Personal Recognition by Finger-Knuckle-Print Based on Log-Gabor Filter Response

Abdallah Meraoumia[1],Salim Chitroub[1] and Ahmed Bouridane[2]

[1]Signal and Image Processing Laboratory, Electronics and Computer Science Faculty, USTHB.
P.O. box 32, El Alia, Bab Ezzouar, 16111, Algeria
[2]School of Computing, Engineering and Information Sciences
Northumbria University, Pandon Building, Newcastle upon Tyne, UK.
Email: Ameraoumia@gmail.com, S_chitroub@hotmail.com, Bouridane@qub.ac.uk

***Abstract*—Biometrics technique is an important and effective solution for automatic personal verification/identification. Recently, a novel hand-based biometric feature, Finger-Knuckle-Print (FKP), has attracted an increasing amount of attention. Like any other biometric identifiers, FKPs are believed to have the critical properties of universality, uniqueness and permanence for personal recognition. This paper investigates a new approach for human FKP recognition using 1D Log-Gabor filter response. We employ 1D Log-Gabor wavelet to extract the information. Thus each finger is represented by a two finger codes (real and imaginary template). Those templates (finger codes) are compared with those in the database using Hamming distance. The experimental results showed that the designed system achieves an excellent recognition rate on the Hong Kong polytechnic university (PolyU) Finger-Knuckle-Print Database. The proposed technique is computationally effective with recognition rates of 99.71% and 99.91% for verification and identification, respectively.**

***Index Terms*—Biometrics, Verification, Identification, FKP, Log-Gabor Filter, Hamming distance, Data fusion.**

I. Introduction

A BIOMETRIC system provides automatic recognition of an individual based on some sort of unique feature or characteristic possessed by the individual. Biometric systems have been developed based on fingerprints, faces, palmprints, hand geometry, iris, etc [1]. Currently, a number of biometrics-based technologies have been developed. Hand-based person identification provides a reliable, low-cost and user-friendly viable solution for a range of access control applications [2]. Recently, a novel hand-based biometric feature, finger-knuckle-print (FKP), has attracted an increasing amount of attention. The image-pattern formation of a finger-knuckle contains information that is capable of identifying the identity of an individual [3]. Biometric FKP recognizes a person based on the knuckle lines and the textures in the outer finger surface. These line structures and finger textures are stable and remain unchanged throughout the life of an individual. This paper describes the prototype of a biometric recognition system based on a fusion of finger-knuckle-print features.

An important issue in FKP recognition is to extract FKP features that can discriminate an individual from the other. Our biometric recognition system is based on features extracted from FKP images by one-dimensional Log-Gabor filter response. In this method, a FKP is filtered using 1D Log-Gabor filter. The real and imaginary part of each filtered image produces the feature vector (template). Subsequently, we use hamming distance for the FKP matching. It is noted that, our database contains FKPs from four types of fingers, Left Index Fingers (LIF), Left Middle Fingers (LMF), Right Index Fingers (RIF) and Right Middle Fingers (RMF). For this raison, An ideal FKP recognition system should be based on the fusion of these fingers.

This paper is organized as follows. A scheme for FKP recognition is presented in section 2. Section 3 gives a brief description of the region of interest extraction. 1D Log-Gabor filter and encoding process are discussed in section 4. FKP matching and the decision module are shown in sections 5 and 6, respectively. A sections 7 is devoted to describe evaluation criteria. The experimental results prior to fusion and after fusion are presented and commented in section 8. Finally, the conclusions and further works are presented in sections 9.

II. System design

Fig. 1 illustrates the main steps of our proposed method. In the first phase, the FKP image preprocessing step performs the localization of Region Of Interest (ROI) which is regarded as one of the most important areas of the FKP pattern. In the second phase, the knuckle lines and the textures are extracted using 1D Log-Gabor filter and a encoding process. Finally, the resulting template is matched to the templates from the FKPs database using Hamming distance.

