Proceedings of the World Congress on Engineering 2010 Vol I
WCE 2010, June 30 - July 2, 2010, London, U.K.

Palm Print Verification System

D.B.L. Bong, R.N. Tingang, and A. Joseph

***Abstract*—Biometrics-based personal identification is a powerful security features in the technology era. Palm print is a reliable biometric that can be used for identity verification because it is stable and unique for every individual. The palm print acquired from a charge coupled device (CCD) based camera is preprocessed and the edge of the image is obtained. The palm prints are matched using the AND function and the verification process is based on whether a person is who he/she claims to be. Five hundred verifications were obtained and analyzed. The false acceptance rate (FAR) and false reject rate (FRR) values against different threshold values were plotted and the equal error rate (EER) was acquired. The system's EER is approximately 15% with the verification threshold of 23. Overall, the system has an accuracy of 87.4%.**

***Index Terms*—Palm print, image processing, false acceptance rate, false reject rate.**

I. Introduction

Reliability in computer aided personal authentication is becoming increasingly important in the information-based world, for effective security system. Biometrics is physiological characteristics of human beings, unique for every individual that are usually time invariant and easy to acquire. Palm print is one of the relatively new physiological biometrics due to its stable and unique characteristics. The rich information of palm print offers one of the powerful means in personal recognition.

Palm prints contain distinctive features such as principal lines, wrinkles, ridges and valleys on the surface of the palm. Unlike palm print identification that matches one feature to many features in the database, palmprint verification system is a one-to-one matching process. It verifies the person's claimed identity to the stored pattern in the system. There are two inputs for the system. The first input is the first sample from every individual which has been set as the stored database. While, the second input is the palm print that needs to be verified. During verification, the line features of the palm prints are extracted and matched.

II. Research Background

Biometric recognition is the application of science to measure individual's properties which are the physiological characteristics. These properties can be a behavior or a physical feature. There are various types of different biometric recognition system. Some examples of them are face, voice, fingerprint and iris recognitions. There are also gestures and signature recognitions. The physical feature used in a biometric recognition system must be unique and stable over a lifetime. Therefore, biometric personal identification is an emerging powerful means to automatically recognize a person's identity.

Recently, voice, face, and iris-based verifications have been studied extensively [1-3]. As a result, many biometric systems for personal identification have been successfully developed. Nevertheless, few works has been reported on palm print identification and verification, despite the importance of palm print features.

The most widely used biometric feature for personal identification is the fingerprint and the most reliable feature is the iris. Even so, it is very difficult to extract small unique features known as minutiae from unclear fingerprints [4] and iris input devices are very expensive. Other biometrics features such as face and voice are not accurate enough since they can change in time [2-3]. In contrast, palm print has several advantages. Palm print contains more information than fingerprint and they are much more distinctive [5]. Palm print can also be captured by using charge coupled device (CCD) camera, thus are much cheaper than iris devices [6]. Furthermore, palm print contains additional distinctive features that can be extracted from low resolution images such as principal lines and wrinkles. Palm print also varies in sizes [5]. So, it is possible to build a highly accurate biometrics system by combining all the features of palmprint.

Biometric systems work by first capturing a sample of the feature, such as recording a digital sound signal for voice recognition, or taking a digital colour image for face recognition. The sample is then transformed using some mathematical function into a biometric template. The biometric template will provide a normalised, efficient and highly discriminating representation of the feature, which can then be objectively compared with other templates in order to determine the identity. Most biometric systems allow two stages of operation. An enrollment stage for adding templates to a database, and a matching stage, where a template is created for an individual and then a match is searched for in the database of the pre-enrolled templates [7].

A good biometric is characterised by using a feature that is highly unique. So the chance of any two people having the same characteristic will be minimal and thus stable. The feature does not change over time, and can be easily captured in order to provide convenience to the user, and prevent misrepresentation of the feature.

Manuscript received February 19, 2010. This work was supported by Faculty of Engineering, Universiti Malaysia Sarawak.

D.B.L. Bong is with the Faculty of Engineering, Universiti Malaysia Sarawak, 94300 Kota Samarahan. Malaysia. (phone: +60-82-58313; fax: +60-82-583410; email: bbldavid@feng.unimas.my).

R.N. Tingang is a graduate from Faculty of Engineering, Universiti Malaysia Sarawak.

