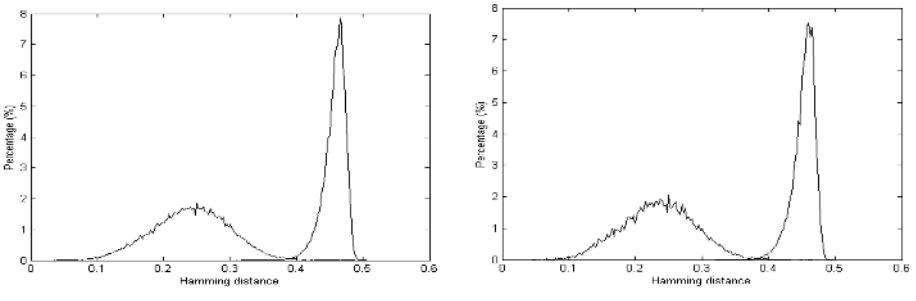
4 Performance Evaluation

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. All the testing images used in the following experiments were 384×284 with 75 dpi.

4.1 Experimental Results of Verification

Verification refers to the problem of confirming or denying a claim of individuals and considered as one-to-one matching. Two groups of experiment are carried out separately. 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. Fig. 3 (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 (a). According to Table 1 (a), 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%.



(a) (b)

Fig. 3. Verification test results. (a) and (b) show the genuine and imposter distributions for verification tests with one and three registered images per palm, respectively.

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. Fig. 3 (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 (a). According to Table 1 (a) and Fig. 3, we can conclude that using three templates can provide better verification accuracy. It is also the reason for those commercial biometric verification systems requiring more than one sample for registration.

Table 1. False acceptance rates (FARs) and false rejection rates (FRRs) with different threshold values, (a) verification results and (b) 1-to-400 identification results

(a)

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

(b)

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

4.2 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. 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. The minimum hamming distances of correct matchings and incorrect matchings are

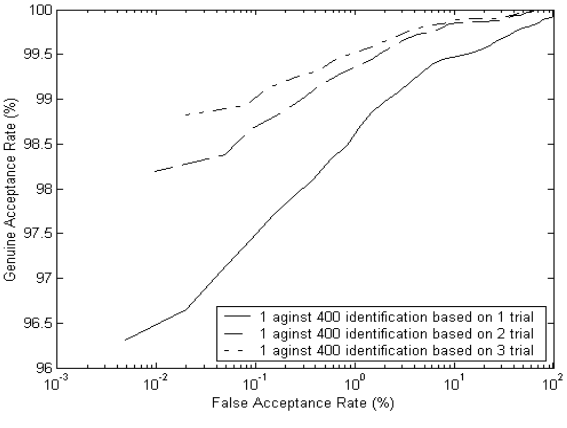


Fig. 4. The ROC curves on a 1-against-400 identification testing with different numbers of trials

regarded as the identification hamming distances of genuine and impostor, respectively. In this experiment, we implement one-, two- and three-trial tests. Fig. 4 shows ROC curves of the three tests and Table 1 (b) lists the threshold values along with its corresponding FARs and FRRs of the tests. According to Fig. 4 and Table 1 (b), more input palmprints can provide more accurate results.

4.3 Robustness

As a practical biometric system, other than accuracy and speed, robustness of the system is another important issue. To verify the robustness of our proposed algorithm against noisy palmprints, we wrote some texts on a palmprint of a hand. Fig. 5 (a) shows a clear palmprint image while Figs. 5 (b)-(f) show five palmprint images, with different texts. Their hamming distances are given in Table 2; all of them are smaller than 0.29. Comparing the hamming distances of imposter in Tables 1 (a) and (b), it is ensured that all the hamming distances in Table 2 are relatively small. Figs. 5 and Table 2 illustrate that the proposed palmprint authentication system is very robust to the noise on the palmprint.

