Multimodal Biometric System using Iris, Palmprint and Finger-Knuckle

Ola M. Aly
Ministry of Military Production

Hoda M. Onsi
Vice dean of post graduate and research, Faculty of Computers and Information
Cairo University

Gouda I. Salama
Egyptian Armed Forces

Tarek A. Mahmoud
Egyptian Armed Forces

ABSTRACT
Most real-life biometric systems are still unimodal. Unimodal biometric systems perform person recognition based on a single source of biometric information. Such systems are often affected by some problems such as noisy sensor data, nonuniversality and spoof attacks. Multibiometrics overcomes these problems. Multibiometric systems represent the fusion of two or more unimodal biometric systems. Such systems are expected to be more reliable due to the presence of multiple independent pieces of evidence. In this paper, we present a multibiometric recognition system using three types of biometrics Iris, Palmprint and Finger_Knuckle Print. The fusion is applied at the matching-score level. The experimental results showed that the designed system achieves an excellent recognition rate with total Equal Error Rate EER zero percent.

Keywords
Finger_Knuckle, Biometric Fusion, Iiris, Matching score, Multibiometrics, Palmprint.

1. INTRODUCTION
A biometric system is essentially a pattern recognition system that performs recognition based on some features derived from measurements of physiological or behavioral characteristics that an individual has. Biometric characteristics, including fingerprint, facial features, iris, voice, signature, and palmprint, finger-knuckle, gait etc. are now widely used in security applications.

These unimodal biometric systems are faced with a variety of problems, noise in sensed data, non universality, inter-class similarities, and spoof attacks. Multibiometrics are a relatively new approach to overcome those problems. Besides enhancing matching accuracy, the multibiometric systems have many advantages over traditional unibiometric systems [1]. They address the issue of non-universality. It becomes increasingly difficult (if not impossible) for an impostor to spoof multiple biometric traits of an individual. A multibiometric system may also be viewed as a fault tolerant system.

Multibiometric sysetms depend on representing each client by multiple sources of biometric information [1]. Based on the nature of these sources, a multibiometric system can be classified into one of six categories, Multi-sensor systems, Multi-algorithm systems, Multi-instance systems, Multi-sample systems, Multimodal systems and Hybrid systems.

Fusion in multimodal biometric systems can happen at three different levels, feature extraction level, matching score level and decision level [2]. Each type of fusion has its advantages and disadvantages. Fusion at feature extraction level has two main problems, the incompatibility between different feature vectors and the difficulty of finding a good classifier for high-dimensional joint feature vectors. Fusion at the decision level is rather loosely coupled system architecture, with each subsystem performing like a single biometric system. So the fusion at match score level is the most widely used fusion type.

Beginning from 1998, multibiometric recognition systems have been proposed. Fierrez-Aguilar and Ortega-Garcia [3] proposed a multimodal approach including face, a minutiae-based fingerprint and online signature with fusion at the matching score level. The fusion approach obtained Equal Error Rate (EER) of 0.5.

Snelick et al. [4] developed a multimodal approach for face and fingerprint, with fusion at the score level and the EER was 0.63%. Viriri and Tapamo [5] introduced a multimodal approach including iris and signature biometrics at score level fusion. False Reject Rate (FRR) 0.008% on a False Accept Rate (FAR) of 0.01%.

Kisku et al. [6] proposed a multibiometric system including face and Palmprint biometrics at feature level fusion. The system attained 98.75% recognition rate with 0% FAR.

Meraoumia et al. [7] presented a multimodal biometric system using hand images and by integrating two different modalities Palmprint and finger-knuckle-print (FKP). EER = 0.003 %. Kim et al. [8] introduced a multibiometric system using soft biometrics suitable for video surveillance system, face and gait.

Aggithaya et al. [9] proposed a personal authentication system that simultaneously exploits 2D and 3D Palmprint features. The sum rule classifier achieves the best EER of 0.002.

Kazi and Rody [10] presented a multimodal biometric system using face and signature with score level fusion. The results showed that face and signature based bimodal biometric system can improve the accuracy rate about 10%, higher than single face/signature based biometric system.