A. Joseph is with the Faculty of Engineering, Universiti Malaysia Sarawak, 94300 Kota Samarahan. Malaysia.

ISBN: 978-988-17012-9-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

III. Methodology

The flow chart in Fig. 1 represents the system's flow. The system started with image acquisition which in this case is the acquisition from the database. There would be two inputs where the first input is the first palm print of an individual which represents the stored database. The second input is the palm print that needs to be verified. Both inputs are then processed to extract lines and then the second input is matched against the first input to verify whether the palm print belongs to the same individual or not.

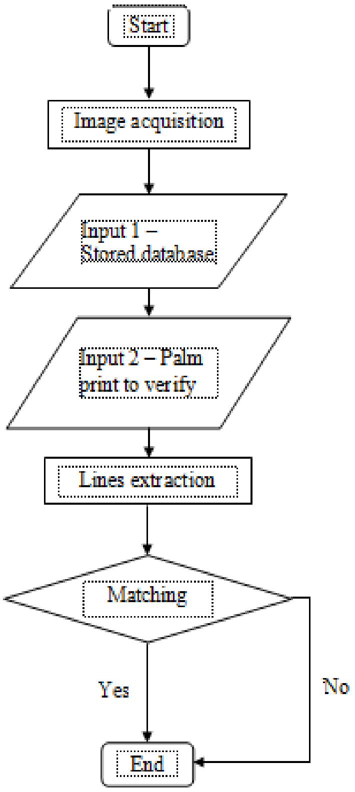


Fig.1: Palm print verification system's flow chart.

All of the works were tested using the PolyU Palmprint Database [8]. The PolyU Palmprint Database contains 7752 grayscale images corresponding to 386 different palms in bitmap image format. Around twenty samples from each of these palms were collected in two sessions where around 10 samples were captured in the first session and the second session, respectively. The average interval between the first and the second collection was two months.

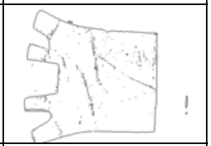
The palm print capture device used for the database includes light source that is shaped as a ring (ring source), CCD camera, lens, frame grabber, and analogue-to-digital converter (ADC). To obtain a stable palm print image, a case and a cover were used to form a semi closed environment, and the ring source provides uniform lighting conditions during the palm print image capturing. Also, six pegs on the platform serves as control points for the placement of the user's hands. The ADC directly transmits the images captured by the CCD camera to a computer. Palm print images can be obtained in two different sizes, 384 x 284 and 768 x 568. The database that is used for this project contains images in the size of 384 x 284 [6].

This project uses ten sets of right hand palm prints from the first session and each set has five samples of palm prints. Hence, there are 50 samples all together.

IV. Experiment Results, Analysis & Discussion

Using different edge detectors, a pair of sample from the same person is used. The following matching percentages and images are obtained.

Table 1: Comparison in using different edge detectors

Edge Detector	Matching Percentage (%)	Resulting Image
Sobel	34.0940	
Prewitt	34.9117	
Roberts	35.8312	
Canny	22.4705	

From Table 1, the edge detector that produced the most matching percentage is chosen to be used in this system. Edge detection using Roberts method produced the highest percentage which is 35.8312%. Canny method has the lowest percentage because the image using Canny filter has a lot of fine details, which is unnecessary for the system. The lines that were extracted using Roberts method are better than the other methods.

A sample from Person 2, P21 is tested against four samples from Person 2 numbered P22, P23, P24, P25, and four other samples from Person 1 (P11), Person 3 (P31), Person 4 (P41) and Person 5 (P51). The results obtained are summarized in Table 2. The results are obtained from MATLAB's command window.

Table 2: Matching percentage of sample P21 against other samples

Samples Pair	**Matching Percentage (%)**
P21 against P22	34.7729
P21 against P23	29.3887
P21 against P24	26.1357
P21 against P25	27.4257
P21 against P11	3.5895
P21 against P31	3.3090
P21 against P41	4.4307
P21 against P51	3.3651

From Table 2, a scatter graph of matching against sample P21 is obtained and shown in Figure 2. The matching percentages for sample P21 against four samples from the

ISBN: 978-988-17012-9-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

same person are very close and high. However, matching results against samples from other persons are low. This can be clearly seen in the scatter graph. It is obvious that the matching percentages between two samples from the same person are high and more than 25%. However, the matching percentages between two samples of different person are smaller than 5%. Therefore, a threshold can be set to determine whether two samples are from the same palm. This threshold is used to verify the palm prints as of the same person or a different person.