III. Preprocessing module

After the image is captured, it is pre-processed to obtain only the area information of the FKP. The detailed steps for pre-processing process are as follows [4]: First, apply a Gaussian smoothing operation to the original image. Second, determine the X-axis of the coordinate system fitted from the bottom boundary of the finger; the bottom boundary of the finger can be easily extracted by a Canny edge detector. Third, determine the Y-axis of the coordinate system by applying a Canny edge detector on the cropped sub-image extracted from the image original base on X-axis, then find the convex direction coding scheme. Finally, extract the ROI coordinate system, where the rectangle indicates the area of the ROI sub-image that will be extracted. The pre-processing steps are shown in Fig. 2.

ICEO'11

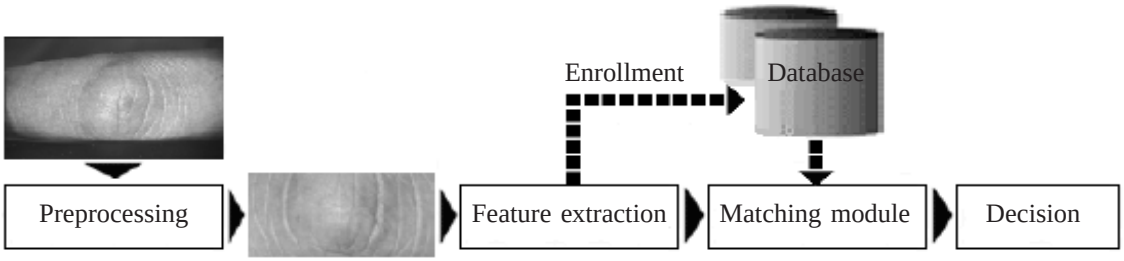


Fig. 1. Block diagram for the person recognition using finger knuckles based on Log-Gabor filter response.

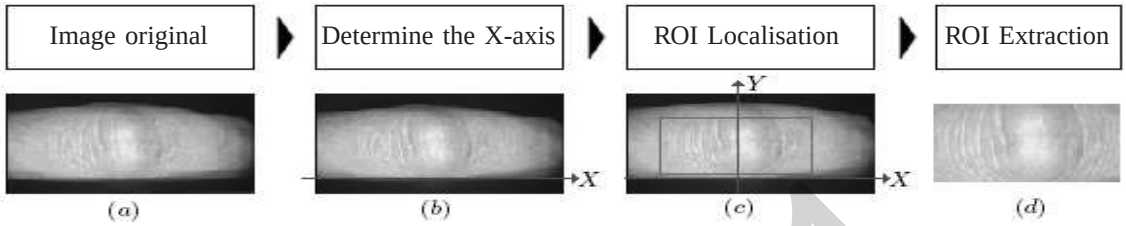


Fig. 2. Illustration for the ROI extraction process. (a) Image original; (b) X-axis of the coordinate system; (c) ROI coordinate system and (d) Region of interest (ROI)

IV. Feature extraction

The most discriminating information present in a FKP pattern must be extracted. Only the significant features of the FKP must be encoded so that comparisons between templates can be made. 1D Log- Gabor filter is able to provide optimum conjoint representation of a signal in space and spatial frequency [5]. In our method, the features are generated from the ROI by filtering the image with 1D Log-Gabor filter.

A. Log-Gabor Filter

Gabor features are a common choice for texture analysis. They offer the best simultaneous localization of spatial and frequency information. One weakness of the Gabor filter in which the even symmetric filter will have a DC component whenever the bandwidth is larger than one octave [6]. To overcome this disadvantage, a type of Gabor filter known as Log-Gabor filter, which is Gaussian on a logarithmic scale, can be used to produce zero DC components for any bandwidth. The frequency response of a Log-Gabor filter is given as:

$$G(f) = \exp\left[\frac{-(\log(f/f_o))^2}{2(\log(\sigma/f_o))^2}\right] \tag{1}$$

where f_o represents the center frequency, and σ gives the bandwidth of the filter. In the experiments, The parameters of Log-Gabor filter were empirically selected as f_o =1/2 and σ = 0.0556. are used in all calculation.

