Personal authentication using hand-geometry and palmprint features – the state of the art

N. Pavešić[1)], S. Ribarić[2)], D. Ribarić[3)]
[1)] *Faculty of Electrical Engineering, University of Ljubljana, Slovenia*
[2)] *Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia*
[3)] *Intelligent Informatics System, Zagreb, Croatia*
nikola.pavesic@fe.uni-lj.si, slobodan.ribaric@fer.hr, damir.ribaric@zg.hinet.hr

Abstract

In this paper we present an overview of the fundamentals of personal authentication based on hand-geometry measurements and palmprint features. Unimodal and multimodal hand-based systems and technologies are presented, and various levels of fusion for hand-based biometric systems are discussed. Finally, a description of the design and development of a multimodal personal authentication system based on the fusion of hand-geometry and palmprint features at the matching-score level is given.

1. Introduction

Biometrics is a scientific discipline that involves methods of identifying people by their physical and/or behavioural characteristics. The most common physical and behavioural characteristics of an individual used for automatic biometric authentication are as follows: fingerprint, hand-geometry, palmprint, face, iris, retina, DNA, ear, signature, speech, keystroke dynamics, gesture and gait [1], [2] and [3].

A biometric authentication (identification or verification) system uses pattern recognition to automatically recognize an individual on the basis of a measurement of a specific physiological or behavioural characteristic that the individual possesses. An authentication system consists of the following basic modules: sensor, feature generator, matcher, decision and template database; see Fig. 1.

In the feature-generator module the set of discriminatory features is extracted from the raw measurements of an individual biometric characteristic. The matcher module compares the templates (mathematical representations of the features set) against the templates stored in the template database in order to generate matching scores, while the final decision concerning the user's identity (identification) or the user's claimed identity (verification) is taken in the decision module.

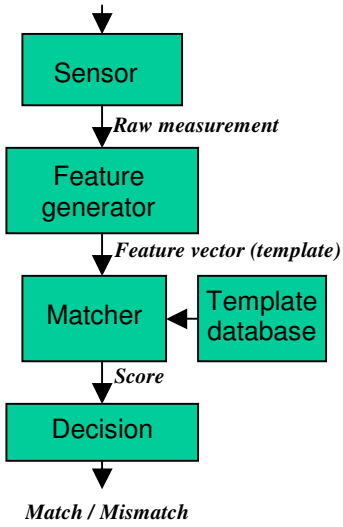


Figure 1. The basic modules of a biometric system.

The most frequently used measures to rate the accuracy of a biometric authentication system are as follows: *false-accept-rate* (FAR), the frequency with which an impostor is falsely accepted; and *false-reject-rate* (FRR), the frequency with which a genuine user is rejected. The error rate at which the FAR equals the FRR, the *equal-error-rate* (EER), is (normally) used as a comparison metric for different biometric systems.

Biometric systems based on a single biometric characteristic are referred to as *unimodal* systems. There are several human and technical factors that influence the performance and operation of a unimodal system, among the most important are the following [2], [3]: *universality*,

each person should have the biometric characteristic being acquired; *uniqueness*, there are no two persons that are the same in terms of the biometric characteristic; *permanence*, the biometric characteristic should be time-invariant; *collectability of the biometric characteristic*, the biometric characteristic can be measured quantitatively; *performance*, the achievable recognition accuracy, speed and robustness of the biometric system; *acceptability,* to what extent people are willing to accept the biometric system; *circumvention,* how easy it is to fool the biometric system by fraudulent techniques; *scalability*, the feasibility of authenticating people in a large population without unacceptable error rates or throughput times; *maturity of the technology*, the stage of development of the biometric system's technology; and *cost*, an estimation of the total cost to deploy a biometric system. Table 1. presents a comparison of the most common unimodal biometric systems in terms of the above factors.

Table 1. Comparison of the human and technical factors of seven popular unimodal biometric systems. H, M, and L denote high, medium, and low, respectively.

	Fingerprint	Face	Hand geometry	Palmprint	Iris	Voice	Signature
Universality	M	H	M	M	H	M	L
Uniqueness	H	L	M	H	H	L	L
Permanence	H	M	M	M	H	L	L
Collectability	M	H	H	H	M	M	H
Performance	H	L	M	H	H	L	L
Acceptability	M	H	M	M	L	H	H
Circumvention	M	H	M	L	L	H	H
Scalability	H	M	L	H	H	L	H
Maturity	H	M	H	L	M	M	M
Cost	M	L	H	M	H	L	M

Unimodal biometric systems are usually more cost-efficient than multimodal systems. However, a single physical or behavioural characteristic of an individual can sometimes fail to be sufficient for identification. For this reason, multimodal biometric systems, i.e., systems that integrate two or more different biometric characteristics, are being developed to increase the accuracy of decisions and to decrease the possibility of circumventing the system [4]. In general, multimodal biometric systems require integration schemes to fuse the information obtained from the individual biometric modalities. This fusion process can be performed at four different levels: sensor, feature-generation, matching and decision; see Fig. 1.

Generally, a biometric system can be classified according to the method used for capturing and processing the biometric characteristic, i.e., an *on-line* or an *off-line* system. An on-line system captures the biometric characteristics of a person who is physically present at the point of authentication by means of a sensor that is directly connected to a computer for real-time processing, while an off-line system processes previously captured biometric characteristics and the authentication is not performed in real-time.