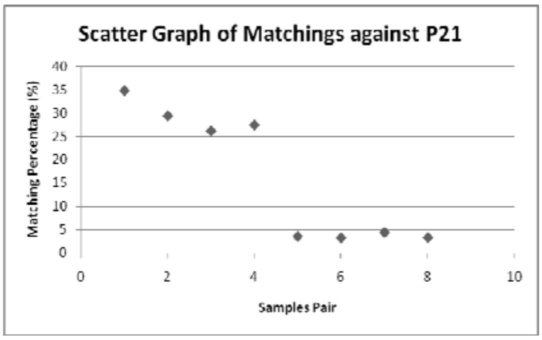


Fig.2: Scatter graph of matching against sample P21.

Five samples from ten individuals are used and are tested against each of the sample. There are 500 verifications done in total. 50 samples are verification of same individuals while the other 450 are verification of an individual against other individuals.

A. False Reject Rate (FRR)

Genuine verification is a verification of the same individual. Matching percentage of genuine verification varies around a certain mean value. If a verification threshold that is too high is applied to the system, some of the genuine matching pairs are falsely rejected. Depending on the value of the threshold, the data that will be falsely rejected can be from zero to all images. The number of rejected data divided by the total data is called False Rejection Rate (FRR). Table 3 shows the varying threshold values and the corresponding FRR obtained from the system's 500 verifications.

Table 3: Different threshold values and the corresponding FRR

Threshold (%)	FRR (%)
10	0
12	0
14	0
16	0
18	4
20	6
22	12
24	22
26	30
28	40
30	46
32	46
34	52

A graph is plotted for the FRR and is as shown in Figure 3. The percentage of the FRR ranges between 0 and 100 and it is exponentially increasing.

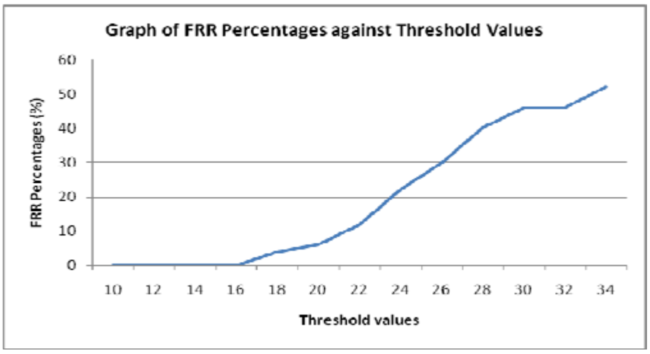


Fig.3: Graph of FRR percentages against different threshold values.

B. False Acceptance Rate (FAR)

Depending on the choice of threshold, the impostor's palm prints that are falsely accepted by the system can be from none to all images. Impostor is an individual that is verified against a different stored database. The threshold of the falsely accepted data divided by the number of all impostor data is called False Acceptance Rate (FAR). Its value is one, if all impostor data are falsely accepted, and zero if none of the impostor data is accepted. Figure 4 shows the percentages of the FAR against different threshold values plotted using the data in Table 4.

Table 4: Different threshold values and the corresponding FAR

Threshold (%)	FAR (%)
10	53.33
12	51.78
14	49.56
16	42.22
18	37.11
20	27.78
22	17.33
24	10.44
26	4.89
28	0.44
30	0
32	0
34	0

The percentage of the FAR ranges between 0 and 100, and it is exponentially decreasing.

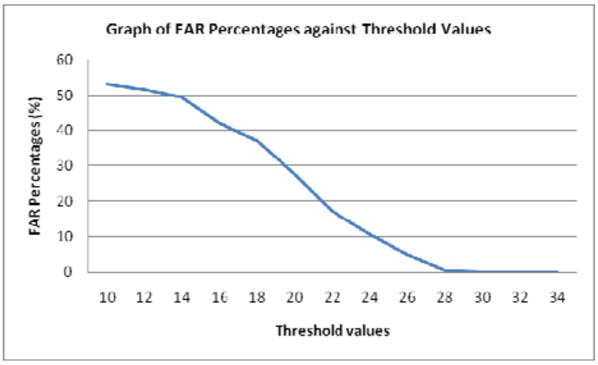


Fig.4: Graph of FAR percentages against different threshold values.