B. Encoding process

The ROI sub-images (rows) were unwrapped to generate 1D vector for feature extraction. These signals were convolved with 1D Log-Gabor filter. The resulting convolved form of the signal is complex valued. We then apply the following inequalities to extract binary response templates for both, real and imaginary part.

$$\begin{cases} b_r = 1 \;\; if \;\; Re[\bullet] \geq 0, & b_r = 0 \;\; if \;\; Re[\bullet] < 0 \\ b_i = 1 \;\; if \;\; Im[\bullet] \geq 0, & b_i = 0 \;\; if \;\; Im[\bullet] < 0 \end{cases} \tag{2}$$

Feature extraction method stores the real and imaginary parts (templates) in the system database. Fig. 3 shows the block diagram of the FKP feature extraction module.

V. Matching module

A. Hamming distance

The criterion for similarity/disimilarity is to minimize the score (distance) between the input template f_v and the stored template f_r. The difference between the templates is labeled "*Hamming Distance*". A simple *XOR* operation between the corresponding pair of features provides this Hamming Distance. Hamming distance does not measure the difference between the components of the feature vectors, but the number of components that differ in value. We can define the hamming distance D_o [7] as,

$$D_o = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} M(i,j) \cap \psi_e(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N} M(i,j)} \tag{3}$$

$$M(i,j) = M_I(i,j) \cap M_S(i,j) \tag{4}$$

$$\psi_e(i,j) = \psi_1(i,j) \oplus \psi_2(i,j) \tag{5}$$

Where D_o is the hamming distance, ψ_1 (ψ_2) is the input (stored) feature, M_I (M_S) is the input (stored) mask, $\oplus$ is the exclusive *OR* operator (*XOR*), $\cap$ is the *AND* operator, and $N \times N$ is the size of the features. The value D_o lies between 0 and 1, inclusive, with 1 meaning that the two features are independent and 0 meaning they are completely identical.

ICEO11

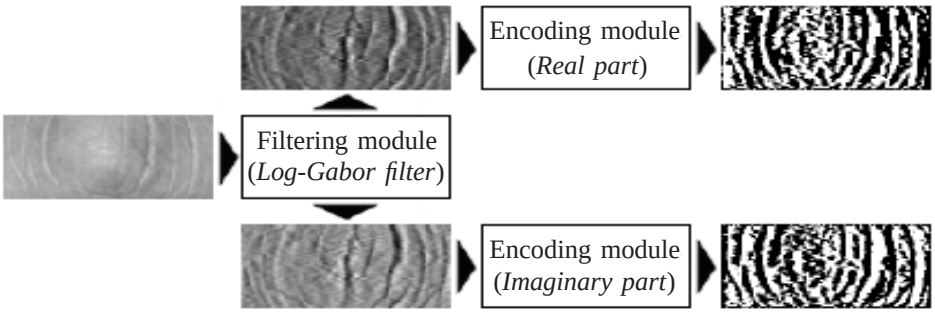


Fig. 3. Block-diagram of the FKP feature extraction module.

B. Normalization and information fusion

1) Normalization process: The normalization process is used only in the case of identification, during the *identification* process, the characteristics of the test FKP image are analyzed by the 2D-DCT corresponding to each person. Then the matching scores are computed for all database templates. Therefore, prior to finding the decision, a *Min-Max* normalization scheme was employed to transform the score vectors computed. Suppose that the score vector is given by:

$$D_i = [D_{i0} \quad D_{i1} \quad D_{i2} \quad D_{i3} \cdots D_{iN_d}] \tag{6}$$

Where N_d represent the size of system database and i the order of image test. Then, the *Min-Max* normalization scheme is given by:

$$D_i^{Nr} = \frac{D_i - min(D_i)}{max(D_i) - min(D_i)} \tag{7}$$

Where D^{Nr} represent the normalized vector. Therefore, these scores are compared, and the highest score provides the identity of the test FKP image.

