A multimodal biometric-based user-identification system for internet use

Slobodan Ribarić[1], Damir Ribarić[2], Nikola Pavešić[3]
[1]Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia
slobodan.ribaric@fer.hr
[2]Intelligent Informatics Systems, Zagreb, Croatia
[3] Faculty of Electrical Engineering, University of Ljubljana, Slovenia
nikola.pavesic@fe.uni-lj.si

Abstract:

Internet security services, such as confidentiality, authentication, integrity, and non-repudiation, rely on public-key cryptography services as well as on techniques to identify the user. Traditional user-identification techniques, such as passwords, personal identification numbers, card keys, etc., cannot differentiate between an authorized person and a fraudulent impostor. Biometrics is an emerging technology that identifies users by their physical and/or behavioural characteristics, and so inherently requires that the users to be identified are physically present at the point of identification.

This paper describes the design and development of a prototype, scanner-based system for the automatic identification of an individual based on the fusion of palm-print, finger and hand-geometry features at the matching-score level. The test performance, FAR = 0.0 % and FRR = 0.2 %, suggests that the system can be used in medium/high-security internet environments.

Keywords: Biometrics, Multimodal biometric system, Palm-print features, Hand-geometry features, Finger-geometry features, Internet security

1. INTRODUCTION

User authentication and encryption are vitally important for the security of computer networks. Public-key cryptography (PKI) provides a secure way of exchanging information, but designing a high-security user-authentication system still remains an unsolved problem. The conventional means of identification, e.g. passwords and personal identification numbers (PINs), can be easily guessed, observed, or forgotten. However, several of the biometric characteristics of an individual are unique, easily observed and time invariant. These properties make biometrics well suited for the purposes of user identification.

Biometrics refers to the automatic identification/verification of an individual based on his/her physical and/or behavioural characteristics [1], [2]. Various physical characteristics and behavioural traits are already being used for automatic

identification/verification of an individual; the most popular at the moment are signature, voice, face, palm print, fingerprint, hand geometry, iris and retinal scan.
However, a single physical characteristic or behavioural trait of an individual sometimes fails to be sufficient for his/her identification/verification; for this reason systems that integrate two or more different biometric characteristics are currently being developed to provide an acceptable performance, to increase the reliability of decisions and to increase robustness with regard to fraudulent technologies. Examples of such biometric systems include the following: a multimodal verification system that integrates face and fingerprint characteristics; a system that integrates face, fingerprint and hand-geometry features; an identification system that combines voice and face; and an identification system based on face, voice and lip movement, [3]–[6].

The human hand provides the source for a number of physiological biometric features, among the most commonly used are the fingerprint, the palm print, the geometry of the hand, the geometry of the finger and the vein pattern on the back of the hand. In this paper we propose a scanner-based multimodal biometric identification system that integrates palm-print, finger- and hand-geometry features. The system is based on a low-cost desktop scanner, which is used as the biometric acquisition device. As the system has a high user acceptance and high user-identification accuracy it is attractive for restricting access to web pages that contain confidential information or for authenticating users of e-commerce applications.

The rest of the paper is organized as follows: Section 2 presents related works in the field of palm-print, hand-geometry-based identification/verification systems, and information fusion in multimodal systems. Section 3 describes the proposed biometric system based on the fusion of palm-print, finger and hand-geometry features at the matching-score level. Section 4 describes the pre-processing and feature-extraction phases. Section 5 presents enrolment and identification. The experimental results on combining the three biometric modalities are presented in Section 6. Some conclusions and future research directions are given in Section 7.

2. RELATED WORK

The interest in biometrics is best evidenced by the growth in the amount of related literature over the past few years [1]–[23], [25]. There are bibliographic references relating to hand-geometry-based authentication systems, as well as some references to commercially available systems [7], [8], [9]. There are also references to palm-print verification; but, as far as we know, there are no references to systems based on the integration of palm-print, finger and hand-geometry features.
In the following paragraphs some related works from the field of hand-geometry- and palm-print-based systems and information fusion in multimodal biometric systems are briefly introduced.

2.1. Hand-geometry-based systems

The human hand provides the source for a number of physiological biometric features; the most frequently used are the fingerprint, the palm print, the geometry of the hand, the geometry of the finger and the vein pattern on the back of the hand.

Golfarelli et al. [10] addressed the problem of performance evaluation in biometric verification systems. In one of two evaluated verification systems they describe the prototype of a hand-based biometric system that takes into account 17 geometrical features of the hand. Jain et al. [11] described the prototype of a verification system based on hand geometry. The features included in this system are the length and the width of the fingers and the thickness of the hand. In the verification phase a 16-dimensional feature vector is associated with the claimed identity, and this is then compared using a feature vector of the hand whose identity has to be verified.

Sanches-Reillo et al. [12] defined and implemented a biometric system based on hand geometry. After capturing and pre-processing the images of the hand the measurement algorithms are applied. The main distances and angles of the hand are divided into four different categories: width, heights, 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 photographed. Euclidean distance, Hamming distance, Gaussian Mixture Models (GMMs) and Radial Basis Function Neural Networks are used for the classification and verification. The best results – success rates of approximately 96% – are obtained using a GMM.

Jain et al. [13] also presented an authentication method based on the deformable matching of hand shapes. The verification decision is based on shape distance, which is automatically computed during the alignment stage. Shape distance proved to be a more reliable classification criterion than a handcrafted feature set. The proposed approach resulted in a 96.5% genuine-accept rate vs. a 2% false-accept rate.