Ramachandra and Abhilash [11] itntroduced a multimodal biometric system using face and fingerprint with fusion at feature level. The best recognition rate was 90% at EER 0.13%.

This paper describes the prototype of a multibiometric recognition system based on a fusion of Iris, Palmprint and Finger_Knuckle Print (FKP) biometrics at matching score level. Different fusion rules have been tested to choose the best one that achieves the desired performance and minimum total error.

The remainder of this paper is organized as follows: Section (2) describes proposed multibiometric system. Section (3) analyzes the experimental results. Section (4) concludes the paper.

2. PROPOSED MULTIBIOMETRIC SYSTEM

Fig. 1 shows the block diagram of the proposed multimodal biometric recognition system. First we apply preprocessing to extract the region of interest from each biometric image. Then the feature vectors are extracted from each biometric separately, then extracting the matching scores for each biometric sample from the corresponding templates. The three different matching scores are combined into a unique matching score. Based on this unique matching score, a final decision is made (the user is identified or rejected).

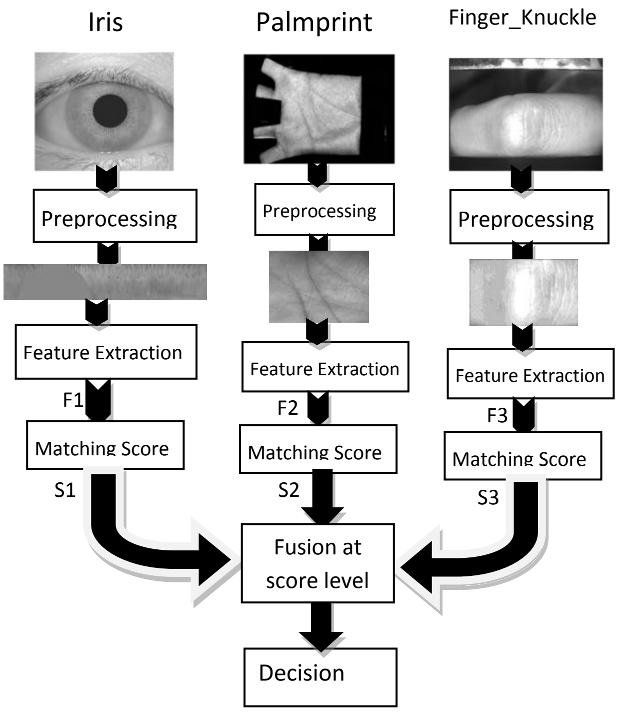

Fig. 1 The block diagram of the proposed system.

2.1 The used unimodal biometric systems

2.1.1 Iris Identification System

Iris recognition is considered to be one of the most accurate biometric technologies when compared to other technologies commercially in use today. This is because the false match and false non-match errors are very small, which implies a very high accuracy.

The Iris identification system consists of three stages, the first stage is the iris analysis which involves iris localization and iris normalization. The second stage is the feature extraction and encoding. The last stage is the recognition stage which involves identification and verification.

We use Daugman's algorithm for performing Iris localization which is based on applying an integro-differential operator to find the iris and pupil contours [12]. Only the significant features of the iris must be encoded in order to generate the iris code for the matching process. In the proposed system, log-Gabor filter [13] [14] is used for extracting the features from the iris images. Finally matching is done using the calculated Hamming distance (HD) [15] which is a measure of the number of different bits between the two iris codes.

2.1.2 Palmprint Identification System

Palmprint based personal verification has quickly entered the biometric family due to its ease of acquisition, high user acceptance and reliability. Palmprint not only has the unique information available as on the fingerprint but has far more amount of details in terms of principal lines, wrinkles and creases.

Palmprint identification system in most cases is similar to Iris system, we use log-Gabor filter for extracting the features [16] [17] from the Palmprint images and Hamming distance for matching stage.