The biometric system that uses hand-based features is one of the seven leading biometric technologies, and had 11% of the world market in 2004 [4]; see Fig 2. Since the shape of the human hand is not a highly distinctive characteristic, hand-geometry-based systems are used for physical access control, and time and attendance applications. On the other hand, palmprint-based systems, due to the uniqueness and permanence of palmprint features, are typically used in criminal forensic applications.

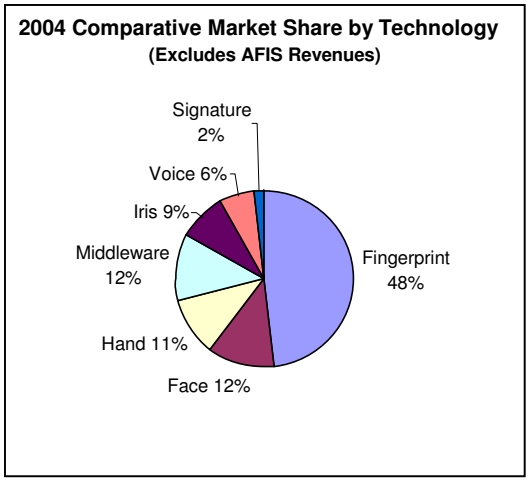
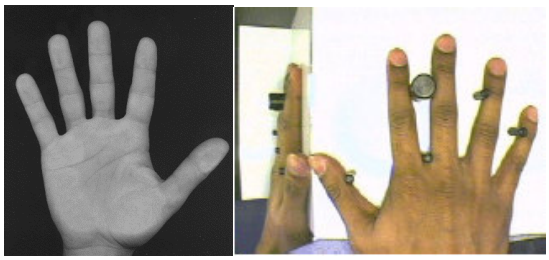


Figure 2. Biometric Market Report (International Biometric Group©) estimates the revenues of various biometrics in 2004 in terms of market share. Note that AFIS are used in forensic applications.

The human hand contains a wide variety of measurable characteristics, e.g., shape, palmprint, fingerprints on the palmar surface of the hand, and veins on the dorsum of the hand, that can be used by biometric systems. Fig. 3 shows typical images of a) the palmar, b) the lateral and c) the dorsal surfaces of the hand.

From these images three classes of biometric features can be extracted: *hand-geometry features,* (e.g., width, thickness and area of the palm, lengths, widths and thickness of fingers), *palmprint features* (e.g., principle lines, wrinkles, ridges, texture), and *fingerprints features* (e.g., minutiae locations, types, number). These characteristics of the human hand are relatively stable and the hand image from which they are extracted can be acquired relatively easily.



(a) (b) (c)

Figure 3. Typical images of: a) the palmar [25], b) the lateral [10] and c) the dorsal [10] surfaces of the hand.

The image of the palmar surface of the hand is usually acquired by a scanner rated at 180 dots per inch (dpi)/256 grey levels (see Fig. 3 a)) or by a low/medium-resolution CCD camera, located under the transparent platform where the hand is placed. In contrast, the lateral and dorsum surfaces of the hand (see Fig. 3 b) and 3 c)) are captured with a CCD camera placed above the platform with a side-mounted mirror inclined at 45^{o} to the platform. There are usually 4–6 pegs on the platform to guide the placement of the user's hands.

The hand biometrics *shape, palmprint* and *fingerprint* are particularly convenient for fusion because they can be extracted from a single-shot measurement; see Fig. 3 a).

2. Systems based on images of the lateral and dorsal surfaces of the hand

In the literature, several prototypal biometric authentication systems based on extracting a set of hand-geometry features from images of the lateral and dorsal hand surfaces have been proposed.

2.1 Hand-geometry-based systems

Hand-geometry-based authentication systems have been available for more than thirty years. Several companies launched such systems during the 1980s [6], [7] and [8]. With the exception of available information in the form of patents there is no accessible literature referring to research in this area during that period. Some results of recent research and developed prototypes are described below.

Golfarelli et al. [9] described an *on-line* biometric system based on 17 hand-geometrical features, extracted from the image by means of an ad-hoc feature-extraction algorithm. Fig. 4 shows the characteristic points and the geometrical features used in the system.

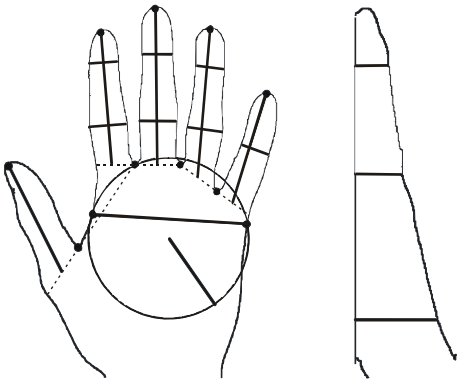


Figure 4. The characteristic points and the 17 geometrical features [9].

100 people took part in a test session where 8 different images of their right hand were taken. With the Bayes classification rule in the matcher module an EER equal to 0.12% was obtained.

Jain et al. [10] described the prototype of an *on-line* verification system based on 16 hand-geometrical features: the length, the width and the thickness of fingers and the widths of the palm (see Fig. 5).