2.2. Palm-print-based systems

Shu et al. [14] presented a prototype system based on different palm-print features, which are classified as geometrical, principal-line and wrinkle features, delta-point features and minutiae. The authors also evaluated the FRR and FAR on different combinations of palm-print features. Their experiments showed that a combination of eight points on the principal-lines and geometry features gives an acceptable identification accuracy (FRR = 0.0% and FAR = 0.2%).

Zhang et al. [15] used two, novel characteristics for their palm-print verification: datum-point invariance and line-feature matching. The palmprint verification with both datum point invariance and line feature matching were tested by 20 couples of palmprint images from 20 right palms. Experimental results of verification exhibited effectiveness of palmprint verification (FAR = 0.0% and FRR = 0.0%).

Duta et al. [16] investigated the feasibility of person identification based on feature points extracted from palm-print images. Their approach is based on a set of feature points extracted from along the principal lines and the associated line orientation. The overlap between the user (genuine) and the impostor distributions is reported to be approximately 5%.

You et al. [17] proposed a texture-based, dynamic selection scheme to facilitate a fast search for the best matching of a palm-print template in the database in a hierarchical fashion.

C. Han et al. [18] described a scanner-based personal authentication system based on palm-print features. These palm-print features are extracted from the so-called region of interest (ROI). 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 verification: the multiple-template matching method and the back-propagation neural network method.

2.3. Multimodal biometrics

A multimodal biometric system requires an integration scheme to fuse the information obtained from the individual modalities. Various levels of fusion are possible ([3], [4], and [19]):

i) Fusion at the feature-extraction level, where the features extracted using two or more sensors are concatenated;

ii) Fusion at the matching-score level, where the matching scores obtained from multiple matchers are combined;

iii) Fusion at the decision level, where the accept/reject decisions of multiple systems are consolidated.

Jain et al. [23] described an interesting approach to the realization of a multimodal biometric verification system that uses fusion at the matching-score level based on learning user-specific matching thresholds as well as the weights of individual biometric traits.

Some other references related to fusion at the matching-score level are [5], [19], [20].

3. SYSTEM DESCRIPTION

Fig. 1. shows the block-diagram of a proposed multimodal biometric identification system based on the fusion of finger, hand-geometry and palm characteristics at the matching-score level. A low-cost scanner is used as the input device. In the pre-processing module some standard image-enhancement procedures are applied. Three feature-extraction modules are used for the extraction of finger, hand-geometry and palm-print features represented, respectively, by the three feature vectors: $\boldsymbol{F_x}$, $\boldsymbol{H_x}$ and $\boldsymbol{P_x}$,. In the subsequent three matching modules the matching between the corresponding vectors and the templates from a database is performed. After normalization of the matcher's outputs, fusion at the matching-score level is obtained by means of the total similarity measure. In the decision module three rules are used in order to establish identity. The first rule is the (k, l)-NN rule, with k = l = 3; the other two are heuristic rules.

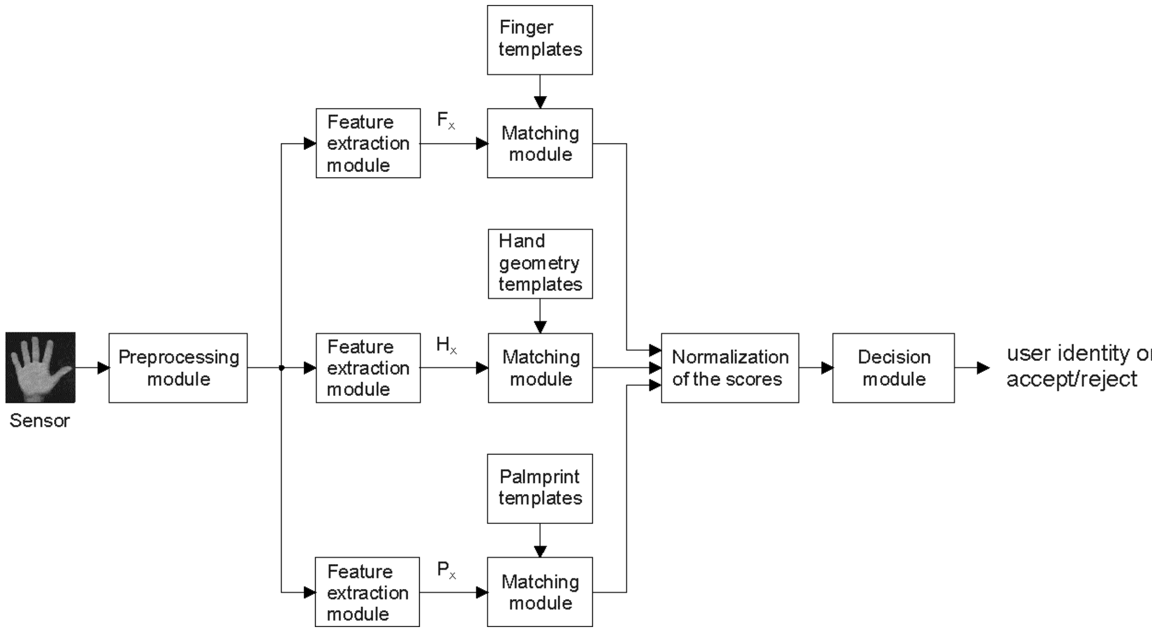


Fig. 1. A block-diagram of the multimodal biometric identification system based on the fusion of finger, hand-geometry and palm-print features at the matching-score level.