2) information fusion: Fusion at the matching score level is the most popular and frequently used method because of its good performance and simplicity [8]. The outputs of the two or more matching modules (LIF, LMF, RIF, RMF) are combined using fusion at the matching-score level. The object is to combine these scores to generate a single score which is then used to make the final decision. The fusion is expressed by *min rule* on the matching scores obtained from these matching modules.

$$D_F = min(D_{LIF}, D_{LMF}, D_{RIF}, D_{RMF}) \tag{8}$$

Where D_{LIF}, D_{LMF}, D_{RIF} and D_{RMF} represents the error (*hamming distance*), of LIF, LMF, RIF and RMF matching, respectively and D_F their fusion. This score is compared to a threshold T_o to make the decision of rejecting or accepting the user.

VI. Decision Module

The final step in the recognition process is the *accepted/rejected* decision based on the security threshold, T_o. This security threshold is either a parameter of the matching module or the resulting score (Hamming distance is compared with the threshold value to make the final decision).

$$Decision = \begin{cases} D_o \leq T_o & \Rightarrow \quad \textit{Accepted;} \\ D_o > T_o & \Rightarrow \quad \textit{Rejected;} \end{cases} \tag{9}$$

The pre-defined threshold, for decision, value also separates *false* and *right* results. The error rate of a system can be determined as a function of threshold when varying the threshold in an experiment. A threshold value is obtained based on equal error rate criteria where *FAR = FRR.*

VII. Evaluation criteria

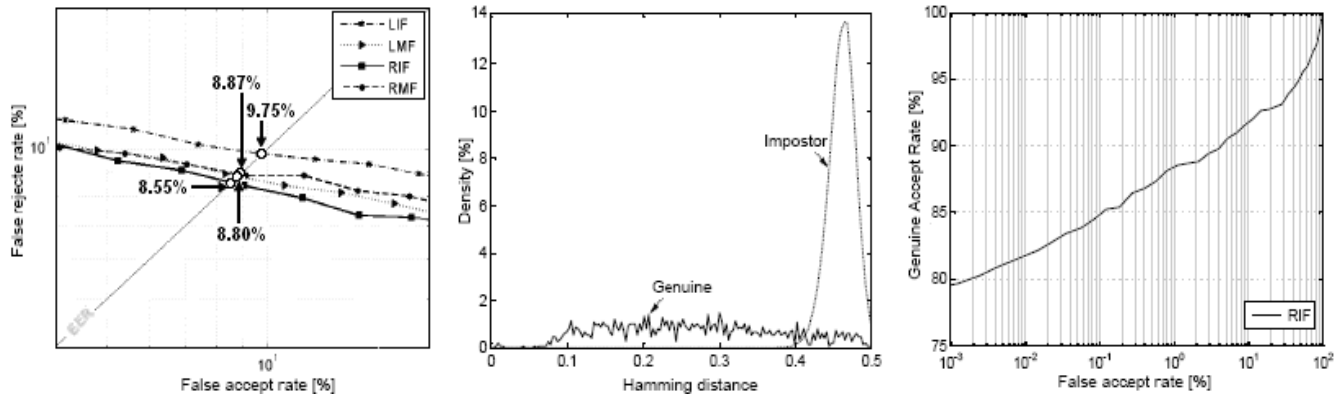
The measure of utility of a FKPs system for a particular application can be described by two values [9]. The False Acceptance Rate (FAR) is the ratio of the number of instances of pairs of different FKPs found to match to the total number of match attempts. The False Rejection Rate (FRR) is the ratio of the number of instances of pairs of the same FKPs is found not to match to the total number of match attempts. FAR and FRR trade off against one another. That is, a system can usually be adjusted to vary these two results for a particular application, however decreasing one increase the other and vice versa. The system threshold value is obtained based on the Equal Error Rate (EER) criteria where FAR = FRR. This is based on the rationale that both rates must be as low as possible for the biometric system to work effectively. Another performance measurement is obtained from FAR and FRR which is called Genuine Acceptance Rate (GAR). It represents the identification rate of the system. In order to visually depict the performance of a biometric system, Receiver Operating Curves (ROC) are drawn. The ROC curve displays how the FAR changes with respect to the GAR and vice-versa [10]. Biometric systems generate matching scores that represent how similar (or dissimilar) the input is compared to the stored template.