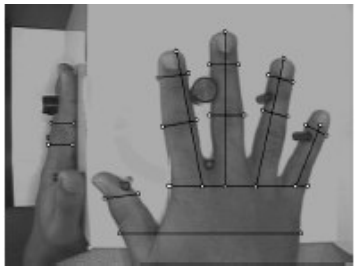


Figure 5. The 16 geometrical features [10].

In the verification phase a 16-dimensional feature vector (stored template) is associated with the claimed identity. This feature vector is then compared with a feature vector of the hand whose identity has to be verified (live template). The system was trained and tested using a database of 50 users. Ten images of each user were captured. Out of 500 images only 360 were used for testing the system (the remaining 140 images were

discarded due to incorrect placement of the hand). The performance of the system for 4 different operating points is displayed in Table 2.

Table 2. The results of the system performance testing [2].

FRR	FAR
1 in 33 (3%)	1 in 7 (15%)
1 in 20 (5%)	1 in 10 (10%)
1 in 10 (10%)	1 in 20 (5%)
1 in 3 (30%)	- (0%)

Sanches-Reillo et al. [11] defined and implemented an *on-line* biometric system based on an optimal set of hand-geometry features. After the capturing and pre-processing of the hand images the measurement algorithms are applied. The main distances and angles of the hand are divided into four different categories: width, lengths, deviations, and angles between the inter-finger points. Thirty-one features are extracted, and after applying a discriminatory analysis a feature vector consisting of 25 components is obtained. The feature vectors are the inputs for a comparison process used to determine the identity of the user whose hand has been captured. The nearest-neighbour (1-NN) classifier based on the Euclidean distance d_E and the Hamming distance d_H, the Gaussian Mixture Models (GMM) and the Radial Basis Function (RBF) Neural Networks are used for the classification and verification. The system was trained and tested using a database of 200 images of 20 users. Table 3 summarizes the results of the biometric recognition testing. In the biometric verification testing an EER < 5% is obtained independently of the classification technique and feature vector size used.

Table 3. Percentage of biometric recognition (classification) success compared to the enrolment set size and the feature vector size.

		d_E	d_H	GMM	RBF
No. of enrolment vectors	3	86%	75%	88%	90%
	4	85%	82%	93%	91%
	5	86%	87%	96%	91%
Feature vector size (5 enrol. vectors)	25	86%	87%	96%	91%
	21	84%	86%	97%	95%
	15	86%	88%	96%	89%
	9	77%	75%	91%	82%

Jain et al. [12] presented an authentication method based on the deformable matching of hand shapes. The proposed authentication method is performed in 5 steps: peg removal from the image, contour extraction, finger extraction and alignment, pairwise distance computation and verification (comparison of the Mean Alignment Error (MAE) with a decision threshold T). The system was tested on a database consisting of 353 (2 to 15 images per person) grey-scale hand images (resolution 480 x 485) of 53 people. The best results, i.e., 2% FAR and 3.5% FRR, were obtained for a decision threshold equal to 1.80.

2.2 Finger-geometry-based systems

There are commercial verification systems available that are based on measurements of only 1 or 2 fingers [13]. The single-finger geometry-based biometric system uses only the index finger. This finger pushes a plunger/button, which goes into the device. The rollers, which scan the finger, take measurements of 12 cross-sections of 1½ phalanx of finger.

The two-finger geometry-based biometric system uses a camera-based sensor system to take 3-dimensional measurements of the index and middle finger. From the image a set of the fingers' geometrical features (length, width and thickness of fingers measured on different finger sections) is extracted.

3. System based on the image of the palmar surface of the hand

From an image of the palmar surface of the hand the hand-geometry, the palmprint and the fingerprint features can be extracted. In this paper we will confine ourselves to a description of biometric systems based on hand-geometry and palmprint features.

3.1 Palmprint-based systems

The palm is the inner surface of the hand between the wrist and the fingers. The palmprint is a rich source of information that is useful for personal authentication. The most important features are the three principal lines (the heart line, the head line, and the life line), wrinkles, and ridges. Fig. 6 shows the image of a palmprint and 6 straight black lines that point out the principal lines, the wrinkles and the ridges.

Palmprint-based biometric (*on-line* or *off-line*) systems can be classified according to the applied feature-generation method into systems that extract features in the *original image space* or in the *transformed image space*.

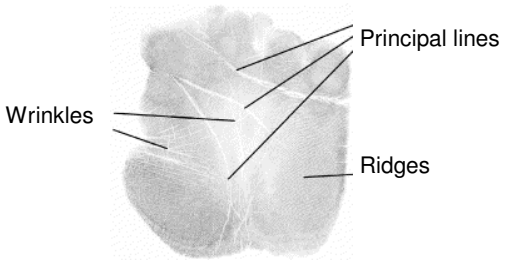


Figure 6. The palmprint image.