4. PRE-PROCESSING AND FEATURE EXTRACTION

4.1 Image capture

The palm is the inner surface of the hand between the wrist and the fingers. The finger, the hand-geometry and the palm features are extracted from the image of the right hand, which is placed on the flat, glass surface of a scanner. The user is asked to put his/her hand on the scanner, with the fingers spread naturally. There are no pegs, which usually serve as control points for the appropriate placement of the hand. A translation or rotation of the hand by approximately $\pm 30^{\circ}$, relative to the vertical line of symmetry of the working surface of the scanner, is allowed. The spatial resolution of the images is 180 dots per inch (dpi) / 256 grey levels. Fig. 2. shows a typical image obtained from the scanner. For the purposes of our research we collected a database comprised of 5 images from 180 individuals, with each image taken using a scanner.

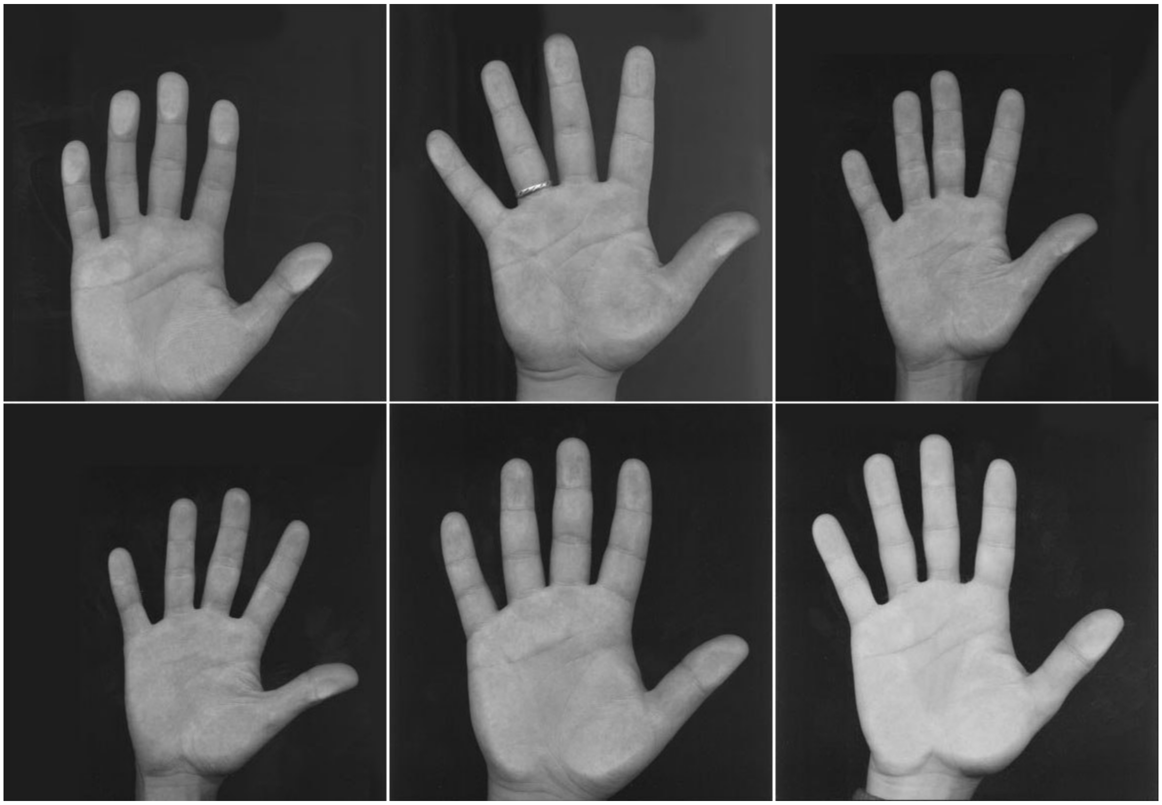


Fig. 2. Some examples of the images of right-hands obtained with a desktop scanner.

4.2 Pre-processing and feature extraction

In the pre-processing phase, global thresholding is applied to extract the hand from the background. We have experimented by using methods based on local thresholding and edge-detection procedures, but due to the regular and controllable conditions of image capturing, simple global thresholding provides satisfactory results. To extract the contour of the hand, a slightly modified contour-tracing algorithm, which is described in [24], is used. The extracted contours of the hands can be seen in Fig. 3. Based on the contour of the hand the fingertips and the valleys between two fingers are determined.

On the hand contour, two reference points are selected:

i) The valley between the little finger and the ring finger (point V_1),

ii) The valley between the index finger and the middle finger (point V_2).

Point V_1 is used to determine a sub region (120 x 60 pixels) of the palm where a segment of the heart line (Fig. 4) can be detected. To detect the segment of the heart line in the palm sub-region, we subsequently applied the following: a Gaussian mask (9 x 9 pixels, $\sigma^2 = 3.0$), a Sobel operator, and double thresholding of the horizontal projection. Fig. 5. illustrates the results of detecting the segment of the heart line.