VIII. Experimental evaluation and results

A. Experimental database

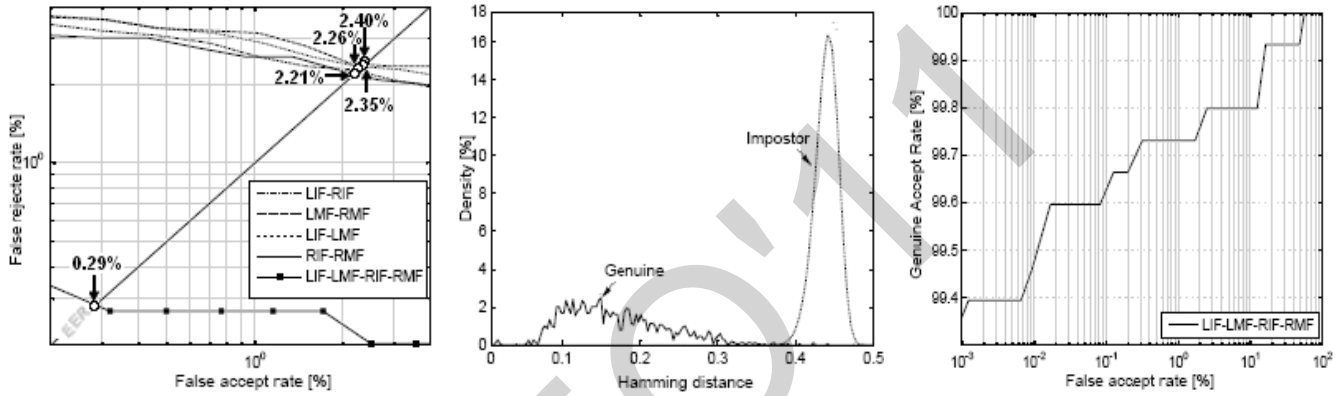
We experimented our approach on Hong Kong polytechnic university (PolyU) Finger-Knuckle-Print Database [11]. The database has a total of 7920 images obtained from 165 persons. this database including 125 males and 40 females. Among them, 143 subjects are 20∼30 years old and the others are 30∼50 years old. these images are collected in two separate sessions. In each session, the subject was asked to provide 6 images for each of LIF, LMF, RIF and RMF. Therefore, 48 images from 4 fingers were collected from each subject.

ICEO'11



(a) (b) (c)

Fig. 4. Unimodal verification test results. *(a)* The ROC curves for all finger types, *(b)* The genuine and impostor distribution and *(c)* The ROC curves for the RIF fingers



(a) (b) (c)

Fig. 5. Multimodal verification test results. *(a)* The ROC curves for all fingers fusion using *min rule*, *(b)* The genuine and impostor distribution and *(c)* The ROC curves based on the fusion of all fingers