3.1.1 Systems based on features extracted in the original image space.

Zhang et al. [14] described an *off-line* palmprint-based verification system based on the end-points and the middle points of the principal lines (datum points) and line-feature matching. For each line segment three features are computed: slope, intercept and angle of inclination. These features, obtained from the lines of two palmprints, are inputs in an invariant line-segment feature-matching process. Two line segments are declared to be the same ***if*** the Euclidian distances between the end-points are less than some threshold D, ***and*** the difference in the angle of inclination is less than some threshold E ***and*** the difference in the intercepts is less than the threshold B, where the thresholds are experimentally determined. The palmprint verification system was tested with 20 pairs of palmprint images from 20 right palms. The experimental results of the identity verification showed the effectiveness of the palmprint verification by obtaining an EER = 0.0% at a decision threshold value of 0.2. The experiments were conducted on 400 x 400 grey-scale inked palmprint images at a resolution of 100 dpi, 256 grey levels.

Duta et al. [15] investigated the feasibility of person identification based on feature points extracted from palmprint images. Their approach is based on a set of feature points extracted from along the principal lines and the associated line orientation. For each palmprint a set of approximately 300 feature points is extracted according to an original algorithm. The decision as to whether two palmprints belong to the same hand is based on computing the matching score between the corresponding sets of feature points of the two palmprints. The matching technique is based on the non-linear deformations of the two sets. The paper palmprints were scanned at a resolution of 200 dpi (image-size 400 x 300 with 256 grey levels). A data set consisting of 30 (15 of each of the two hands) palmprint images of three people was used for experimental purposes. The overlap between the user (genuine) and the impostor distributions is reported to be approximately 5%.

The paper of *P. Ying-Han et al.* [16] introduces an experimental evaluation of the effectiveness of utilizing three well-known orthogonal moments, i.e., Zernike moments, pseudo Zernike moments and Legendre moments, in the application of palmprint verification. These orthogonal moments are able to define statistical and geometrical features containing line-structure information about a palmprint. Experimental results have shown that the performance of the system depends on the moment order as well as on the type of moments. Pseudo Zernike moments of the order of 15 showed the best performance from among all the moments. Its verification rate is 95.75% with FAR = 4.25% and FRR = 4.47% at a decision threshold value of 0.495, which also represents the overall performance of this palmprint verification system. Experiments were conducted using a database consisting of 50 different palmprint classes, with 6 samples for each class.

You et al. [17] proposed a palmprint identification system based on a dynamic selection scheme to facilitate a fast search for the best matching of a palmprint template in the database in a hierarchical fashion. The global texture energy is introduced to guide this dynamic selection of a small set of similar candidates from the database at a coarse level for further matching. At the fine-level identification the same procedure is used as in [14].

C. C. Han et al. [18] described an *on-line* scanner-based personal verification system based on palmprint features. These palmprint features are extracted from the region-of-interest (ROI): the square region in the palm; see Fig. 7.

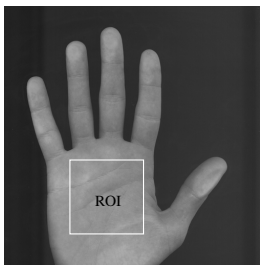


Figure 7. The palmprint region-of-interest.

The multi-resolution feature vectors are derived from the ROI using three different grid sizes (32 x 32, 16 x 16 and 8 x 8). Each component of the feature vector is represented by the mean value of the pixels in the grid element. Two techniques were designed for the identity verification: the multiple-template matching method and the back-propagation neural network method. The hand images of size 845 x 829 in grey-scale format at a resolution of 100 dpi are captured by a scanner. For experimental purposes the 30 hand images of 49

individuals were obtained to construct the database. The best-obtained accuracy rate was 98%.

3.1.2 Systems based on features extracted in the transformed image space.

G. Lu et al. [19] used eigenpalms for palmprint recognition. The images of the palmprints are captured at a resolution of 484 x 384 pixels. They are then aligned and their size is normalized. From these images the palm sub-images with a fixed size (128 x 128 pixels) are extracted and transformed using the Karhunen–Loeve transformation. The extraction of the features involves the proposed eigenspace method with feature-vector lengths of 50, 100, 150 and 200. Classification was performed using a nearest-neighbour classifier based on the weighted Euclidean distance. The test database consists of 191 people, each of whom provided 8 images of their left palm and 8 images of their right palm. Experiments using different numbers of training samples of each person and different lengths of the feature vector are described. The best recognition rate of 99.149% was achieved for 4 training samples and 100 features. Error rates of FAR = 1% and FRR = 0.03% at a decision threshold value of 0.71 were also reported.

W. Li et al. [20] describe a feature-extraction method based on converting a palmprint image from a spatial domain to a frequency domain using a Fourier transform. The features extracted in the frequency domain are used as indexes to the palmprint templates in the database, and the searching process for the best match is conducted in a layered fashion. The experimental results show that palmprint identification based on feature extraction in the frequency domain is effective in terms of accuracy and efficiency. Table 4 shows the results of testing.

Table 4. The results of the palmprint performance testing.

Palmprint images in the database	500
Attempts in testing	2500
Correct answers	2387
Identification rate	95.48%
Average response time (s)	2

The papers of *W. K. Kong et al.* and *D. Zhang et al.* [21], [22] describe an *on-line* palmprint-based system based on the use of an adjusted 2-D Gabor filter to obtain texture information from the palmprint, and a comparison of two 2049-dimensional texture feature vectors using the normalized Hamming distance. In terms of accuracy the best results are obtained using the following filter parameters: orientation equal to $\pi/4$, frequency of the sinusoidal wave equal to 0.0916, and the standard deviation of the Gaussian envelope equal to 5.6179. On a palmprint-images database containing 7752 images collected from 193 individuals, a system EER of 0.6% was reported.

