A Mahalanobis distance-based method for palmprint biometric identification

Sorin SOVIANY¹, Mariana JURIAN²

Rezumat. Articolul prezintă o soluție de identificare biometrică a persoanelor, în care se utilizează caracteristici extrase din regiuni de interes ale palmei. Metoda propusă utilizează distanța Mahalanobis pentru evaluarea similarității paternurilor biometric, iar stabilirea identității persoanelor se realizează prin maximizarea scorurilor de similaritate evaluate. Utilizarea distanței Mahalanobis în evaluarea similarității paternurilor biometric prezintă avantaje semnificative comparativ cu alte tipuri de distanțe, în special prin proprietățile sale de invarianță la scalare și de exploatare a corelațiilor dintre caracteristici. Metoda propusă îmbunătățește precizia sistemelor biometric de identificare.
Cuvinte cheie: distanța Mahalanobis, identificare, regiuni de interes.

Abstract. The paper presents a people biometric identification solution which are using features from the palmprint regions of interest (ROI). The proposed method uses the Mahalanobis distance in order to evaluate the biometric patterns similarity; the people identification is resulting through the matching scores maximization. The Mahalanobis distance using for the biometric patterns matching is suitable because of its main properties providing significant advantages for biometric data, especially the scaling invariance and feature correlation exploiting. The proposed method improves the identification biometric systems accuracy.

Keywords: Mahalanobis distance, identification, region of interests.

1. INTRODUCTION

The more actual approach in security system design and implementation for different applications is to embed biometrics as much as they are strong related to the persons who are presenting in order to perform the authentication process. [1] However, there are still some challenges in biometrics, and especially regarding on the identification applications. Actually the identification accuracy is still providing lower performances than the verification.

This is because of the more computational complexity which is featuring the identification task. [2] However, more applications require not only the pretended identity verification, but also to guess the people identities only based on their physiological and/or behavioral traits. In order to improve the actual performances for biometric identification systems, we proposed a solution based on features from palmprint regions of interests (ROI). Also in our approach, the matching scores are computed based on Mahalanobis distance estimation, because of its main properties: scale invariance and features correlation exploiting. [4][6] Some of the palmprint features are similar to the fingerprint ones (minutiae

² Universitatea din Pitesti, Facultatea de Electronică, Comunicații.
like delta, core, bifurcations), but palmprint provides more features because of its higher surface. [3]

The remainder of this paper is structured as follows. Section 2 presents the identification system architecture together with a brief description of its main functions. In section 3 we resumed the feature generation stage. Section 4 presents the matching score computing stage in order to perform the identification. The achieved results are given in section 5. Section 6 concludes our research and provides some further research areas.

2. THE IDENTIFICATION SYSTEM ARCHITECTURES AND ITS MAIN FUNCTIONS

Figure 1 depicts the palmprint identification system architecture with its main functional stages.

The basic functions of the palmprint identification system are the following:
- Feature generation function, which is performed on a specified palmprint region of interest which we achieved by training a Gaussian detector model;
- Matching function which computes a set of similarity scores between the current biometric pattern and N stored biometric templates (1:N matching)

The final decision is either on the matched identity (according to the resulting matching score) or the unrolled person identity, if no marching for no one of the enrolled identities. The system is designed for a security application which requires identification accuracy improvement.

3. PALMPRINT FEATURES GENERATION

For the palmprint biometric, we applied a feature generation strategy in 2 steps:
- defining region of interest by training a detector in order to make an initial decision for the most relevant image areas to be used for biometric templates generation;
- applying a co-occurrence matrix approach in order to achieve the features from the palmprint ROI defined by a classifier decisions, according to the 1st step of the features generation function.

Fig. 1. The palmprint-based identification system architecture.
3.1. Palmprint Region of Interest Selection

A palmprint image Region of Interest (ROI) is an image region which contains only the relevant details for our task, actually the most relevant features providing the best accuracy in people identification using the palmprint biometric (in our approach). Actually we are interest in select the region containing either main lines in the palmprint but also some fingerprint-like details or minutiae. In order to get a more easily way to define ROI we defined and trained a special kind of classifier for the manually-defined ROI in each image; this is a detector. Actually we trained the detector for a target class recognition (which is the palmprint ROI), and also to reject the data from all the remainder of the processed image (as not-target class). [8][9]

For the palmprint ROI detection we used a Parzen non-parametric estimation classification model. The essential mathematical model for the palmprint ROI detector is [7]

\[
p(x | y) = \frac{1}{N_z} \sum_{j=1}^{N_z} \frac{1}{h^2} K\left(\frac{z_j - x}{h}\right)
\]

