A Multimodal Biometric System Based on Fingerprint and Signature Recognition

Hakob Sarukhanyan
Institute for Informatics and Automation Problems of NAS RA
Yerevan, Armenia
E-mail: hakop@ipia.sci.am

Davit Kocharyan
Institute for Informatics and Automation Problems of NAS RA
Yerevan, Armenia
E-mail: david.kocharyan@gmail.com

Vahe Khachaturyan
Institute for Informatics and Automation Problems of NAS RA
Yerevan, Armenia
E-mail: vahe@7smarts.com

ABSTRACT
In this paper, we propose a multimodal biometric system, based on fingerprint and signature recognition. Fingerprint recognition is the most popular *physiological* characteristic used to identify a person in biometric systems, because of feasibility, permanence, distinctiveness, reliability, accuracy, and acceptability. Signature recognition is the most popular *behavioral* characteristic used in biometric systems. Thus, we believe that the combination of these two methods will have a reliable and accurate result. We propose a weighted fusion scheme, which transforms the scores into a common range, assigned weights and combines them, giving the final fused score.

Keywords
Biometric systems, multimodal biometrics, fingerprint, signature, minutiae, discrete radon transform, biometric fusion.

1. INTRODUCTION
Biometric systems identify a person using behavioral and physiological biometric data. The behavioral biometrics are: signature, gait, speech and keystroke, which change with age and environment. Physiological characteristics do not change throughout the lifetime of a person. Such characteristics include face, fingerprint, palm print and iris. The biometric systems verify and identify a person using his biometric data. Most biometric systems are *unimodal* - rely on a single source of information for authentication (e.g., single fingerprint, face or signature) [1]. Due to a large number of users, these systems experience problems, such as: noise in sensed data (e.g.: a fingerprint image with a scar, dirty sensor, etc.); intra-class variations (e.g., incorrect facial pose); inter-class similarities (e.g.: there may be inter-class similarities in the feature space of multiple users); non-universality (e.g.: incorrect minutiae features caused by poor quality of ridges). To overcome these problems, multiple sources of information can be used. Such systems are known as *multimodal* biometric systems, and are expected to be more reliable due to the presence of multiple, independent biometric data.

In this paper, we propose a multimodal biometric system, based on *fingerprint* and *signature* recognition. Fingerprint recognition is the most popular physiological characteristic used to identify a person in biometric systems, because of feasibility, permanence, distinctiveness, reliability, accuracy, and acceptability. Signature recognition, from the other hand, is the most popular behavioral characteristic used in biometric systems. Thus, we believe that the combination of these two methods will have a reliable and accurate result. The proposed multimodal biometric system takes input in the following sequential order: first, the signature is taken, and a matching score is calculated for the signature. Afterwards, the fingerprint is taken and a separate and independent matching score is calculated for the fingerprint. The calculated results are then combined by a matching score level fusion scheme and the final decision is made, based on the fusion. The fusion scheme transforms all the scores into a common range to be able to combine them into one final score and make the decision.

2. FINGERPRINT RECOGNITION METHOD
A fingerprint is a pattern of ridges and valleys. The ridges are the dark areas of the fingerprint and the valleys are the white areas that exist between the ridges. (see Fig. 1) [2].

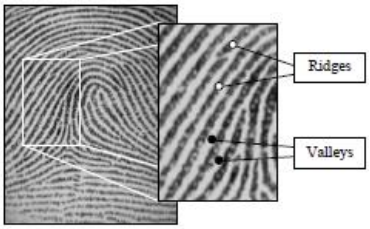


Fig.1: Ridges and valleys of a fingerprint

Fingerprint classification involving 6 classes with critical points in a fingerprint called core and delta marked as circles and triangles given in Fig. 2 [1].

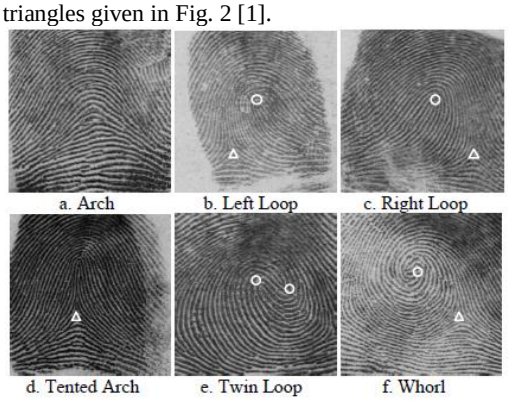


Fig. 2: Fingerprint classification

Many classifications are given to patterns that can arise in the ridges of a fingerprint (see Fig. 3). These points are called the minutiae of the fingerprint. The most commonly used minutiae in current fingerprint recognition technologies are ridge endings and bifurcations, because they can be easily detected by only looking at points that surround them (Bifurcation is the location where a ridge is divided into two separate ridges). A good quality fingerprint contains 30 – 80 minutiae points. [3]

The most commonly used fingerprint recognition methods are based on the minutiae points, because extraction of the points does not require a high-resolution image, and the minutiae points can be extracted from a not-aligned and

dissorted fingerprint image. Thus, the method can be alignment invariant.