In *X. Wu et al.* [23] an *off-line* palmprint-based verification system based on the use of Fisher's linear discriminant (FLD) was described. The palmprint image is projected from the high-dimensional original palm space to the low-dimensional Fisherpalms space. A database with 3000 palmprint images from 300 different palms was used for testing purposes. For the palmprint region-of-interest with resolution 128 x 128, 64 x 64 and 32 x 32, the feature vector of each testing palmprint is matched against each stored template at each resolution. A nearest-neighbour classifier based on the Euclidean distance is used. The EERs at the 128 x 128, 64 x 64 and 32 x 32 resolutions are 1.00%, 0.95% and 0.82%, respectively.

3.2 Systems based on the fusion of palmprint and hand-geometry features

Shu et al. [24] presented a prototype of an *off-line* system based on the following palmprint features: geometrical features (width, length and area of the palm), principal-line, wrinkle and delta-point features, and minutiae. Principal-line and wrinkle features obtained from a low-resolution image (100 dpi), and delta-point features and minutiae features extracted from a high-resolution image (400 dpi), are fused at the sensor level. The authors evaluated the FAR and FRR for different combinations of palmprint features. Their experiments showed that the combination of eight points on the principal-lines and palm-geometry features gives an acceptable identification accuracy, i.e., FAR = 0.2% and FRR = 0.0%, at the decision threshold T_0. All experiments were carried out on a database containing 48 pairs of prints of the same palm and 844 pairs of prints of different palms.

The paper "A Biometric Identification System based on the Fusion of Hand and Palm Features" by *S. Ribarić et al.* [25] describes the design and development of a prototype system for the on-line identification of an individual based on the fusion of palm features, finger- and palm-geometry parameters. Information fusion at the matching-score level, where the three matchers are combined, is discussed. After training with the template files of 50 people, the system was tested with the template files of 61 people not "seen" during the training phase. The test performance of the system based on the fusion of palmprint features, finger geometry and palm geometry was reported to be FAR = 0.0% and FRR = 1.7%. The FAR and FRR, where the *total-error-rate* TER (TER =

FAR + FRR) achieves a minimum, are displayed in Table 5 for different unimodal and multimodal systems.

Table 5. Performance scores for minimum total error rate for unimodal systems: FG finger-geometry features; PG palm-geometry features; P palmprint features, and on the systems based on the fusion of these features (e.g., FG-P denotes the fusion of finger-geometry (FG) and palmprint (P) features).

	FAR	FRR
FG	0%	5.2%
PG	32.6%	27.7%
P	8.1%	6.1%
FG-PG	0%	4.6%
PG-P	2.6%	2.3%
FG-P	0%	1.8%
FG-PG-P	0%	1.7%

The design and implementation details, as well as the experimental testing of an improved version of the system are given in Section 4.

The paper by *A. Kumar et al.* [26] describes improvements to the performance of an *on-line* palmprint-based verification system by integrating hand-geometry features. A digital camera (1280 x 960 pixels) is used to acquire the hand images. The acquisition setup is inherently simple and does not use any pegs, but users were requested to make sure that their fingers do not touch each other and that most of their hand's back side touches the table. After image pre-processing, extraction of the palmprint image and its normalization, the palmprint feature vector is represented by standard deviations in the n overlapping blocks within the palmprint ROI. Additionally, a total of 16 hand-geometry features are used: 4 finger lengths, 8 finger widths, palm width, palm length, hand area, and hand length. These two feature vectors are used for information fusion at the feature-generation level, as well as at the decision level. Experimental results on the image dataset of 100 users are displayed in Table 6.

Table 6. Performance scores for minimum total error rate on 472 test images. FGL and FDL denote fusion at feature generation level and fusion at decision level, respectively.

	FAR	FRR	Threshold
Palmprint	4.49%	2.04%	0.9830
Hand-geometry	5.29%	8.34%	0.9314
FGL	5.08%	2.25%	0.9869
FDL	0%	1.41%	0.9840

Jain et al. [27] describes realization of a multimodal biometric verification system based on face, fingerprint and hand-geometry features that uses fusion at the matching-score level based on learning user-specific matching thresholds as well as the weights of an individual biometric characteristic.

