judge the presence and absence of moving objects by the contour of the signal.

We acquire the contour of the signal in two steps. First, the signal is multiplied by itself, \( R(R) = R \ast R \). We then use a low-pass filter to filter \( R(R) \). The bandwidth of the filter is determined according to the knowledge of size and speed of moving objects in the scene. The part of the signal that the local maxima of which are lower than a threshold can be considered as background. We can then obtain the labels of the different parts. In this procedure, not only is the value of the pixel used to justify the classification, but also the temporal consistency is utilized implicitly. The entire process is illustrated in Fig. 1.

Experimental results: Image sequences of natural outdoor scenes were captured using a static camera (see Figs. 2 and 3). Figs. 2d and 3d show the restored initial background image. We can see that the extracted background image is very accurate even though many objects are moving in the scenes. After each primary value is extracted, we classify pixels using simple thresholding to detect the moving objects, as shown in Figs. 2e and 3e. Segmentation using our method is also performed, and the results are shown in Figs. 2f and 3f.

It can be seen that segmentation based on our method is significantly more accurate than segmentation using the conventional method. For real-time implementation, our algorithm requires more machine memory to memorise the volume as buffer. However, this is not a problem for today’s computers. Our algorithm is also slower than the conventional method, especially when there are many moving objects in the scenes. However, the new method is fast enough to be implemented in real-time (many possible improvements can be made to achieve real-time performance such as using faster computers or by optimising source codes).

Discussion and future work: We have proposed a new framework to estimate the background image and detect moving objects for video surveillance applications. The method can also be applied to other situations that satisfy our assumption, for example teleconferencing. It can easily be extended to colour image sequences. For colour image sequences, it is easier to classify the pixels, as more information is provided. A decision fusion method can be adopted to improve the algorithm. Future work will focus on improving the algorithm, not only to segment moving objects, but also to estimate moving parameters from one volume.

Acknowledgment: This work is funded by NSFC (Grant No.59825105) and the Chinese Academy of Sciences.

© IEE 2001
24 October 2000
Electronics Letters Online No: 20010836
DOI: 10.1049/el:20010836
Hongzan Sun and Tianiu Tan (National Laboratory of Pattern Recognition (NLPR), Institute of Automation, Chinese Academy of Sciences, 100080, Beijing, People’s Republic of China)
E-mail: sunhz@nlpr.ia.ac.cn

References

Wavelet domain features for fingerprint recognition

M. Tico, P. Kuosmanen and J. Saarinen

A fingerprint recognition approach based on features extracted from the wavelet transform of the discrete image is presented. The efficiency of the method is proven by the high recognition rates achieved using the k-nearest neighbour (k-NN) classifier. The method requires lower computational effort than most of the fingerprint recognition methods proposed to date.

Introduction: Several approaches of automatic fingerprint matching have been proposed in the literature. The most popular ones are based on the minutiae pattern of the fingerprint and are collectively called minutiae-based approaches. Although rather different from one another, most of these methods require extensive preprocessing operations (e.g. orientation flow estimation, ridge segmentation, ridge thinning, minutiae detection) in order to reliably extract the minutiae features [1]. Another class of fingerprint matching approaches do not use the minutiae features of the fingerprint. They either match directly the fingerprint images [2], or match features extracted from the image by means of certain filtering or transform operations [3], hence their name image-based methods. These approaches require less preprocessing effort than minutiae-based methods but, on the other hand, they have a limited ability to track variations in position, scale and rotation angle. The variation in position is usually cancelled by registering the images with respect to a reference point which can be consistently detected in different instances of the same fingerprint. Such a reference point may be the core point of the fingerprint image [3]. In this Letter, we propose an image-based approach towards fingerprint recognition. The fingerprint images are matched based on features extracted in the wavelet transform domain.

Wavelet domain features: The two-dimensional (2D) wavelet decomposition on J octaves of a discrete image \( a(n, m) \) represents the image in terms of \( 3J + 1 \) subimages

\[
\begin{align*}
  a_j, \{d_{j1}, d_{j2}, d_{j3}\} & \quad j = 1, \ldots, J
\end{align*}
\]

where \( a_j \) is a low resolution approximation of the original image, and \( d_{j1}, d_{j2}, d_{j3} \) are the wavelet subimages containing the image details at different scales (2) and orientations (6). Wavelet coefficients of large amplitude in \( d_{j1}, d_{j2}, d_{j3} \) correspond, respectively, to vertical high frequencies (horizontal edges), horizontal high frequencies (vertical edges), and high frequencies in both directions [4].

Fingerprints are quasi-periodic patterns whose dominant frequencies are located in the middle frequency channels. The ridge orientation as well as the ridge spatial frequency in different image regions represent the intrinsic nature of the fingerprint image. Both kinds of information are well extracted into the wavelet coefficient subimages \( d_{j2} \).

The normalised L2-norm of each wavelet subimage is computed in order to create a feature vector of length \( 3J \)

\[
\begin{align*}
  \{f_{21}, f_{22}, f_{23}\} & \quad j = 1, \ldots, J
\end{align*}
\]
where

\[ e_k^j = \left( \sum_{i=1}^J \sum_{l=1}^N \| \mathbf{d}_i^l \|_2 \right) \]

for all \( j = 1, \ldots, J \), and \( k = 1, 2, 3 \).