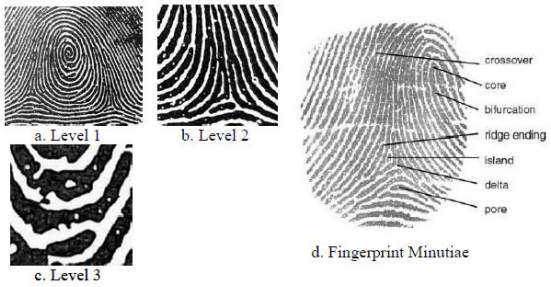


Fig. 3: Fingerprint features

Minutiae based fingerprint recognition process includes the following steps: Binarization, Thinning, Minutiae Extraction, Minutiae Matching, Computing Matching Score (see Fig. 4) [4].

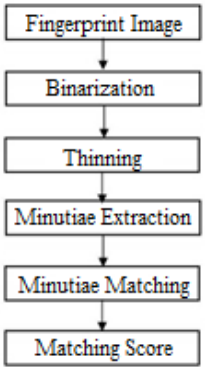


Fig. 4: Minutiae Based Fingerprint Recognition Method

A. Binarization

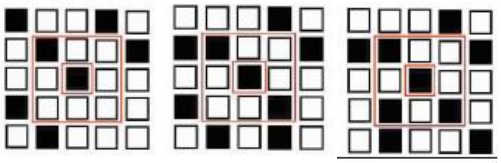
In this step the fingerprint image is converted into grayscale, and then to binary data. The step also includes image enhancement, during which the image is normalized and filters (Gabor filter) are applied to recover the ridge structures and remove noise [5].

B. Thinning

The binarized image is thinned to reduce the thickness of all ridges lines to one pixel width.This step will help to extract minutiae points, as thinning does not change the location of the minutiae points compared to the original fingerprint.

C. Minutiae Extraction

This step derives the minutiae locations and angles. The terminations caused by the outer boundary are not considered as minutiae points. Crossing number (Cn) is used to identify the minutiae points, which is defined as half of the sum of differences between intensity values of two adjacent pixels. If crossing number is 1, 2, 3 or greater, then the minutiae points are considered as ending, normal ridge, bifurcation, respectively (see Fig. 5).



(a) (b) (c)

Fig. 5: Minutiae Extaction:
(a) Ending minutiae, C_n=1;
(b) Normal ridge pixel, C_n=2;
(c) Bifurcation minutiae, C_n=3.

D. Minutiae Matching

In this step, the fingerprint data is compared with the template data of the system. The extracted minutiae data is stored as a matrix with number of rows equal to the number of minutiae points, and with four columns: column 1 is the row index of each minutiae point; column 2 is the column index of each minutiae point; column 3 is the orientation angle of each minutiae point; column 4 is the type of minutiae (1 – ending, 2 – bifurcation, 3-normal ridge).

During the matching process each minutiae point is compared with the template data. There are several rotation invariant algorithms for comparing minutiae points in two fingerprints. One of them connects each point to its nearest neighbor, and calculated some values of the resulted connected structure (crossing ridge number, point types, distance, rotation angle). The algorithm tries to find similar structures in the two fingerprints. This step is called local matching. After finding those, the alignment parameters are calculated and the two images are aligned. Then, all the minutiae points are matched on the global level. This approach allows to match not aligned, as well as partial fingerprint images, that contain few minutiae points.

E. Matching Score

The matched minutiae points are devided into four different groups: N_1 – they belong to a structure that has 3 or more similar local structures; N_2 - they belong to a structure that has 2 similar local structures; N_3 - they belong to a structure that has 1 similar local structure; N_4 - they are matching, but the local structures are not. The grouping is used to give a weight to each point and make the matching score more accurate. The final matching score is calculated, based on the following equation:

$$score = 100 * \frac{2 * (3N_1 + 2N_2 + 1.5N_3 + N_4)}{7.5}$$

The higher the score, more similar are the compared fingerprints. The score is based on the number of matching minutiae points.

3. SIGNATURE RECOGNITION METHOD

During the enrollment phase, a set of reference signatures are used to determine user dependent parameters characterizing the variance within the reference signatures. The reference set of signatures, together with these parameters, are stored with a unique user identifier in the system's database.

In the training phase we choose a number of genuine and forged signatures for training each classifier.