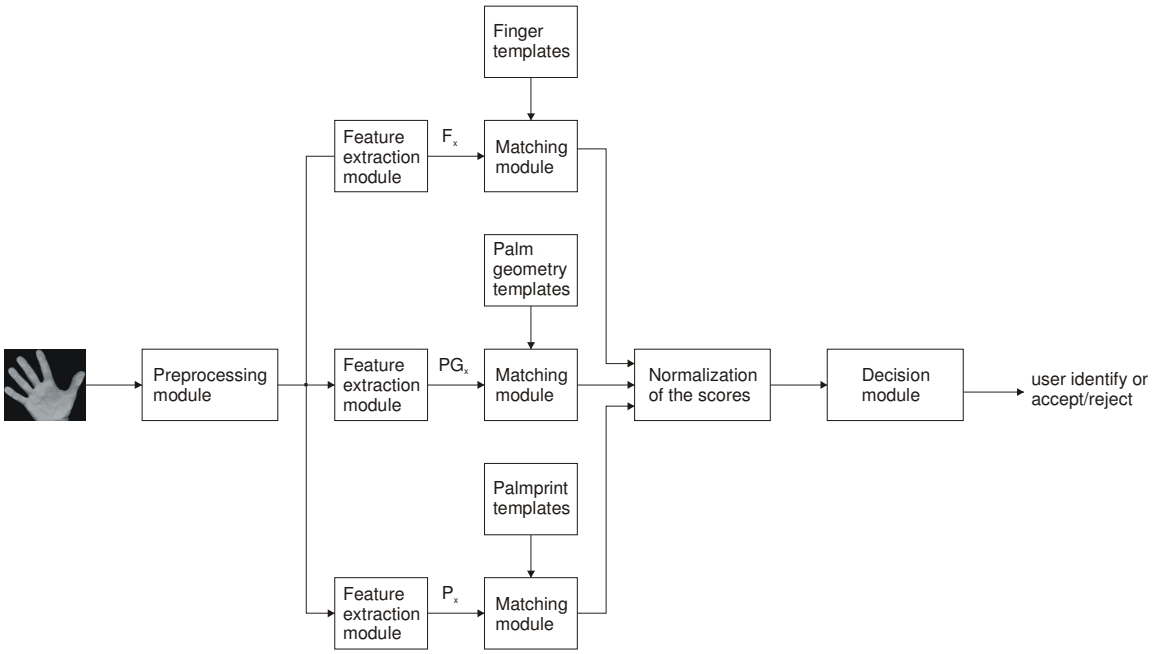


Figure 8. A block-diagram of the multimodal biometric identification system based on the fusion of finger-, palm-geometry and palmprint features at the matching-score level.

4. Design of a three-modal hand-based system

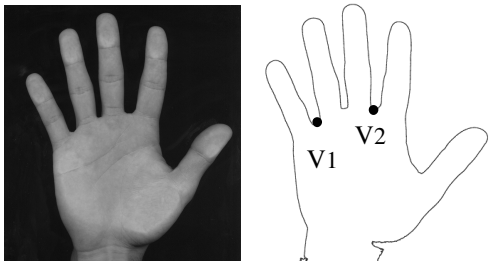
In this section the prototype of an on-line hand-based multimodal authentication system [28] is described. The system is based on the fusion of finger- and palm-geometry features, as well as palmprint features at the matching-score level.

4.1 System description

The block diagram of the proposed system is shown in Fig. 8.

A desktop scanner (180 dpi, 256 grey levels) is used to acquire the hand images. The user is asked to put his/her hand on the flat glass surface of the scanner, with the fingers spread naturally. There are no pegs for controlling the placement of the hand, and there are no requirements for any additional illumination. All the biometric features, i.e., finger-, palm-geometry and palmprint features, are obtained from the hand image in a single shot. Fig. 9 a) shows a typical image obtained by the input device.

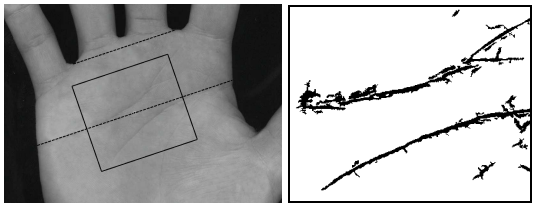
During the pre-processing phase, by applying thresholding the hand is extracted from the image background. Due to the regular and light-controllable conditions of the image-capturing, global thresholding provides satisfactory results. By using a modified contour-tracking algorithm [29], the contour of the hand is extracted (see Fig. 9 b)).



(a) (b)

Figure 9. a) Example of an image of the right hand obtained with a desktop scanner; b) Extracted contour of the hand showing the two reference points (V1 and V2).

From the hand contour two stable points are determined (V1 and V2); see Fig 9 b). Point V1 is used to determine the sub-region (120 x 60 pixels) of the palmprint where a segment of the heart line can be detected. The third stable point is defined as a point on the heart line. It is detected by subsequently applied operations as follows: convolution with a Gaussian mask, Sobel operator, hysteresis thresholding and horizontal projection. These points (V1, V2 and the point on the heart line) are used to define the palmprint's region-of-interest (ROI) with dimensions 315 x 285 pixels. Applying the same sequence of operations the principal lines in the ROI are detected (see Figs. 10 a) and 10 b)).

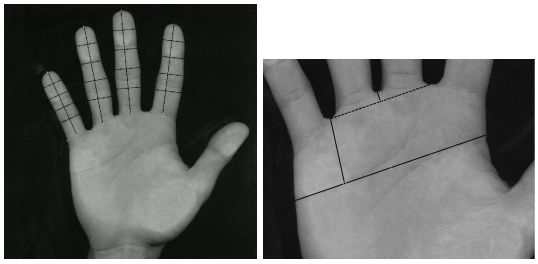


(a) (b)

Figure 10. a) The palm region-of-interest (ROI); b) Pre-processed ROI.