(1)

where: \( p(x | y) \) is the class-conditional probability density function which is providing the detector decisions based on the Bayes rule; \( N_z \) – the training images dataset size (50); \( h \) – the kernel smoothing parameter. The optimal value which we found out for our palmprint data is 0.45; \( x \) – the current image data sample to be classified by the detector in order to return the ROI class; \( z_j \) – the training images data sample; \( K \) – the kernel function. We tried the following kernels for the Parzen-based palmprint ROI-image detector [10]:

- the Laplace kernel, given by
  \[ K(x, z) = \frac{1}{h} \exp\left(-\frac{|x - z|}{\sigma}\right) \]
  (2)

- the power-law based kernel, given by
  \[ K(x, z) = -\|x - z\|^p \]
  (3)

- the linear (homogeneous) polynomial kernel, given by
  \[ K(x, z) = \alpha x \cdot z \]
  (4)

In our experiments, the scaling coefficient \( \alpha \) provided best performance for palmprint ROI detection accuracy if ranging within (1.0; 1.5).

The decision of the palmprint ROI Parzen-based detector is relying on the following discriminant function [4, 10]:

\[
R(x) = p(x | y_{target}) \cdot P(y_{target}) - p(x | y_{non-target}) \cdot P(y_{non-target})
\]

(5)

where the class \( y_{target} \) is generated by the manually selection of a rectangular ROI in the best-quality training palmprint image for each of the 50 persons who provided their biometrics in our experiment. The class distribution \( y_{non_target} \) is the dataset which contains the image information outside the selected region. The class priors are provided by accounting the pixels from each of the image regions (ROI and background irrespectively).

Figure 2 depicts the performance trade-offs for the palmprint ROI detectors while using each of the three kernels.

The performances trade-offs for palmprint ROI Parzen-based detectors are resulting by applying the ROC analysis on the available palmprint images which are provided from 50 persons. The ROC analysis provided a set of operating points for each of the 3 Parzen detectors. From these sets we choose the optimal points which are minimizing the average classification error rate on the 2 class: ROI and non-ROI. In Table 1 we recorded the optimal operating points which we achieved while applying each of the 3 kernels in the Parzen detector model (Laplace kernel, Power-law kernel and Linear kernel).
A Mahalanobis distance-based method for palmprint biometric identification

Table 1

<table>
<thead>
<tr>
<th>Measure Kernel</th>
<th>Error on ROI class</th>
<th>Error on non-ROI class</th>
<th>Average error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laplace</td>
<td>0.27%</td>
<td>0.44%</td>
<td>0.355%</td>
</tr>
<tr>
<td>Power-law</td>
<td>0.28%</td>
<td>0.48%</td>
<td>0.38%</td>
</tr>
<tr>
<td>Linear</td>
<td>0.26%</td>
<td>0.57%</td>
<td>0.415%</td>
</tr>
</tbody>
</table>

The optimal operating point is the closest to the axis origin. From the Table 1 we could see that the kernel Laplace exhibited the best behavior for the palmprint image ROI Parzen-based detector. However, the best absolute performance for the palmprint ROI class was provided by the Linear kernel. Finally we decided to use only Laplace kernel, according to its optimal operating point.

3.2. Co-occurrence matrix for feature extraction

After ROI detection on palmprint images, we extracted the features from the regions of interest using the co-occurrence matrices. The co-occurrence matrix is an array which estimates, for each entry, of the probability that a pixel has a certain gray-level while a displaced pixel issues another intensity value. Having a \( m \times n \)-sized original image \( I \), its co-occurrence matrix \( C \) is given by eq. 6 [5]

\[
C_{m,N}(i,j) = P\{l(x,y) = i, l(x+\Delta x, y+\Delta y) = j\} \tag{6}
\]

where \( \Delta x \) and \( \Delta y \) are the offset parameters. The number of gray-level bins which we used for feature extraction from palmprint image ROI is 3, resulting in 9 features for the palmprint biometric recognition.
4. MATCHING SCORES BASED ON MAHALANOBIS DISTANCE

The matching stages for the palmprint identification process includes the following operations [7]:
- computing the distance \( d(x,z) \) between the palmprint biometric template \( z \) and the actual test palmprint sample \( x \);
- distance score normalization;
- distance to similarity-score conversion;
- computes the set of similarity scores for identification (1:N).