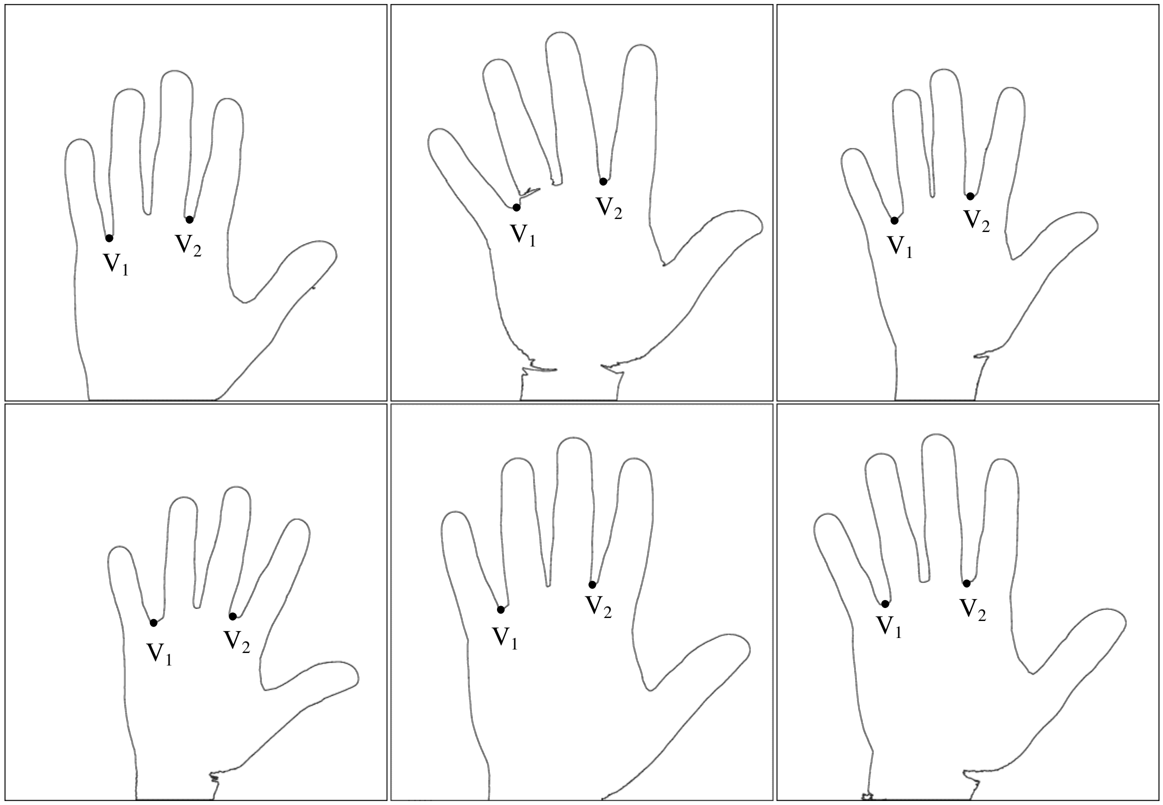


Fig. 3. Extracted contours of the hands showing the two reference points (V_1 and V_2).

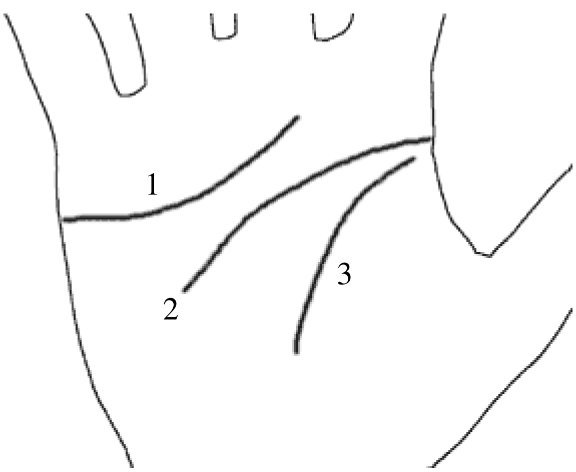


Fig. 4. Principal lines of a palm print: 1 heart line, 2 head line, 3 life line.

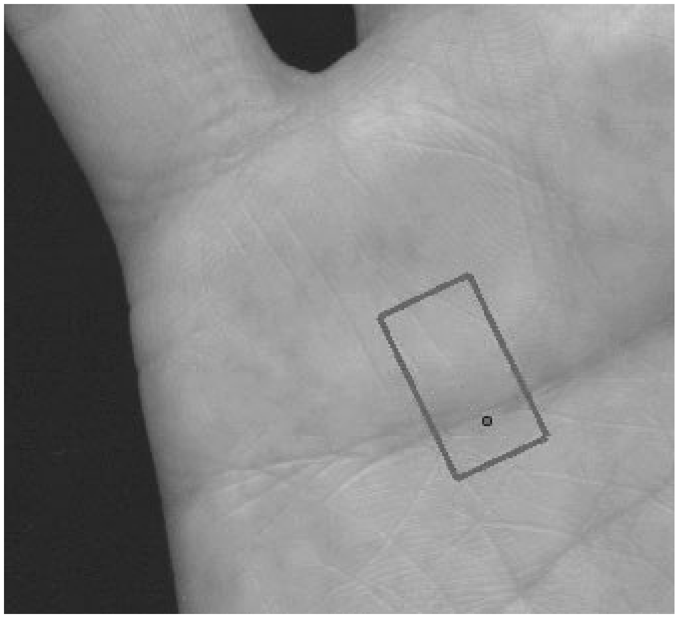


Fig. 5. Result of detecting the segment of the heart line.