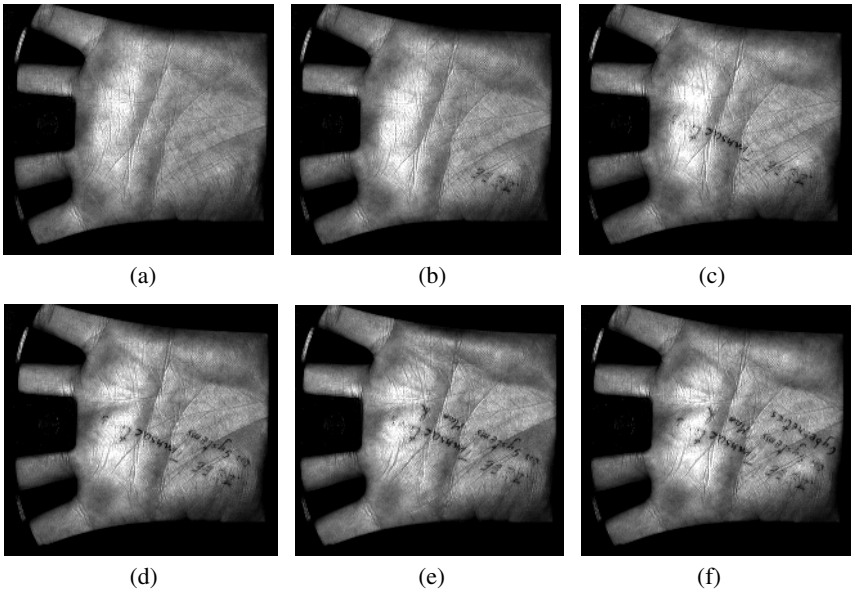


Fig. 5. Palmprint images with different texts for testing the robustness of the system

Table 2. The hamming distances of Figs. 5

Figs	5 (b)	5 (c)	5 (d)	5 (e)	5 (f)
5 (a)	0.19	0.21	0.27	0.29	0.28
5 (b)		0.18	0.27	0.26	0.27
5 (c)			0.27	0.28	0.28
5 (d)				0.23	0.19
5 (e)					0.19

5 Applications

Biometrics can be used in systems ranging from customer oriented to employee oriented applications to improve the work flow and eliminate frauds. Our system can be treated as a supplement of existing service or even a replacement of current method such as smart card or password based authentication systems.

One of the most popular biometric applications is the time and attendance system implemented to prevent frauds from buddy punching. In fact, our palmprint authentication system is most suitable to be used in this type of application because it can be operated in real time for identification/verification, has high accuracy rate and high user acceptance rate. In addition, our system has two modes of operations: identification and verification so that employees do not need to bring any card but their hand to identify their identity. Log files are stored on the file system and can be linked with external software for the automatic salary calculation.

Our system can be extended from a standalone system to a networked version. In addition, we provide different means of input methods such as barcode reader, smart card, and keyboard to allow the most flexible deployment arrangements for the need of different business organizations. In summary, our system can be used in the following applications: ATMs, credit card purchases, airports, building access control, time and attendance management, citizen ID program, biometric passport, voting and voter registration, etc. Fig. 6 shows a standalone version of our prototype system.

Fig. 6. A standalone version of our prototype system

6 Conclusions

In this paper, we have presented a novel personal authentication system using palmprint technology. The proposed system can accurately identify a person in real time, which is suitable for various civil applications such as access control and employee management systems. Experimental results show that the proposed system can identify 400 palms with very low false acceptance rate (0.02%), and a relative 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 superior to other hand-based biometrics systems, such as hand geometry and fingerprint verification system [2, 12] and is practical for real-world applications. The system has been installed at the Biometric Research Center, Department of Computing, The Hong Kong Polytechnic University since March 2003 for access control [10].

References

1. Jain, R. Bolle and S. Pankanti (eds.), *Biometrics: Personal Identification in Networked Society*, Boston, Mass: Kluwer Academic Publishers, 1999.
2. R. Sanchez-Reillo, C. Sanchez-Avilla and A. Gonzalez-Marcos, "Biometric identification through hand geometry measurements", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 10, pp. 1168-1171, 2000.
3. S.K. Im, H.M. Park, Y.W. Kim, S.C. Han, S.W. Kim and C.H. Kang, "An biometric identification system by extracting hand vein patterns", *Journal of the Korean Physical Society*, vol. 38, no. 3, pp. 268-272, 2001.
4. A. Jain, L. Hong and R. Bolle, "On-line fingerprint verification", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 4, pp. 302-314, 1997.
5. A.K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition", *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 14, no. 1, January 2004.
6. NEC Solutions (America), Inc., 2002. *Automated Palmprint Identification System*, http://www.necsam.com/idsolutions/ download/palmprint/palmprint.html
7. Omnitrak AFIS/Palmprint Identification Technology, http://www.motorola.com/LMPS/ RNSG/pubsafety/40-70-10.shtml
8. G. Lu, D. Zhang, K.Q. Wang, "Palmprint recognition using eigenpalms features", *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1473-1477, 2003.
9. D. Zhang, W.K. Kong, J. You and M. Wong, "Online palmprint identification", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 9, pp. 1041-1050, 2003.
10. D. Zhang, *Palmprint Authentication*, Kluwer Academic Publishers, USA, 2004.
11. W.K. Kong and D. Zhang, "Feature-level fusion for effective palmprint identification", *Proceedings International Conference on Biometric Authentication*, 15-17, July, 2004, pp. 761-767, Hong Kong.
12. A.K. Jain, S. Prabhakar, L. Hong and S. Pankanti, "Filterbank-based fingerprint matching", *IEEE Transactions on Image Processing*, vol. 9, no. 5, pp. 846-859, 2000.