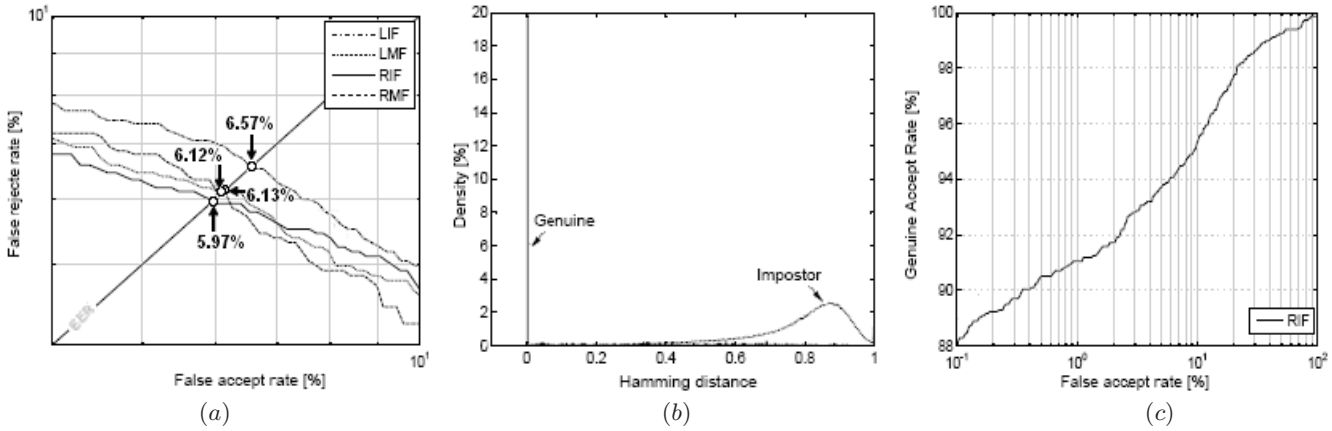
ICEO'11

B. Verification tests

In the process of verification, the input template is compared only with the model of claimed person. The feature vector is compared with features from the model previously stored in the database. The result is the person is either authorized or not authorized. The verification experiments were performed by using each of the LIF, LMF, RIF and RMF features, as well as the fusion of them at the score level based on the *min* rule technique.

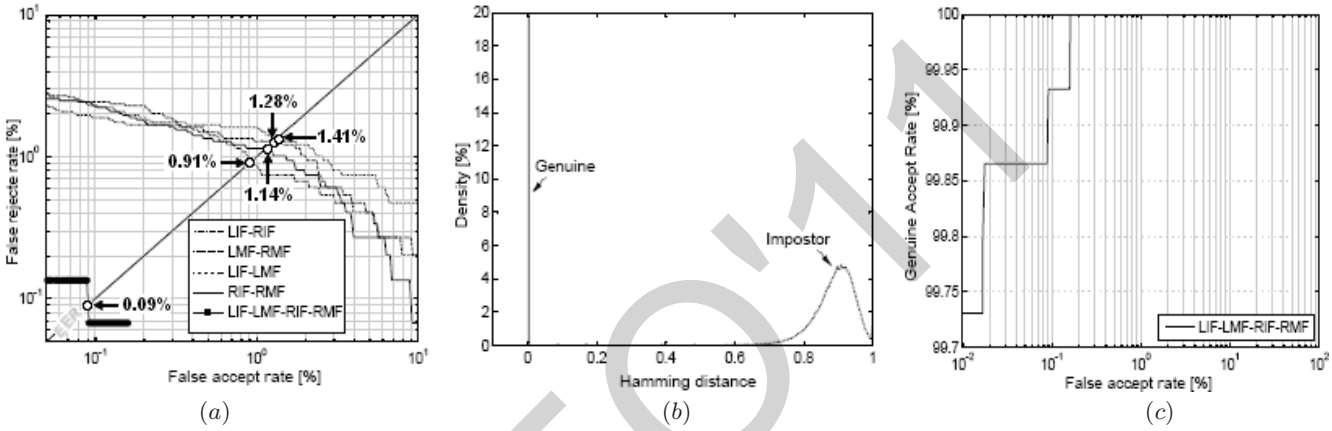
1) Verification in the case of unimodal system: In this experiment, three samples of each palm were randomly selected to construct a training set (enrollment). And the other were taken as the test set. Thus, there are total 495 training images and 1485 test images, respectively. Therefore, there are totally 495 genuine comparisons and 13530 impostor comparisons are generated. Verification performance of the four fingers are illustrated in Fig. 4.a. From Fig. 4.a, we can observed the benefits of using the RIF modality in term of EER. For example, if if only the LIF modality is used, we have EER = 9.75 % at the threshold T_o = 0.429. In the case of using the RMF modality, EER was 8.87 % at the threshold T_o = 0.435. This EER was 8.80 % at T_o = 0.435 for the LMF. RIF modality improves the result (8.55%) for a database size equal to 165 users. Therefore, the system can achieve higher accuracy at RIF modality compared with the others fingers. Finally, the distribution of genuine and impostor matching of the FKP verification system when the RIF modality is used are illustrated in Fig. 4.b and its ROC curve is plotted in Fig. 4.c.