In the verification phase when a test signature is input to the system, it is compared to each of the reference signatures of the claimed person. The person is authenticated if the resulting dissimilarity measure is low a threshold of the classifier, rejected otherwise. The details of the system are described in the following sections.

A. Discrete Radon Transform and feature extraction

The Discrete Radon Transform (DRT) is a matrix, where each column represents a projection or shadow of the original image at a certain angle. DRT can be expressed as follows [7-9]:

$$R_j = \sum_{i=1}^{\Psi} w_{ij} I_i; j = 1,2,\dots,N_\varphi N_\theta \qquad (1)$$

where R_j – the cumulative intensity of the pixels that lie within the jth beam; Ψ – total pixels in an image; w_{ij} – the

contribution of the *i*th pixel to the *j*th beam-sum; I_i – the intensity of the *i*th pixel; N_φ – nonoverlapping beams per angle; N_θ – number of total angles (see Fig. 6).
For extracting the global features firstly, the background of the signature image is mapped to zero and the pen strokes to one. After that, median filtering is applied to remove speckle noise. Subsequently the DRT of the signature image is calculated, using the algorithm discussed in this section (see Fig. 7). This algorithm calculates the DRT at N_θ angles. These angles are equally distributed between 0 and 180°. This image has 128 columns, where each column represents a projection.

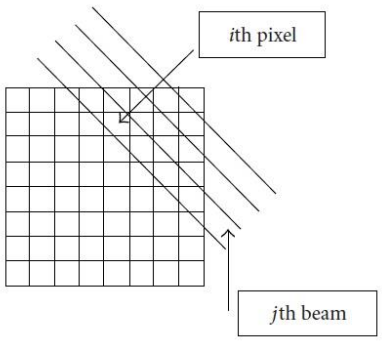


Fig. 6: Discrete model for the Radon transform

Although the DRT is not a shift invariant representation of a signature image, shift invariance is ensured by the subsequent image processing. This is done by removing (decimation) all the zero-valued components from each projection. These decimated vectors are then shrunk or expanded to the required dimension *d* through linear interpolation. Each vector is subsequently normalized by the variance of the intensity of the entire set of feature vectors. In order to ensure rotation invariance, the projections at angles that range from 180 to 360° are also included in the observation sequence.

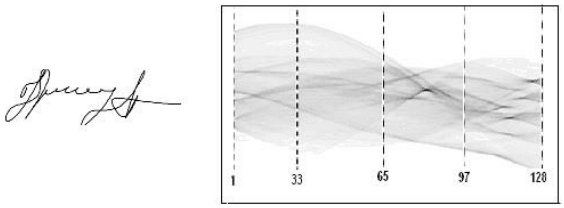


Fig. 7: A signature and its DRT, which is displayed as a gray-scale image.

An observation sequence, therefore, consists of T = $2N_\theta$ feature vectors, that is

$$X_1^T = \{x_1, x_2, \ldots, x_T\} \quad (2)$$

B. Signature Alignment

In order to compare two signatures of differing lengths, we use our algorithm, which has been suggested for matching the characteristic vectors and comparing handwritten signatures [6], [8].
In order to ensure that each observation sequence is a rotation invariant representation of the corresponding signature image, an observation sequence alignment is necessary. The optimal alignment of two observation sequences can be achieved in a linear way. It iteratively shifts the observation sequences with respect to each other. During any iteration, the distances between the corresponding observations (feature vectors) are calculated. The alignment is optimal when the average distance between the corresponding observations is minimum. The distance between two signatures is simply the average of the distances between the optimally aligned feature vectors.

C. Signature Enrollment

During enrollment to the system, we use a number of signatures (five in our system) for each user. These signatures are pair-wise aligned to find the distance between each pair, as described in section B.
From these alignment scores, the following reference set statistics are calculated:

1) average distance to farthest signature (d_{max});
2) average distance to nearest signature (d_{min}).

A training data set consisting of five genuine signatures and five forgery signatures is used in order to learn the threshold parameter separating the forgery and genuine classes. These signatures are separate from the signatures used as reference signatures.

D. Training

First, each training signature is compared to the reference set of signatures it claimed to belong, using the algorithm described in Section C, giving a 2-dimensional feature vector (p_{min}, p_{max}). The feature values are then normalized by the corresponding averages of the reference set (d_{min}, d_{max}): this is calculated as in equations (3) and (4) to give the distribution of the feature set.

$$N_{max} = d_{max}/p_{max} \quad (3)$$
$$N_{min} = d_{min}/p_{min} \quad (4)$$

The distribution of this normalized data supports that genuine and forgery samples in the training set are well separated with these normalized features. Note that by normalizing the measured distance vectors by the corresponding reference set averages, we eliminate the need for user-dependent thresholds commonly used in deciding whether a signature is similar enough to the reference set.
Finally, we train a classifier to separate the genuine and forgery. For this work, we trained the SVM classifier using the 2-dimensional feature vectors. Then, a linear classification is made by picking a threshold value separating the two classes within the training set.
This threshold is fixed and later used in the verification process.