The middle point of the segment of the heart line and a joint line connecting the reference points V_1 and V_2 are used, together with the three hand-geometry features, to define the focus-of-attention region (FOAR) of the palm (Figure 6a, 6b), (Figure 6c). The FOAR (315 x 285 pixels) is pre-processed (Figure 6d) using a Gaussian mask and a modified Sobel operator, followed by a double thresholding. In order to detect the principal lines we also experimented with the ridgeline-following algorithm described in [25], but we were not able to obtain satisfactory results.

Finally, three feature vectors are obtained: the 20-component vector $\boldsymbol{F_x}$, containing the features of the fingers (the lengths and widths of the four fingers measured at different heights, (Fig. 7)); the 3-component vector $\boldsymbol{H_x}$, carrying information about the hand geometry (the width of the hand and the distances between the valleys that are between fingers (Fig. 7)); and the 399-component vector $\boldsymbol{P_x}$, that relies on palm-print features. The palm-print features are based on the principal lines – the heart line, the head line, the life line, (Fig. 4) – and on the texture attributes of the palm print. All the various features are invariant to rotation and translation of the hand on the image.

5. IDENTIFICATION

5.1 Enrolment

In the enrolment process the feature vectors (the templates representing the user's hand) are saved to the template file. This file also contains the relevant authentication information: in our case each authorized user is represented by an index. In the enrolment process three templates for each user are taken. On the basis of these templates an additional four templates are generated. So, for each person the template file contains seven templates: three original templates, one average template, and three templates calculated as an average of each pair of the original templates.

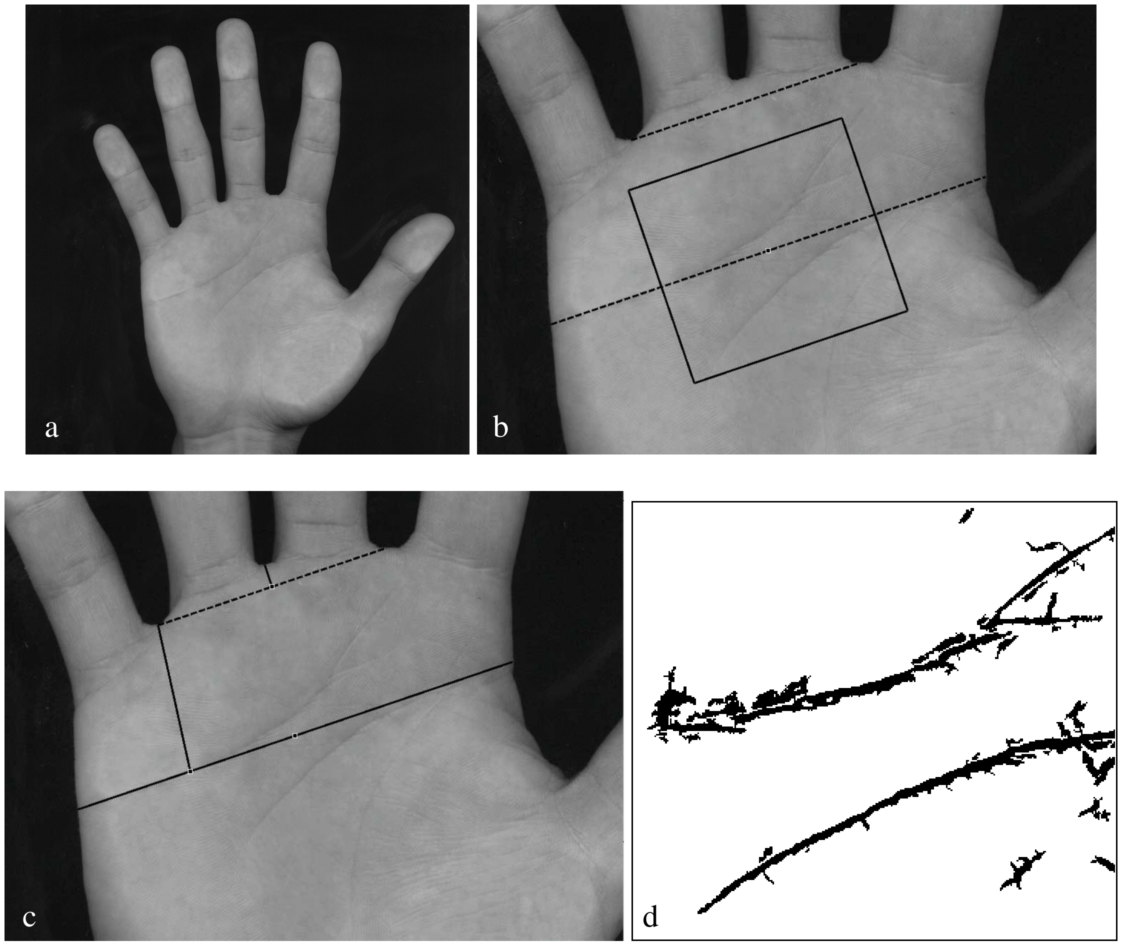


Fig. 6. a) An input image, b) The focus-of-attention region (FOAR), c) Simple hand-geometry features, d) Pre-processed FOAR.