In the feature-extraction modules the three feature vectors F_x, PG_x and P_x are obtained. The 20-component vector F_x contains the features of the four fingers (the lengths and four widths of each finger measured at different heights); see Fig. 11 a).

The 4-component vector PG_x carries information about simple palm-geometry (the width of the palm, the distance between points V1 and V2, and the two distances between the line segments; see Fig. 11 b)).



(a) (b)

Figure 11. a) Finger-geometry features; b) Palm-geometry features.

The 399-component vector P_x relies on palmprint attributes, i.e., on the palmprint's principal lines and texture. The matching between the live-template (represented by 3 feature vectors: F_x, PG_x and P_x) and the user template (F_u, PG_u and P_u) stored in the database is based on a computation of the Euclidian distances: $d(F_x, F_u)$, $d(PG_x, PG_u)$ and $d(P_x, P_u)$. These distances are normalized and transformed into similarities S^F_{xu}, S^{PG}_{xu} and S^P_{xu}. These transformations are performed by three transition functions that are determined experimentally during the learning phase of the system.

The fusion is performed in the decision module, where the total similarity measure $TSM_{xu} = w_1 S^F_{xu} + w_2 S^{PG}_{xu} + w_3 S^P_{xu}$ is computed. The values of the weights are proportional to the three-unimodal system performances. The final decision as to whether the live template matches with the user template is based on an additional rule. This rule requires that the similarity between the live and the user templates has to exceed some decision threshold value. This value is determined during the system validation phase.

In the case that the system is used for identification purposes, then the additional rule (k, l)-NN; (k = l = 3) has to be applied in the decision module.

4.2 Experiment and results

The verification experiments were done on a database consisting of two parts: a user database and an impostor database. The user database consisted of the images of 110 people, with 7 hand images per person. Three of these 7 images were used in the enrolment stage, to create the user database, and the remaining 4 were used for testing. The impostor database consisted of 399 images of 57 people (7 images per person). This setup makes possible 440 (110 x 4) user experiments and 399 impostor experiments. The impostor database was also used as a training database in the template-generation process.

The verification experiments were done as follows: After entering the user PIN code and capturing the user hand image, the system calculates the total similarity measure (TSM) between the live-template and all the corresponding templates in the user database (there are 3 user templates). In the next step, the final decision (the user is accepted or rejected) is based on thresholding with the decision threshold T:

if

$$\min_i \{TSM_i\} \geq T; i = 1,2,3$$

then the user represented by the live template is accepted as a user registered in the database with the corresponding PIN code.

otherwise, the person represented by the live template is rejected as an impostor.

The results, expressed in terms of FRR and FAR, vary depending on the decision threshold value T. Fig. 12 presents the verification test results and shows the dependency of the FAR and the FRR on the threshold value.

From Fig. 12 it can be seen that the described verification system achieves an EER equal to 0.41% at the decision threshold T = 0.814, and a minimum total error rate equal to 0.75% is achieved at T = 0.82. It achieves FAR = 0%, FRR = 0.68% at T = 0.86 and FRR = 0%, FAR = 1.18% at T = 0.78.

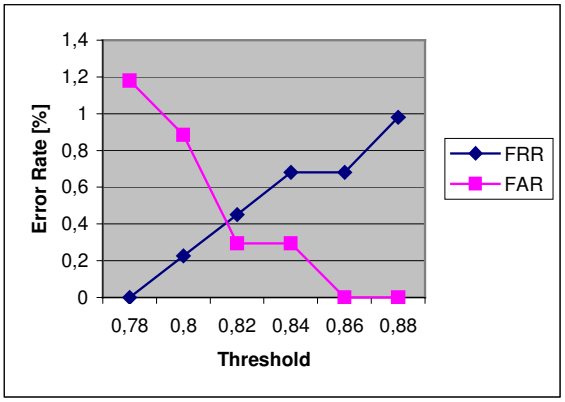


Figure 12. Verification test results, the dependence of the FAR and the FRR on the threshold value.

5. Summary

This paper presents an overview of biometric hand-based systems. Systems based on images of the lateral and dorsal surfaces of the hand, as well as systems based on the image of the palmar surface of the hand are described.

In spite of the fact that hand-geometry features (finger length, width, thickness, curvatures and the relative location of these features) are not unique, hand-geometry-based biometric systems are attractive for a number of reasons. Hand-geometry measurements are easily collectible and non-intrusive, template generation is fairly simple, template size does not exceed 100 bytes, and a stand-alone system is easy to build [2].

The finger-geometry-based biometric systems are smaller than those based on complete hand-geometry parameters, they also tend to be low cost and user friendly (no "criminality" feeling). The main drawbacks of such systems are the low uniqueness and accuracy, as well as the low scalability.

Palmprint authentication is one of the relatively new biometric technologies. Palmprint-based biometric systems, due to the uniqueness and permanence of the palmprint features, are considered as highly accurate and scalable systems.

Multimodal biometric systems increase the performance as well as the scalability, and they are generally more robust to fraudulent technologies. Multimodal authentication systems based on the integration of hand-geometry and palmprint features at the different fusion levels, are described in the paper. The

implementation details of a system based on the fusion of finger-geometry, palm-geometry and palmprint features at the matching-score level are given.