E. Verification

A verification data set consisting of five genuine signatures and ten forgery signatures are used in order to test the trained classifiers. These signatures are separate from the signatures used in the enrollment and in the training phases.
In order to verify a test signature as genuine or forgery, we first proceed as in the training stage: the signature is compared to all the reference signatures belonging to the claimed ID using the algorithm described in Section B. Then, the resulting distance values (p_{min}, p_{max}), normalized by the averages of the claimed reference set (d_{min}, d_{max}), then these normalized values are used in classifying the signature as genuine or forgery, by the trained classifier.

4. FUSION SCHEME

The fusion scheme is used to combine the two results and take the final decision. Prior to combining the scores, we need to normalize them, as they are not homogeneous. The normalization is transforming the scores into a common domain, before combining them. We propose to transform the scores into a common range of [0, 1]. Given a set of

matching scores {sk}, k = 1, 2,… n, the normalized scores are given by:

$$s'_k = \frac{s_k - min}{max - min},$$

where the minimum (min) and maximum (max) values are estimated from the training data. This approach retains the original distribution of scores except for a scaling factor and transforms all the scores into a common range of [0, 1]. As the score obtained from the signature recognition method shows the dissimilarity of the compared signatures (the higher the score, the lower the similarity), unlike the fingerprint recognition method, where the score shows the similarity, the dissimilarity score is transformed to a similarity score by subtracting the normalized score from 1. Each score is assigned a weight. The weight is calculated based on the EER (Equal Error Rate) of the recognition method.

$$W_f = \frac{EER_f}{EER_f + EER_s}$$

$$W_s = \frac{EER_s}{EER_f + EER_s}$$

where W_f and EER_f are the weight and EER of the fingerprint recognition method, respectively. Similarly, W_s and EER_s are the values for the signature recognition method. The final fusion score is calculated by the following equation:

$$S = W_f S_f + W_s S_s$$

where S_f and S_s are the normalized scores of the recognition methods. The fused score is also in the range of [0, 1] as the sum of the weights is equal to 1.

As an example, if the EER of the fingerprint recognition method is 4%, and the EER of the signature recognition method is 10%, then W_f = 0.72 and W_s = 0.28.

4. ACKNOWLEDGEMENT

The authors would like to thank the Institute for Informatics and Automation Problems of NAS RA for supporting their research.

REFERENCES

[1] James L. Wayman (Editor), Anil K. Jain, "Biometric Systems", *Springer*, 2004.

[2] Davide Maltoni, Dario Maio, Handbook of Fingerprint Recognition, *Springer*, 2009.

[3] S. Prabhakar, A. K. Jain and S. Pankanti, "Learning fingerprint minutiaelocation and type", *Pattern Recognition*, 36(8): 1847–1857, 2003.

[4] Naser Zaeri, "Minutiae-based Fingerprint Extraction and Recognition", *Biometrics, Dr. Jucheng Yang (Ed.), ISBN: 978-953-307-618-8, InTech*, 2011.

[5] Raymond Thai, "Fingerprint Image Enhancement and MinutiaeExtraction", *Computer Science and Software Engineering*, The University of Western Australia, 2003.

[6] Jain A., Griess F., Connell S. "On-line signature verification", *Pattern Recognition 35*, 2963–2972, 2002.

[7] F. Hao, C.W. Chan, "Online signature verification using a new extreme points warping technique", *Pattern Recognition Letters*, Vol 24, Issue 16, 2943-2951, 2003.

[8] V. Khachaturyan, "Handwritten Signature Verification Using the DRT" *Mathematical Problems of computer science*, vol 39, Yerevan, Armenia, 2013, pp. 31-39.

[9] V. Khachaturyan, "Handwritten Signature Verification Using Hidden Markov Models" *In Proceedings of The 2012 International Conference on Image Processing, Computer Vision, & Pattern Recognition*, Volume I, WORLDCOMP'12, Las Vegas, Nevada, USA, July 16 - 19, 2012, pp. 347-351.

[10] D. Kocharyan, H. Sarukhanyan, "High-Speed Fingerprint Recognition Method", *2nd International Conference on Multimedia Technology (ICMT2011)*, July 26 - 28, 2011, Hangzhou, China, pp. 5892 – 5895.

[11] D. Kocharyan, H. Sarukhanyan, "Feature Extraction Techniques and Minutiae-Based Fingerprint Recognition Process", *The International Journal of Multimedia Technology*, 2011, vol.1 No.1., 30.09.2011, pp. 31-35.