2) Verification in the case of multimodal system: The objective of this section is to investigate the integration of all fingers features, and to achieve higher performance that may not be possible with unimodale biometric alone. Thus, in order to see the performance of the system, we usually plot the ROC curve, which plots the FAR against the FRR, for all the combination possible {LIF-RIF, LMF-RMF, LIF-LMF, RIF-RMF and LIFLMF- RIF-RMF} (see Fig. 5.a). From Fig. 5.a, we can observed the benefits of using the LIF-LMF-RIF-RMF fusion modalities. For example, fusion of LIF and LMF give an EER equal to 2.35 % at T_o = 0.411. This system can achieve an EER of 2.21 % for T_o = 0.415 in the case of RIF and RMF fusion. Fusion of LIF and RIF done an EER equal to 2.40 % at T_o = 0.415. In the case of using the LMF-RMF, EER = 2.40 % at the threshold T_o = 0.415. Finally, tthe system can operate at a 0.29 % EER, and the corresponding threshold is T_o = 0.392. The experimental result shows that fusion of all finger-knuckles is much higher than the individual fingers. The genuine and imposter distributions are shown in Fig. 5.b. Fig. 5.c depicts the ROC curve. Compared with the approaches described in [12], [13] our system achieves better results expressed in terms of the equal error rate.



(a) (b) (c)

Fig. 6. Unimodal identification test results. *(a)* The ROC curves for all finger types, *(b)* The genuine and impostor distribution and *(c)* The ROC curves for the RIF fingers



(a) (b) (c)

Fig. 7. Multimodal identification test results. *(a)* The ROC curves for all fingers fusion using *min rule*, *(b)* The genuine and impostor distribution and *(c)* The ROC curves based on the fusion of all fingers

C. Identification tests

Identification occurs when the biometric system attempts to determine the identity of an individual. A biometric is collected and compared to all the templates in a database. Identification is *closed-set* if the person is assumed to exist in the database. In *open-set* identification, the person is not guaranteed to exist in the database. In our work, the proposed method was tested through the second mode test (*open-set*).

1) Identification in the case of unimodal system: In order to obtain the performance characteristics, we perform a total of 495 genuine and 13530 impostor comparisons. Fig. 6.a shows the identification performance of the four fingers. It can safely be see the benefits of using the RIF modality. For example, if only LIF modality is used for the identification, we have EER = 6.57 % at T_o = 0.445. In the case of using RMF, EER was 6.13 % at T_o = 0.474. In the case of LMF the system can achieve an EER equal to 6.12 % at T_o = 0.453. Finally, a RIF done a result of 5.97 % for a T_o = 0.469. Fig. 6.b presents the distribution of genuine and impostor matching, and the ROC curve obtained by the proposed scheme is plotted in Fig. 6.c.

2) Identification in the case of multimodal system: To find the better finger type, with the lowest EER, graphs showing the ROC curve were generated (see Fig. 7.a). By the analysis of this plot, it can be observed the identification system achieves highest performance when using the all fingers fusion (LIF-LMF-RIF-RMF). For example, our identification system can achieve an EER of 0.91 % for T_o = 0.397 with the LIF and RIF and it can achieves an EER equal to 1.14 % at the decision threshold T_o = 0.459 for RIF and RMF. If fusion of LMF and RMF is used for the identification, our system can achieve an EER = 1.28 % with T_o = 0.455. In the case of using LIF and LMF, EER was 1.41 % at T_o = 0.448. However, it can be concluded that the fusion of all finger-knuckles yields much better identification results compared with one finger. Fig. 7.b presents the distribution of genuine and impostor matching, and the ROC curve obtained by the proposed scheme is plotted in Fig. 7.c. The developed system isexpected to give higher accuracy than [14], [15].