For still higher accuracy and scalability, we propose the development of a multimodal system that integrates features extractable from the palmar surface images, such as finger-geometry, palm-geometry, palmprint and fingerprint features. Such a system could also be interesting because all these features can be obtained from just one high-resolution single-shot image.

6. References

[1] D. Zhang, Automated Biometrics: Technologies & Systems, Kluwer Academic Publishers, USA, 2000.

[2] R.M. Bolle, J.H. Connell, S. Pankati, N.K. Ratha and A.W. Senior, Guide to Biometrics, Springer-Verlag, 2003.

[3] A. K. Jain, A. Ross and S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Tr. on CSVT, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, 2004, pp. 4-20.

[4]International Biometric Group, http://www.biometricgroup.com/reports/

[5] S. Prabhakar, S. Pankanti and A.K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security and Privacy Magazine, Vol. 1, No. 2, 2003, pp. 33-42.

[6] Recognition Systems Inc, http://www.recogsys.com.

[7] B. Spencer, "Biometrics in Physical Access Control Issues", Status and Trends, http://www.recogsys.com

[8] R. Zunkel, "Hand Geometry-based Verification", in [1], pp. 87-101.

[9] M. Golfarelli, D. Maio and D. Maltoni, "On the Error-Reject Trade-Off in Biometric Verification Systems", IEEE Tr. on PAMI, Vol. 19, No. 7, 1997, pp.786-796.

[10] A. K. Jain, A. Ross and S. Pankanti, "A Prototype Hand Geometry-based Verification System", 2nd Int. Conference on Audio- and Video-based Personal Authentication (AVBPA), Washington, March 1999, pp. 166-171.

[11] R. Sanchez-Reillo, C. Sanchez-Avila and A. Gonzalez-Marcos, "Biometric Identification Through Hand Geometry Measurements", IEEE Tr. on PAMI, Vol. 22, No. 10, 2000, pp. 1168-1171.

[12] A. K. Jain and N. Duta, "Deformable Matching of Hand Shapes for Verification", Proceedings of IEEE International Conference on Image Processing, Kobe, October 1999, 5 pages.

[13] BioMet Partners Inc., http://www.biomet.ch/.

[14] D. Zhang and W. Shu, Two Novel Characteristics in Palmprint Verification: Datum Point Invariance and Line Feature Matching, Pattern Recognition 32, 1999, pp.691-702.

[15] N. Duta, A. K. Jain and K. V. Mardia, Matching of Palmprints, Pattern Recognition Letters, Vol. 23, No. 4, 2002, pp. 477-485.

[16] P. Ying-Han, T.B.J. Andrew, N.C.L. David and F.S. Hiew, "Palmprint Verification with Moments", Journal of WSCG, Vol.12, No.1-3, WSCG'2004, Feb 2-6, 2003.

[17] J. You, W. Li and D. Zhang, "Hierarchical Palmprint Identification via Multiple Feature Extraction", Pattern Recognition 35, 2002, pp. 847-859.

[18] C-C. Han, H-L. Cheng, C-L. Lin and K-C. Fan, "Personal Authentication Using Palm-print Features", Pattern Recognition 36, 2003, pp. 371-381.

[19] G. Lu, D. Zhang and K. Wang, "Palmprint Recognition using Eigenpalms features", Pattern Recognition Letters 24, 2003, pp. 1463-1467.

[20] W. Li, D. Zhang and Z. Xu, "Palmprint Identification by Fourier Transform", IJPRAI, Vol. 16, No. 4 (2002), pp. 417-432.

[21] W. K. Kong, D. Zhang and W. Li, "Palmprint Feature Extraction using 2-D Gabor Filters", Pattern Recognition 36, 2003, pp. 2339-2347.

[22] D. Zhang, W. K. Kong, J. You and M. Wong, "Online Palmprint Identification", IEEE Tr. on PAMI, Vol. 25, No. 9, 2003, pp. 1041-1050.

[23] X. Wu, D. Zhang and K. Wang, Fisherpalms-based Palmprint Recognition, Pattern Recognition Letters 24, 2003, pp. 2829-2838.

[24] W. Shu and D. Zhang, "Automated Personal Identification by Palmprint", Opt.Eng. 37(8), 1998, pp. 2359-2362.

[25] S.Ribarić, D. Ribarić and N. Pavešić, "A biometric identification system based on the fusion of hand and palm features", Proceedings of the advent of biometrics on the Internet, Rome, Italy, 7-8 Nov. 2002, pp. 79-82.

[26] A. Kumar, D. C. M. Wong, H. C. Shen and A. K. Jain, "Personal Verification Using Palmprint and Hand Geometry Biometric", *Proc. of 4th Int'l Conf. on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, Guildford, UK, June 9-11, 2003, pp. 668-678.

[27] A. K. Jain and A. Ross, " Multibiometric Systems", Communications of the ACM, Special Issue on Multimodal Interfaces , Vol. 47, No. 1, 2004, pp. 34-40.

[28] S.Ribarić, D. Ribarić, N. Pavešić, "Multimodal biometric user-identification system for network-based applications", IEE Proc. Vis. Image Signal Process., Vol. 150, No. 6, 2003, pp. 409-416.

[29] T. Pavlidis, Algorithms for Graphics and Image Processing, Springer Verlag, 1982