2.1.3 Finger_Knuckle Print Identification System

The usage of Finger_Knuckle images for personal identification has shown promising results and generated a lot of interest in biometrics [18]. Finger_Knuckles of the human hand are characterized by the creases on them. These creases differ from person to person.

In the FKP identification system, after collecting the FKP images then apply preprocessing techniques on all the training images then extract the feature from the finger images. We use Linear Discriminant Analysis (LDA) to extract the only significant features from FKP images and reduce the dimensionality of the feature vector [19] [20].

2.2 Multimodal biometric system score level fusion

Score level fusion refers to the combination of matching scores provided by the unimodal classifiers in the system. This is the most widely used fusion approach, as evidenced by the experts in the field. One could think that merging information from the different modalities at some previous stage of the system (sensor level, feature level) will provide more effectiveness, but there are several reasons that support score fusion, such as conceptual simplicity, ease implementation, practical aspects, etc. Thus, the dominant option in the majority of published papers is score-level fusion [21].

But before the fusion step, in order to combine the matching scores, we should first normalize these scores. There are different types of normalization, Min-max, median-MAD and z-score [21]. We use the first type Min-max which transforms scores into a common range [0, 1]. The normalized scores are given by

$$S_i' = \frac{Si - S_{\min}}{S_{\max} - S_{\min}} \quad (1)$$

Where

S_i' : the normalized matching scores

S_i : the matching scores, i= 1,2, …..

$S_{\min}$ & $S_{\max}$: the min and max match scores

In order to combine the scores reported by the three matchers we can use any score level combinations from sum or average, product, weighted sum rule and min rule.

$$Sum = \sum_{i=1}^{n} S_i \quad (2)$$

$$\Pr oduct = \prod_{i=1}^{n} S_i \quad (3)$$

$$Weighted\ \_Sum = \sum_{i=1}^{n} w_i S_i \quad (4)$$

Where:

N : number of match scores wanted to be fused

S : the matching score

w_i : The weight for each score which calculated as follow

$$W_i = \frac{EER_i}{\sum_i EER} \quad (5)$$

Where EER_i is the unimodal biometric error.

3. EXPERIMENTAL RESULTS

3.1 Databases

In our work we use three different databases for three modalities (Iris, Palmprint and Finger_Knuckle).

For Iris images, we have used CASIA Iris Image Database [22] (ver. 1.0) includes 756 iris images from 108 eyes For each eye, 7 images are captured in two sessions, where three samples are collected in the first session and four in the second session. All iris images are 8 bit gray-level JPEG files, collected under near infrared illumination (fig. 2).

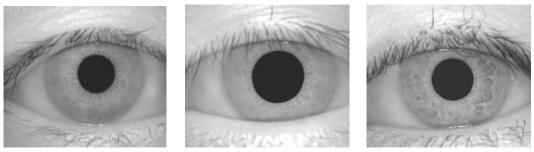

Fig. 2 Sample images for one person from CASIA iris

For Palmprint images, we have used PolyU palmprint database [23] contains 7752 grayscale images corresponding to 386 different palms (10 samples for each hand) (fig. 3).

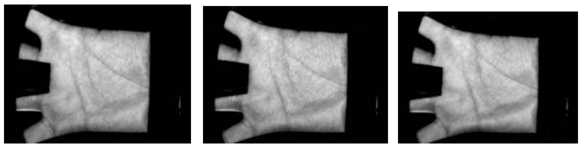

Fig. 3 Sample images for one person from PolyU Palmprint database

For Finger_Knuckle images, we have used database images [24] collected from 165 volunteers, including 125 males and 40 females (fig. 4).

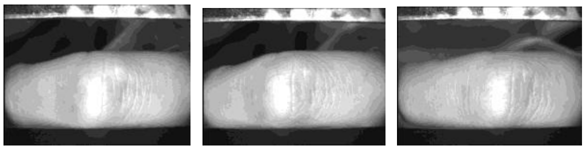

Fig. 4 Sample images for one person from Finger_Knuckle

3.2 Performance measure of the biometric systems

Generally, the performance of the biometric verification system is measured by False Acceptance Rate (FAR) and False Rejection Rate (FRR) or Genuine Acceptance Rate (GAR) [25] [26].