The feature vector represents an approximation of the image energy distribution over different scales (2) and orientations (\( k \)). It exhibits valuable discriminatory properties for fingerprint patterns, as shown in Fig. 1. All three images shown in this Figure have been decomposed on 4 octaves, and the corresponding feature vectors of length 12 have been computed as in eqns. 2 and 3. In order to facilitate the visual inspection the feature vectors are represented as grey-levels, emphasizing also the scale level (\( j \)) and the orientation (\( k \)) of each component. Note the high degree of similarity between feature vectors extracted from images representing the same finger (the first two images), and the important differences between the feature vectors extracted from images which represent different fingers.

The intersection operator introduced by Swain and Ballard in [5] is used in our work as a measure of similarity between two feature vectors.

**Table 1**: Recognition rate in different wavelet basis (a) and comparative results on subset of the database (b)

<table>
<thead>
<tr>
<th>Filter</th>
<th>1-NN</th>
<th>2-NN</th>
<th>3-NN</th>
<th>4-NN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daubechies 5</td>
<td>84.4</td>
<td>91.3</td>
<td>92.4</td>
<td>92.9</td>
</tr>
<tr>
<td>Daubechies 6</td>
<td>82.3</td>
<td>91.3</td>
<td>95.2</td>
<td>94.0</td>
</tr>
<tr>
<td>Daubechies 10</td>
<td>80.9</td>
<td>91.3</td>
<td>92.4</td>
<td>95.2</td>
</tr>
<tr>
<td>Symmetric 6</td>
<td>85.0</td>
<td>92.9</td>
<td>95.2</td>
<td>92.9</td>
</tr>
<tr>
<td>Symmetric 9</td>
<td>83.0</td>
<td>92.1</td>
<td>94.3</td>
<td>94.1</td>
</tr>
<tr>
<td>Symmetric 10</td>
<td>80.3</td>
<td>90.5</td>
<td>92.4</td>
<td>94.1</td>
</tr>
<tr>
<td>Proposed method (a)</td>
<td>91.2</td>
<td>97.4</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Method proposed in [3]</td>
<td>90.1</td>
<td>98.7</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Gabor (b)</td>
<td>90.1</td>
<td>98.7</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

Experimental results: The database of [6], which contains 168 fingerprint images collected from 21 individuals (8 images per finger) was used for the experiments. All images in the database were 256 x 256 in size and had been captured with 256 grey levels using an inkless fingerprint scanner.

The recognition performances achieved by using the proposed wavelet features were evaluated using a k-NN classifier, with no rejection option. A number of \( K \) images from each individual were used as the training set, whereas the remaining \( K - k \) images from each individual were used for testing.

A wavelet decomposition on 6 octaves of each fingerprint image was performed in order to extract a feature vector of length 18. We have tested different wavelet bases, and the best results were achieved using Daubechies, and Symmetr orthonormal wavelet filters [4]. The recognition rates obtained by using Daubechies filters with 5, 6, and 10 vanishing moments, as well as Symmlet filters with 6, 9, and 10 vanishing moments, are shown in Table 1a. High recognition rates of 95.2% were achieved for the 3-NN and 4-NN classifiers. The relatively low recognition rate of 85% for the 1-NN classifier is due to the fact that several pairs of images collected from the same individual exhibit portions of the fingers which overlap in less than 30% of their area.

We compared our approach with the method proposed by Lee and Wang in [3]. In their method, Lee and Wang used Gabor filter-based features for fingerprint recognition. The method requires first the detection of the reference point (core point) in the fingerprint image. The magnitude Gabor features are then extracted only from a small subimage centred in the core point. In order to test their method we had to select from our database a subset of 164 fingerprint images which exhibit a core point close to the centre of the image. The selected images represent the fingerprints collected from 13 individuals (eight images per finger). The core points were indicated manually and the magnitude Gabor features extracted on 4 orientations from a 64 x 64 subimage centred in the core point of each fingerprint. Dividing the 64 x 64 central subimage into a set of 8 x 8 non-overlapping blocks and sampling this set using the Gabor filters, we obtained a feature vector of length 256 containing magnitude Gabor features. The only difference with respect to the original method was the size of the central subimage chosen in each fingerprint. We found that a larger central subimage than 64 x 64 would also include extraneous details located outside the fingerprint pattern and therefore would decrease the performance of Lee and Wang's method. The recognition rates achieved by the method proposed in [3] are identical to the recognition rates achieved by our method using a Symmlet orthonormal wavelet filter with 9 vanishing moments, as shown in Table 1b. Nevertheless, our method was applied directly onto the entire image with no prior operations such as detection of the core point or extraction of a central subimage. In addition, we used a much smaller feature vector (of length 18) than the feature vector (of length 256) required in this case by the method of Lee and Wang.

Conclusions: We have introduced a new approach towards fingerprint recognition based on wavelet domain features. The features are directly extracted from the wavelet transform of the discrete fingerprint image, with no preprocessing. The high recognition rates achieved show that the proposed wavelet features exhibit valuable properties for matching complex patterns of oriented texture-like fingerprints.

© IEE 2001

**References**


**Remarks on Wang-Chang's password authentication scheme**

C.-K. Chan and L.M. Cheng

An attack on a remote password authentication scheme proposed by Wang and Chang is presented. It is shown that the scheme is breakable. An intruder can easily construct a valid login request from a previously intercepted one and replay it later to pass the system authentication process.

Introduction: In [1], Wang and Chang proposed a smart card based password authentication scheme the security of which rests in part on the difficulty of factoring a large number and discrete logarithm problem. The scheme has several merits: (i) users can freely choose their preferred passwords; (ii) the remote system does not require verification tables to verify the legitimacy of the login users; (iii) the remote system is protected against replay by time stamping the password. However, in this Letter, we show that an intruder can easily construct a valid login request from a previously intercepted one and replay it later to pass the system authentication process.