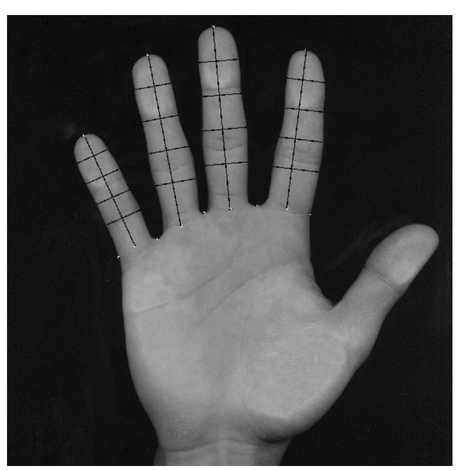


Fig. 7. Finger features.

5.2 Identification

Identification is a one-to-many process that compares the biometric information presented by an individual (the live template) with the biometric information stored in a database (the user's templates), and based on this comparison a decision is made as to whether a match can be declared. Fig. 8. depicts the data-flow diagram of the identification process applied in the system. During the identification stage the input device captures the characteristics of the individual to be identified and converts them into the same format as the user's templates. The template is represented by three feature vectors, $\boldsymbol{F_x}$, $\boldsymbol{H_x}$ and $\boldsymbol{P_x}$, which are packed into the feature vector (the live template) $\boldsymbol{X} = [\boldsymbol{F_x}, \boldsymbol{H_x}, \boldsymbol{P_x}]$. The Euclidean distances, $d(\boldsymbol{F_x}, \boldsymbol{F_{ij}})$, $d(\boldsymbol{H_x}, \boldsymbol{H_{ij}})$ and $d(\boldsymbol{P_x}, \boldsymbol{P_{ij}})$, between corresponding components of the feature vector $\mathbf{X}$ and the stored feature vector (the user template) $\boldsymbol{N_{ij}} = [\boldsymbol{F_{ij}}, \boldsymbol{H_{ij}}, \boldsymbol{P_{ij}}]$ in the database are calculated in the matching modules. The index i, *where* $i = 1, 2, 3, ..., u$, denotes the index of the user (u is total number of users in the system database). The second index, $j = 1, 2, \ldots, p$, denotes the j-th template of the user i obtained during the enrolment process. The distances are normalized and transformed into the similarity measures, S^F_{ij}, S^H_{ij}, and S^P_{ij}, by means of three transition functions, which were determined experimentally from a database consisting of 50 users, 5 templates per user (p = 5), as follows: For each system user p(p-1)/2 = 10 pairs of templates are formed. The Euclidean distances, d^F, d^H and d^P, between elements of pairs are calculated and the corresponding frequency distributions of the distances are generated. The transition functions are two-segment functions over the distances interval [0, +∞]. The first segment is a constant function over the interval [0, mean value] and an exponential function that approximates to the histograms' right-hand tails over the interval (mean value, +∞). The corresponding histograms, as well as the transition functions, are shown in Fig. 9a, 9b and 9c.

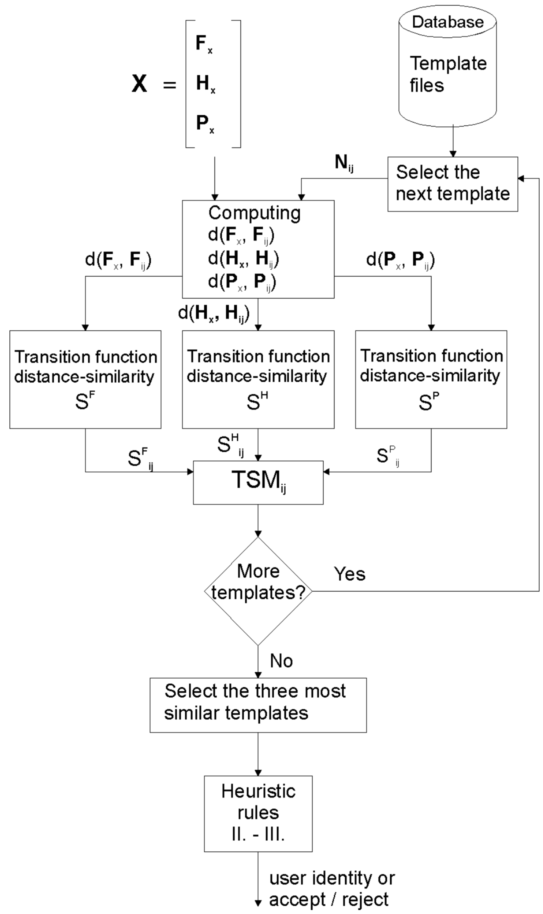
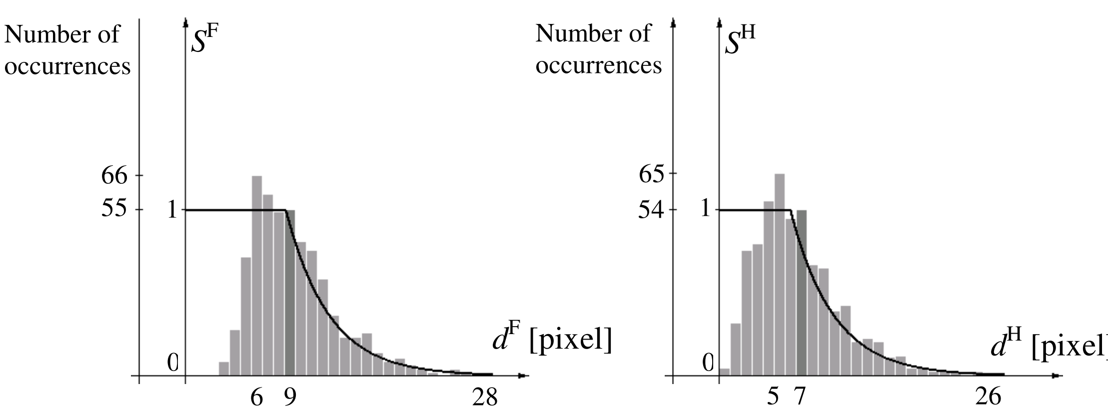


Fig. 8. The data-flow diagram of the identification process.



