Spatial surface coarseness analysis: technique for fingerprint spoof detection

L.F.A. Pereira, H.N.B. Pinheiro, G.D.C. Cavalcanti and Tsang Ing Ren

Proposed is a technique for fingerprint spoof detection, the spatial surface coarseness analysis. This approach improves the wavelet analysis of the fingerprint surface texture by introducing spatial features to the model. Thus, the accuracy of the fingerprint classification is increased to 70.09% compared with the original solution.

Introduction: Presently, the fingerprint is the most commonly used biometric identifier in authentication systems. It was responsible for more than 50% of the biometric revenue in 2009 [1]. According to Roberts [2], one way to overtake the security of those systems is providing to the sensor a fake physical biometric. Thus, an efficient technique for spoof detection [3,4] is an essential requirement for any fingerprint based system in operation.

Moon et al. [5] proposed a wavelet analysis of the fingerprint surface texture. This approach relies on the fact that commonly used materials in spoof fingerprints consist of large organic molecules which tend to agglomerate at the moment that the forgery is created. As a consequence, asperities are introduced to the surface of the fake fingerprints. In this method, the surface coarseness is modelled as Gaussian white noise added to the image. Moon et al. [5] achieved significant results for images captured in high resolution fingerprint scanner (~1000 dpi).

For economic reasons, most of the commercialised scanners nowadays generate images of lower resolution (typically, 500 dpi). In fact, the databases used in the second edition of the Fingerprint Livelihood Detection Competition (LivDet), in 2011, comprise only fingerprint images of 500 dpi [6].

Proposed technique: We propose a wavelet analysis of the fingerprint surface texture for each image region. This technique, the spatial surface coarseness analysis (SSCA), is described in three main steps: Coarseness mapping, Descriptor extraction and Classification.

Coarseness mapping: Coarseness in the fingerprint surface is mapped through the estimation of the residual Gaussian white noise added to the image [5]. The residual noise \(\eta(x,y)\) is defined by the following equation:

\[
\eta(x, y) = f(x, y) - f'(x, y)
\]

where \(f(x, y)\) is the original fingerprint image and \(f'(x, y)\) is the denoised image which is evaluated according to the stages described below:

(a) \(f(x, y)\) is decomposed in two levels using the discrete wavelet transform. It yields to one approximation and six details, \(g_k(x, y)\) with \(k \in \{1, 2, \ldots, 6\}\);

(b) each one of the details is denoised using the hyperbolic shrinkage method [7]:

\[
\hat{g}_k(x, y) = \text{sgn}(g_k(x, y))\sqrt{|g_k(x, y)^2 - \delta^2|},
\]

\[
\delta = \sqrt{2\log(N)}\sigma
\]

where \(\text{sgn}(a)\) is the signal of \(a\), \(a_{\text{max}}\) is the maximum value between \(a\) and zero, \(N\) is the length of \(g_k(x, y)\) and \(\sigma\) is the standard deviation of the three details obtained in the first level of decomposition;

(c) \(f'(x, y)\) is obtained through the wavelet reconstruction from the approximation and the details previously denoised, \(g_k'(x, y)\).

Descriptor extraction: To generate a descriptor, the coarseness map is divided into \(\frac{1}{p_x} \times \frac{1}{p_y}\) partitions, as shown in Fig. 1. The standard deviation of each partition is calculated to generate a deviation map, which is divided into \(\frac{1}{q_x} \times \frac{1}{q_y}\) sections. For each section of the deviation map, a histogram of \(\lfloor \frac{q_y}{q_x} \times \frac{q_y}{q_x} \rfloor\) bins is computed. The final descriptor is obtained through the concatenation of the histograms of all sections of the deviation map. The most suitable value for the 4-tuple \([p_x, p_y, q_x, q_y]\) is determined using a genetic algorithm (GA).


In the Descriptor extraction step, the GA obtained the optimal value for \([p_x, p_y, q_x, q_y]\), which is \(\frac{1}{25} \times \frac{1}{25} \times 1 \times 1\). Thus, each fingerprint image generated a descriptor of length equal to 162. Fig. 2 shows the obtained descriptors for a spoof and a live fingerprint image.

Table 1 presents the results obtained using the SSCA technique, the analysis of the fingerprint surface texture proposed by Moon et al. [5] and the best algorithm submitted to the LivDet 2011 (Federico).

<table>
<thead>
<tr>
<th>Technique</th>
<th>FAR (%)</th>
<th>FRR (%)</th>
<th>ACE (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moon et al.</td>
<td>38.7</td>
<td>46.9</td>
<td>42.8</td>
</tr>
<tr>
<td>Federico</td>
<td>13.8</td>
<td>13.1</td>
<td>13.4</td>
</tr>
<tr>
<td>SSCA</td>
<td>11.3</td>
<td>14.4</td>
<td>12.8</td>
</tr>
</tbody>
</table>

Classification: The descriptor is classified with a support vector machine (SVM) using a polynomial kernel which operates in a k-dimensional vectorial space, where \(k\) is the descriptor length.
Conclusion: A new technique for fingerprint spoof detection, the SSCA, has been proposed. The average classification error (ACE) related to this technique was 70.09% lower than that obtained using the original solution proposed by Moon et al. [5]. This improvement is due to the introduction of spatial features in the analysis of the texture of the fingertip surface. Furthermore, the SSCA technique was more efficient than the best algorithm submitted to the LivDet 2011 [6].

Acknowledgments: This work was partially supported by CAPES, CNPq and FACEPE.

References