FRR, FAR, GAR and Total Error Rate (TER) are determined as follow:

$$FAR(\%) = \frac{false\ accep\tan ce\ numbers}{No\ of\ imposter\ test} X100\% \quad (6)$$

$$FRR(\%) = \frac{false\ rejection\ numbers}{No\ of\ client\ test} X100\% \quad (7)$$

$$GAR(\%) = 100 - FRR(\%) \quad (8)$$

$$TER(\%) = FRR(\%) + FAR(\%) \quad (9)$$

3.3 Iris Recognition Experimental Results

We have 100 persons, for each one we have 5 Iris images for training and 2 for testing, 8 Palmprint images for training and 4 for testing, also 8 Finger_Knuckle images for training and 4 for testing. 20 imposter persons are used to testing the accuracy of the system (FAR).

Experimental results from (table 1) show that the threshold value is directly proportional to FAR and inversely proportional to FRR. At the threshold value of 0.390, the percentages of FAR and FRR are 7.14 and 1.5 respectively.

Table 1. Experimental results of iris recognition system

Test	No. Training Model (5 samples)	No. Client Model (2 samples)	No. Imposter Model (2 samples)	Threshold	FAR %	FRR %	TER %
1	100	100	20	3.90E-01	7.14	1.50	8.64
2	100	100	20	3.99E-01	14.20	1.50	15.78
3	100	100	20	4.00E-01	16.60	1	17.60

When the threshold is increased FAR is increased and FRR is reduced. The best GAR is 98.5% at total error 8.64%.

3.4 Palmprint Verification Experimental Results

Table 2. Experimental results of Palmprint verification system

Test	No. Training Model (8 samples)	No. Client Model (4 samples)	No. Imposter Model (4 samples)	Threshold	FAR %	FRR %	TER %
1	100	50	20	2.52E-01	2.38	1.92	4.30
2	100	50	20	2.49E-01	1.19	1.92	3.11
3	100	50	20	2.40E-01	0.00	1.92	1.92

At threshold value 0.24, the Palmprint verification system has GAR 98% at 1.92% TER which is the smallest error in the three systems.

3.5 Finger-Knuckle Print recognition Experimental Results

Table 3. Experimental results of FKP recognition system

Test	No. Training Model (8 samples)	No. Client Model (4 samples)	No. Imposter Model (4 samples)	Threshold	FAR %	FRR %	TER %
1	100	100	20	4.99E-01	0.00	5.50	5.50
2	100	100	20	5.99E-01	0.00	2.50	2.50
3	100	100	20	6.50E-01	0.00	2	2.00

The performance of Finger_Knuckle verification experiment is much better than Iris verification system. The best GAR is 98% but this is at TER 2%.

3.6 Matching Score-Level Fusion Experimental Results

The goal of this experiment is to evaluate the system performance when we are using a unimodal biometric system and a multibiometric system using two or three or more biometrics. So after we analyze each unimodal system and see how the accurate choice of the best threshold can affect the accuracies of the system, and getting the best GAR with minimum TER from the three systems.

Now we investigate the integration of the three biometric modalities: Iris, Palmprint and FKP in the biometric recognition system in order to achieve a better performance that may not be achievable by using only one of them.

Table 4. Experimental results of Iris_Knuckle Fusion system using different fusion rules

Fusion rule	No. Training Model	No. Client Model	No. Imposter Model	Threshold	FAR %	FRR %	Total Error rate %
Product	100	100	20	0.19461	4.76	0.00	4.76
Sum	100	100	20	0.884	4.76	1.00	5.76
W_Sum	100	100	20	0.725	0.00	1.00	1.00

Table 5. Experimental results of Iris_Palmprint Fusion system using different fusion rules

Fusion rule	No. Training Model	No. Client Model	No. Imposter Model	Threshold	FAR %	FRR %	Total Error rate %
Product	100	50	20	0.0936	0.00	0.00	0.00
Sum	100	50	20	0.6234	0.00	0.00	0.00
W_Sum	100	50	20	0.489	0.00	0.00	0.00