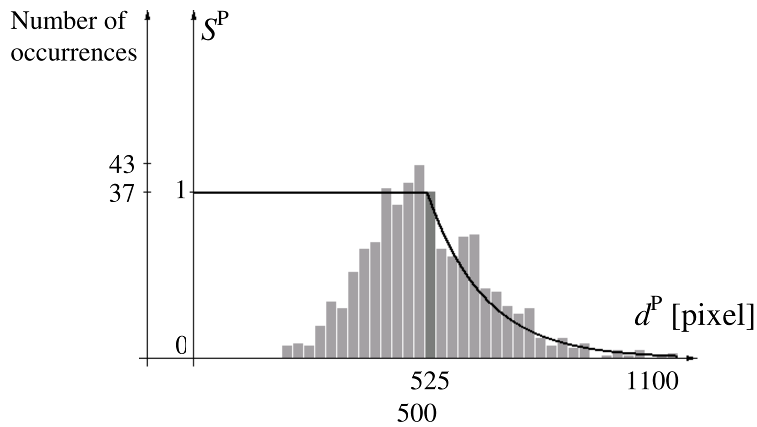


Fig. 9. Histograms and transition functions for normalization, and distance to similarity measure transformation.

Fusion is performed at the matching-score level. During the identification process the feature vector (the live template) $\boldsymbol{X}$ is compared with all the templates in the user database, $\boldsymbol{N_{ij}}$. For each template in the database the total similarity measure

$$TSM_{ij} = w_1\, S^F{}_{ij} + w_2\, S^H{}_{ij} + w_3\, S^P{}_{ij}$$

is computed. The values of the weights w_1, w_2, and w_3 are proportional to the three unimodal system performances F, H, P, respectively (see Table 1.), and fulfil the condition $w_1 + w_2 + w_3 = 1$. From the database, the three most similar templates, $\boldsymbol{N_{qk}}$, $\boldsymbol{N_{rl}}$, and $\boldsymbol{N_{sm}}$, are selected as inputs into the final decision process.

The final decision as to whether $\boldsymbol{X}$ is matched with the enrolled user templates in the database is based on the following rules:

I. RULE: All three indexes of the selected templates, $\boldsymbol{N_{qk}}$, $\boldsymbol{N_{rl}}$, and $\boldsymbol{N_{sm}}$, have to be the same ($q = r = s$), i.e. all three selected templates have to be from the same user.

II. RULE: The individual biometrics similarity measures have to fulfil the following conditions:
$S^F{}_{qk} > \theta_1$ and $S^F{}_{rl} > \theta_1$, and $S^F{}_{sm} > \theta_1$ and $S^H{}_{qk} > \theta_2$ and $S^H{}_{rl} > \theta_2$ and $S^H{}_{sm} > \theta_2$ and $S^P{}_{qk} > \theta_3$ and $S^P{}_{rl} > \theta_3$ and $S^P{}_{sm} > \theta_3$,
i.e. the individual biometrics similarities between the live template and user templates have to exceed some threshold values.

III. RULE: The total similarity measures have to fulfil the following conditions: $TSM_{qk} > \theta_4$ and $TSM_{rl} > \theta_4$ and $TSM_{sm} > \theta_4$ and $(1/3)\,(TSM_{qk} + TSM_{rl} + TSM_{sm}) > \theta_5$,
i.e. the weighted average similarities between the live template and user templates have to exceed some threshold values, too.

The threshold values θ_t, $t = 1, 2, \ldots, 5$, are experimentally determined during the system-validation process. Note, that only if all three rules are satisfied is the individual represented by $\boldsymbol{X}$ successfully identified as a user registered in the database with an index i, $i = 1, 2, 3, \ldots, u$ (see I. RULE).

6. EXPERIMENTAL RESULTS

In this section an experiment demonstrating the identification reliability of the proposed multimodal biometric system is described.
The system was tested on a database of 130 persons. Five images of each person's hand were captured, thus a total of 650 images were made available. In the enrolment phase, three images per person were used; the remaining two images were used for testing. For the impostors, however, all five images were available for testing.
The experiment proceeded as follows: One template file was randomly selected from the set of 130 template files as the input in the enrolment process. The remaining 129 template files were considered as impostors' template files. The identification was performed and the results were recorded. Next, from 129 template files, another file was randomly selected and added to the set of template files of the authorized users. So, at this point, there were 2 user template files and 128 impostor template files. Again, a process of identification was performed and the results were recorded. The above procedure was repeated until the 129 user template files and 1 file of an impostor were obtained. The whole of the above-described process was repeated 20 times. There were a total of over 450 million matchings between templates during the experiment.
The experiment was performed for individual modalities and for their different possibilities of fusion. Table 1. shows how the feature fusion of different hand modalities influences the system's FAR and FRR.