ISBN: 978-988-17012-9-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

C. Equal Error Rate (EER)

The choice of the threshold value is made easier by determining the Equal Error Rate (EER). As the name implies, EER is the value where the FAR and the FRR overlaps and the value is equal for both rate. The EER of a system can be used to give a threshold independent performance measure. The lower the EER is, the better is the system's performance, as the total error rate which is the sum of the FAR and the FRR at the point of the EER decreases. The EER of this system is shown in Figure 5.

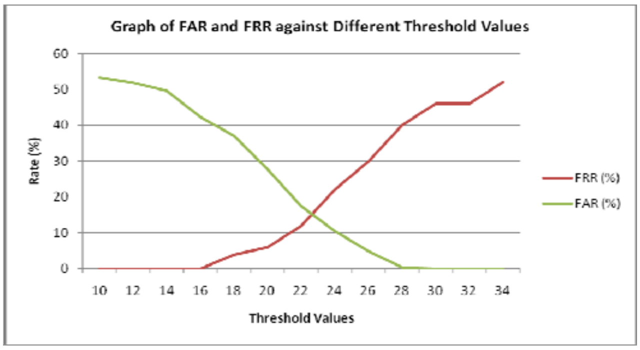


Fig.5: Graph of FAR and FRR against different threshold values.

From Figure 5, the EER of the system is approximately 15%. The threshold taken for verification is 23.

Using the determined threshold value as 23, the data obtained from 500 samples are considered. The number of times that the system responds with correct and incorrect verification is counted. Total data counts are 500. There are six verifications of the same person rejected, while 57 verifications are falsely accepted. The total of correct verifications is 437. Verification rate is counted by taking the percentage of correct verifications over total data count. Therefore, the verification rate of this approach is 87.4%. Table 5 summarizes the data.

Table 5: Summary of experiment results

Falsely rejected data	6
Falsely accepted data	57
Correct Verifications	437
Total data count	500

The rate of false acceptance and false reject can be influenced by several reasons. The reasons could be two different palm prints having the same principal lines, different illumination and also alignment of the palms on the capturing device. True negative rate which is the genuine rejection can also be influenced by having different principal lines and also different palm sizes.

V. Conclusion

After several testing and experiments, a palm print verification system is developed with 87.4% of verification rate using five samples from ten person of Hong Kong Polytechnic University (PolyU) Palmprint Database [8]. This is considered as acceptable and the performance of the system is satisfactory. The EER of the system is also quite low, which is about 15%.

There are several limitations encountered while completing this project. One of them is determining the region of interest (ROI). An algorithm is needed to determine the coordinate system of the palm print and then to obtain a region that is rich in information to match. This problem is solved by using the Hong Kong Polytechnic University (PolyU) Palmprint Database [8] that provides fixed size images of palm prints. The images are also aligned because of a peg used between the fingers.

Another limitation encountered is when analyzing the system. The program cannot be executed through the database automatically. Results are obtained one by one by using the GUI and the matching percentage is obtained from the command window of MATLAB. This is time consuming and could lead to confusion if a lot of database is to be used. Thus, a real time system with automated process is recommended as future works.

Acknowledgment

The authors would like to acknowledge the support given by Faculty of Engineering, Universiti Malaysia Sarawak for the provision of research facilities, and The Hong Kong Polytechnic University for sharing the palm print database.

References

[1] C. Zhang and S. F. Cohen, *3-D face structure extraction and recognition from images using 3-D morphing and distance mapping*. IEEE Transactions on Image Processing, 2002. 11: p. 1249-1259.
[2] Y. Gao and M. K. H. Leung, *Face recognition using line edge map*, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002. 24: p. 764-779.
[3] J. Liu-Jimenez, R. Sanchez-Reillo and C. Sanchez-Avila, *Biometric co-processor for an authentication system using iris biometrics.* IEEE Transactions, 2004. 02: p. 131-135.
[4] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. Jain, *FVC2000 : Fingerprint verification competition*. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002. 24: p. 402-412.
[5] X. Wu, D. Zhang, and K. Wang, *Palm line extraction and matching for personal authentication*. IEEE Transactions on Systems, Man, and Cybernetics, 2006. 36: p. 978-987.
[6] D. Zhang, W. Kong, J. You and M. Wong, *Online palmprint identification*. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003. 25: p. 1041-1050.
[7] L. Masek, Recognition of human iris patterns for biometric identification, Thesis, University of Western Australia, 2003.
[8] The Hong Kong Polytechnic University (PolyU) Palmprint Database (The Second Version) [online]. Available: http://www.comp.polyu.edu.hk/~biometrics/.