4.1. Distance in the feature space

In order to compute the distance score between the biometric template \( z \) and the current biometric sample \( x \), we used Mahalanobis distance, given by [6]

\[
D_{\text{M}}(x,z) = \sqrt{(x-z)^T \cdot \Sigma^{-1} \cdot (x-z)}
\]

where \( \Sigma \) is the 2 palmprint feature vectors co-variance matrix:

\[
\Sigma = \text{Cov}(x,z) = E[(x-E[x]) \cdot (x-E[z])^T]
\]

We used this distance metric in the feature vector space because of its main properties: scaling invariance and feature correlation exploiting [4, 6]. The 1st property is important especially while the application need to scale the features in order to compare them against different individuals and to study the features contribution on the identification accuracy. The 2nd property is important because it allows to earlier select the optimal feature subsets, according to their correlation, in order to avoid applying more computationally intensive feature selection algorithms.

4.2. Distance score normalization

The distance score normalization allows us to provide a common values range for all matching score which we are computing for the biometric patterns. There are a lot of available normalization techniques, such as z-score normalization, Min-Max normalization, decimal scaling normalization, sigmoid normalization and so on. [7] For our available biometric data we applied the double sigmoid function, given by

\[
D(x,z) = \begin{cases} 
1, & \text{for } d_{\text{M}}(x,z) < \theta \\
1 + A_1 \cdot \exp\left(-B_1 \cdot \left(\frac{d_{\text{M}}(x,z) - \theta}{C_1}\right)\right), & \text{for } d_{\text{M}}(x,z) \geq \theta 
\end{cases}
\]

in which:
- the coefficients \( A_1, A_2, B_1, B_2 \) are given from the experimental data; they are shape parameters for the sigmoid function;
- \( C_1 \) and \( C_2 \) are the quasi-linear behavior region boundaries for the sigmoid function; these parameters are provided from the experiment;
- \( \theta \) is a threshold value which is related to the security level which is settled for the application.

The normalized distance score is measuring the difference between the test palmprint feature vector \( x \) and the compared biometric template \( z \).

4.3. Distance to similarity conversion

In order to measure the similarity or the closeness of the current biometric sample \( x \) to the biometric template \( z \), it is necessary to apply a further transform so the highest scores provide more similarity and the lowest scores provide more difference. All the computed scores are in the range \([0,1]\), according to the property of the sigmoid function. Because of this range, the distance-to-similarity conversion could be performed by

\[
S = s(x,z) = 1 - D(x,z)
\]

4.4 Set of the similarity scores

We are computing \( N \) scores for each of the person to be identified, because the comparison is 1:N. Therefore, the identification similarity scores are given by
A Mahalanobis distance-based method for palmprint biometric identification

5. RESULTS

Figure 3 depicts the performance trade-offs for our system, while showing the average identification error rates which we achieved on 10 experiments. We selected 2 person and counted their identification attempts using the palmprint biometric.

From figure 3 we could see that the biometric system optimal operating point is featured by the following identification error rates:

- mean identification error rate on person A: 0.19%
- mean identification error rate on person B: 0.36%
- mean identification error rate on both persons A and B: 0.275%

The operating point for a biometric system is related by the application thresholding for the security requirements. Also the results are strongly depending on the biometric application. Usually the verification is much more accurate than the identification. In Figure 3 we represented the identification error rate, not false acceptance or false rejection error rates. We could see that moving on ROC curve to the right of the selected optimal operating point, the identification error rate for person A is increasing, going to almost 1%, and the identification error rate for person B is corresponding decreasing, going to almost 0 %. Similarly, moving to the left of
the fixed operating point improves the accuracy for the person A identification and decrease the accuracy for person B identification.

6. CONCLUSIONS

The biometric identification is still less accurate than the verification. This is mainly due to the computational complexity, as much as the process needs to perform much more comparisons than the verification task. One of the sources of this complexity is the high number of features which are used. In order to handle this trouble, for our palmprint identification system we applied a feature extraction solution with provided a low-sized feature space.

Although we applied an innovative strategy for feature, in order to avoid more complex procedures like PCA, LDA and some feature selection algorithms. Actually we trained a special kind of classifier in order to detect the region of interest in the palmprint image. This approach allowed as also to reduce the feature space size, because not all of the features which could be extracted have the same discriminant capacity. We are interest to achieve only the most relevant features.

On the other hand, we applied a special kind of distance in order to evaluate the similarity between the biometric patterns. Although Mahalanobis distance requires more computational complexity than Euclidian distance, it is better suitable for typical pattern recognition applications like biometric identification.

Despite of these improvements, the identification performance improvement still remains an opened trouble. This is due especially to the broad range of the security applications requirements. Some systems needs to provide not just the real identity of a person, but only to ensure that the person is within a list of the authorized people. However, other applications need to precisely identify a person who has to authenticate in order to get access to a protected critical resource.

References