	F	H	P	F-H	H-P	F-P	F-H-P
FAR [%]	0	15.3	3.8	0	1.22	0	0
FRR [%]	1.2	13.0	1.4	1.15	1.1	0.3	0.2

Table 1: The system's FAR and FRR, which is based on the use of the following: F, finger-geometry features; H, hand-geometry features; P, palm-print features; and on the fusion of these features (e.g. F-P denotes fusion of finger geometry (F) and palm-print (P) features)

7. CONCLUSION

In this paper we describe the design and development of a prototype biometric identification system based on the fusion of hand-geometry, finger and palm-print features. The experimental results showed that information fusion at the matching-score level improves the results of the identification. The results, FAR = 0.0 % and FRR = 0.2 %, have demonstrated the possibility of using this system in medium/high-security environments, for example in access control or in virtual access control (web access, e-commerce).
The main advantages of the system based on the fusion of hand-geometry, finger and palm-print features are:

i) A single sensor (a low-cost scanner) is used as the input device. It makes the system suitable for home and for many network-based applications.

ii) The system is based on hand-geometry, finger and palm-print features, and is invariant to hand translation and rotation on the scanner. The fact that there is no need to use control pegs in the input device makes the system more acceptable from the users' point of view.
iii) In spite of the fact that the human hand is not a unique human characteristic [2], the fusion of hand-geometry, finger and palm-print features, which is applied in the proposed system, provides us with a reliable method for identifying people.

Further work should be undertaken to increase the database size with template files collected over a longer period of time, as well as experimenting with novel palm characteristics like datum points and global texture features.

REFERENCES

[1] A. K. Jain, R. Bolle, S. Pankanti (eds.), Biometrics, Personal Identification in Network Society, Kluwer Academic Publishers, 1999.
[2] D. D. Zhang, Automated Biometrics, Technologies and Systems, Kluwer Academic Publishers, 2000.
[3] L. Hong, A. K. Jain, Multimodal Biometrics, in [2], pp. 326-344.
[4] A. Ross, A. Jain, J.Z. Qian, Information Fusion in Biometrics, Proc. 3rd AVBA Conf. Halmstad, Sweden, June 2001, pp. 354-359.
[5] R. Brunelli, D. Falavigna, Personal Identification Using Multiple Cues, IEEE Trans on the PAMI, Vol. 17, No. 10, October 1995, pp. 995-966.
[6] R. W. Frischholz, U. Dickmann, BioID: A Multimodal Biometric Identification System, IEEE Computer, Vol. 33, No. 2, February 2000, pp.64-68.
[7] Recognition Systems Inc, http://www.recogsys.com
[8] B. Spencer, Biometrics in Physical Access Control Issues, Status and Trends, http://www.recogsys.com
[9] R. Zunkel, Hand Geometry Based Verification, in [2], pp. 87-101.
[10] M. Golfarelli, D. Maio, D. Maltoni, On the Error-Reject Trade-Off in Biometric Verification Systems, IEEE Trans. on PAMI, Vol. 19, No. 7, July 1997, pp.786-796.
[11] A. K. Jain, A. Ross, 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.
[12] R. Sanchez-Reillo, C. Sanchez-Avila, A. Gonzalez-Marcos, Biometric Identification Through Hand Geometry Measurements, IEEE Trans. on PAMI, Vol. 22, No. 10, October 2000, pp. 1168-1171.
[13] A. K. Jain, N. Duta, Deformable Matching of Hand Shapes for Verification, Proceedings of IEEE International Conference on Image Processing, Kobe, October 1999, 5 pages.
[14] W. Shu, D. Zhang, Automated Personal Identification by Palmprint", Opt.Eng. 37(8), August 1998, pp. 2359-2362.
[15] D. Zhang, W. Shu, Two Novel Characteristics in Palmprint Verification: Datum Point Invariance and Line Feature Matching, Pattern Recognition 32, 1999, pp.691-702.

[16] N. Duta, A. K. Jain, K. V. Mardia, Matching of Palmprints, Pattern Recognition Letters, Vol. 23, No. 4, February 2002, pp. 477-485.
[17] J. You, W. Li, 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, K-C. Fan, Personal Authentication Using Palm-print Features, Pattern Recognition 36, 2003, pp. 371-381.
[19] A. Ross, A. Jain, Information Fusion in Biometrics, to appear in Pattern Recognition Letters, Special Issue in Multimodal Biometrics, 2003, 18 pages.
[20] A. K. Jain, S. Prabhakar, S. Chen, Combining Multiple Matchers for a High Security Fingerprint Verification System, Pattern Recognition Letters 20 (1999), 1371-1379.
[21] J. Kittler, M. Hatef, R. P. W. Duin, J. Matas, On Combining Classifiers, IEEE Trans. on the PAMI, Vol. 20, No. 3, March 1998, pp. 226-239.
[22] E. S. Bigun, J. Bigun, B. Duc, S. Fischer, Expert Conciliation for Multi Modal Authentication Systems by Bayesian Statistics, Proc. First Int. Conference on Audio- and Video-based Biometric Person Authentication, Crans-Montana, Switzerland, 1997, pp. 327-334.
[23] A. K. Jain, A. Ross, Learning User-Specific Parameters in a Multibiometric System, http://www.rossarun.jain.cse.msu.edu, 2001, 4 pages.
[24] T. Pavlidis, Algorithms for Graphics and Image Processing, Springer Verlag, 1982.
[25] D. Maio, D. Maltoni, Minutiae Extraction and Filtering from Grey-Scale Images, in L.C. Jain, U. Halici, I. Hayashi, S. B. Lee, S. Tsutsui (eds.), Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press, 1999, pp. 155-192.