Table 6. Experimental results of Knuckle_Palmprint Fusion system using different fusion rules

Fusion rule	No. Training Model	No. Client Model	No. Imposter Model	Threshold	FAR %	FRR %	Total Error rate %
Product	100	50	20	0.137	99.03	0.00	0.96
Sum	100	50	20	0.75	98.07	0.00	1.92
W_Sum	100	50	20	0.669	0.00	0.00	0.00

The tables from (table 4 to 6) illustrate the performance of the system when we fused two types of biometrics. As seen in (table 4) we have used Iris and knuckle biometrics with different fusion rules, product, sum and weighted sum. This system gives the best performance when using weighted sum rule, GAR is 99% at TER 1%. This seems logical as the weight of each score is proportional to its accuracies, since the accuracies (FAR, FRR) of knuckle are better than those for iris, so the system is expected to give best performance.

When we used Palmprint and Finger_Knuckle (table 6) the system achieved the best performance also when using the weighted_sum rule, GAR was 100% at TER 0%. But here the weight of Palmprint scores was slightly higher than the Knuckle scores.

When Iris and Palmprint (table 5) were used the system gave the best result with any fusion rule, GAR was 100% at TER 0%.

Moreover, we studied using the fusion of the three biometrics to see how this affects the performance, and as expected it give zero total equal error when using any fusion rule as shown in (table7).

The main goal of these experiments to prove that we can design a system that achieves the desired performance or the best desired performance when using two or three types of biometrics, but these depends on the application.

This means that according to the system security requirements, the system can use the three types of biometrics or choosing randomly only two from them and achieve the desired performance. This is suitable for application that required different levels of security with different costs.

TABLE7. Experimental results of Iris_Knuckle_Palmprint Fusion system using different fusion rules

Fusion rule	No. Training Model	No. Client Model	No. Imposter Model	Threshold	FAR %	FRR %	Total Error rate %
Product	100	50	20	0.025	0.00	0.00	**0.00**
Sum	100	50	20	1.03	0.00	0.00	**0.00**
W_Sum	100	50	20	0.67	0.00	0.00	**0.00**

4. Conclusion

In this paper, a multimodal biometric recognition system using three modalities including Iris, Palmprint and Finger-Knuckle with fusion at matching score level is proposed. Also the effect of different fusion methods and different score normalization methods on the recognition performance of our multimodal biometric system are studied. We show that our system also exhibits an excellent recognition performance and outperforms unimodal systems weather we use two or three biometrics.

This work can be used in the development of multimodal biometric system that can include multiple fusion rules in a dynamic architecture to ensure varying security levels using the adaptive combination of multibiometrics.

5. REFERENCES

[1] A. Ross, K. Nandakumar and A. K. Jain. Handbook of Multibiometrics. Springer, New York, USA, 1st edition, 2006.

[2] Ross, A. and Jain, A. K. “Information Fusion in Biometrics”. 3rd Int'l Conference on Audio- and Video-Based Person Authentication (AVBPA), pp. 354-359, Sweden, June 6-8, 2001.

[3] J. Fierrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero, and J. Gonzalez Rodriguez, ―A comparative evaluation of fusion strategies for multimodal biometric verification,‖in Proc. 4th Int, Conf,Audio-video-based Biometric Person Authentication , J. Kittler and M. Nixon, Eds., 2003 vol. LNCS 2688, pp. 830–837

[4] R. Snelick, U. Uludag, A. Mink, M. Indovina and A. K. Jain, ―Large scale evaluation of multimodal biometric authentication using state-of the-art systems,‖ IEEE Trans. Pattern Anal. Mach. Intell, Vol. 27, No. 3, pp. 450– 455, Mar. 2005.

[5] S. Viriri and R. Tapamo, "Integrating Iris and Signature Traits for Personal Authentication using User-Specific Weighting", 2009.