IX. Conclusion and Further Work

In this paper, we have designed a biometric recognition system based on the fusion of FKPs modalities. The scheme uses the 1D Log-Gabor for feature extraction process and a Hamming distance for a matching process. The experimental results showed that information fusion at the matching score level improves the results of both identification and verification. The obtained results showed that the proposed methods obtains an highest recognition rate. Our future work will focus on the performance evaluation in both phases (verification and identification) using large size database and integration of the

ICEO'11

1D Log-Gabor with phase correlation function to get security system with high accuracy.

REFERENCES

[1] Ajay Kumar and David Zhang, "Improving Biometric Authentication Performance From the User Quality", IEEE transactions on instrumentation and measurement, vol. 59, no. 3, march 2010.

[2] K Kumar Sricharan, A Aneesh Reddy and A G Ramakrishnan, "Knuckle based Hand Correlation for User Authentication", Biometric Technology for Human Identification III, Proc. of SPIE Vol. 6202, 62020X, (2006)

[3] Rui Zhao, Kunlun Li , Ming Liu, Xue Sun, "A Novel Approach of Personal Identification Based on Single Knuckleprint Image", Asia-Pacific Conference on Information Processing, APCIP, 2009

[4] L. Zhang, L. Zhang, D. Zhang, "Finger-knuckle-print: a new biometric identifier", in: Proceedings of the ICIP09, 2009.

[5] S. Senapati, G. Saha, "Speaker Identification by Joint Statistical Characterization in the Log-Gabor Wavelet Domain", International Journal of Intelligent Systems and Technologies, Winter 2007.

[6] F. Wang, J. Han, "Iris recognition method using Log-Gabor filtering and feature fusion", Journal of Xian Jiaotong University, Vol.41, 2007.

[7] A. Meraoumia, S. Chitroub and A. Bouridane, "Person's Recognition Using Palmprint Based on 2D Gabor Filter Response", J. Blanc-Talon et al. (Eds.): ACIVS 2009, LNCS 5807, pp. 720-731, Springer-Verlag Berlin Heidelberg 2009.

[8] A. Meraoumia, S. Chitroub and A. Bouridane, "Efficient Person Identification by fusion of multiple Palmprint representations", A. Elmoataz et al. (Eds.): ICISP 2010, LNCS 6134, pp. 182-191, Springer-Verlag Berlin Heidelberg 2010.

[9] T. Connie, A. Teoh, M. Goh and D. Ngo, "Palmprint Recognition with PCA and ICA", Palmerston North, 2003.

[10] A. K. Jain, A. Ross and S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, N. 1, 2004.

[11] PolyU Finger KnucklePrint Database. ttp://www.comp.polyu.edu.hk/biometrics/FKP.htm

[12] Ajay Kumar and Ch. Ravikanth, "Personal Authentication Using Finger Knuckle Surface", IEEE Transactions On Information Forensics And Security, Vol. 4, No. 1, March 2009, pp: 98-110.

[13] Ajay Kumar and K. Venkata Prathyusha, "Personal Authentication Using Hand Vein Triangulation and Knuckle Shape ", IEEE Transactions On Image Processing, Vol. 18, No. 9, September 2009, pp: 2127-2136.

[14] A. Kumar and Y. Zhou, "Personal identification using finger knuckle orientation features ", Electronics Letters September 2009 Vol. 45 No. 20.

[15] Hee-Sung Kim, Byungku Bae, "Finger Pattern Identification for Authentication Purpose", IEEE International Symposium on Industrial Electronics (ISlE 2009) Seoul Olympic Parktel, Seoul, Korea July 5-8, 2009

ICEO'11