[6] D. Kisku, P. Gupta and J. Sing, "Multibiometrics Feature Level Fusion by Graph Clustering ", International Journal of Security and Its Applications Vol. 5 No. 2, April, 2011.

[7] A. Meraoumia, S. Chitroub and A. Bouridane, "Fusion of Finger-Knuckle-Print and Palmprint for an Efficient Multi-biometric System of Person Recognition ", IEEE ICC 2011.

[8] M. Kim, H. Moon and S. Pan “Framework of Human Identification using Multi-Modal Biometrics”, International Journal of Multimedia and Ubiquitous Engineering Vol. 7, No. 2, April, 2012.

[9] V. Aggithaya, D. Zhang and N. Luo “A Multimodal biometric authentication system based on 2D and 3D palmprint features”, Proc. of SPIE Vol. 6944 69440C-1-2012.

[10] M. Kazi and Y. Rode,”multimodal biometric system using face and signature : a score level fusion approach” Advances in Computational Research, Vol. 4, No. 1, 2012.

[11] A. Ramachandra and S. Abhilash, “Feature Level Fusion Based Bimodal Biometric Using Transformation Domine Techniques”, IOSR Journal of Computer Engineering (IOSRJCE), No. 3 (July-Aug. 2012).

[12] J. Daugman, “High Confidence Visual Recognition of Persons by a Test of Statistical Independence,” IEEE Trans. Pattern Anal. Machine Intell, vol. 15, pp. 1148-61, 1993.

[13] D.Gabor, “ Theory of communication “, J. inst. Elect. Eng. London, Vol. 93, No. III, 1946.

[14] A. Kumar and A. Passi, “Comparison and Combination of Iris Matchers for Reliable Personal Aauthentication,” Pattern Recogniion., Vol. 23, No. 3, pp. 1016–1026, March 2010.

[15] L. Ma, T. Tan, Y. Wang and D. Zhang, “Efficient Iris Recognition by Characterizing Key Local Variations”, IEEE Transactions on Image Processing, Vol. 13, No. 6, June 2004, pp739-750.

[16] R. Chu, Z. Lei, Y. Han, S.Z. Li,” Learning Gabor magnitude features for palmprint recognition”, ACCV, 2007, pp. 22–31.

[17] A. Kong, “Palmprint Identification Based on Generalization of IrisCode”, PhD Thesis, University of Waterloo, Canada, 2007 (available at http://uwspace.uwaterloo.ca/handle/10012/2708)

[18] A. Kumar and C. Ravikanth, “Personal authentication using finger knuckle surface”, IEEE Trans. Info. Forensics & Security, vol. 4, no. 1, pp. 98-110, March 2009

[19] H. Yu and J. Yang, "A direct LDA algorithm for high dimensional data with application to face recognition," Pattern Recognition, September 2001.

[20] P. Navarrete and J. Ruiz-del-Solar, "Analysis and Comparison of Eigenspace-Based Face Recognition Approaches," International Journal of Pattern Recognition and Artificial Intelligence, Vol. 16, No. 7, November 2002.

[21] A. Pour, K. Faez, and R. Amirfattahi "Multimodal biometric system using face, ear and gait biometrics", 10th International Conference on Information Science, Signal Processing and their Applications (ISSPA 2010).

[22] Chinese Academy of Science - Institute of Automation, Database of the Eye Grayscale Images. http://www.sinobiometrics.com

[23] PolyU Palmprint Palmprint Database, http://www.comp.polyu.edu.hk/~biometrics/

[24] L. Zhang, "Finger-Knuckle-Print: A new Biometric Identifier", ICIP 2009.

[25] T. Sabareeswari and S. Stuwart," Identification of a Person Using Multimodal Biometric System", International Journal of Computer Applications (0975 – 8887) Vol. 3 – No.9, July 2010

[26] L. Hong and A. Jain, "Integrating faces and fingerprints for personal identification", IEEE Trans. Pattern Anal. Mach. Intell. , Vol. 20, No. 12, pp. 1295– 1307, December 1998