Off-line Signature Verification Using Structural Features

Sohail Zafar
Department of Computer Science
City University Peshawar
+92–314–9194508
suhail_tajik@yahoo.com

Rashid Jalal Qureshi
Department of Computer Science
Islamia College Peshawar
+92–346–9147629
rashidjalal@hotmail.com

ABSTRACT
Biometric identification is an emerging technology that can solve the security problems in our networked society. A lot of work has been done in the field of automatic off-line signature verification. While a large portion of the work is focused on random forgery detection, more efforts are still needed to address the problem of skilled forgery detection. In this paper a novel method for signature verification is proposed. In this method, each pixel belonging to signature is studied and endpoints from the geometry of the signature are extracted. A polygonal closed shape is drawn by joining these endpoints. Various structural features from the shape including parameter, area, minimum enclosing rectangle, rectangularity measure, and circularity measure and form factors are computed. These features were combined to build a verification function, which is evaluated using statistical procedures.

Keywords
Signature verification, Structural features, forgeries, Euclidean distance model

1. INTRODUCTION
Off-line signature verification can be used in many applications such as cheques, certificates, contracts and historical documents. A signature verification system can be classified as either online or offline. In an online system, a signature data can be obtained from an electronic tablet and in this case, dynamic information about writing activity such as speed of writing, pressure applied, number of strokes available [1, 2]. In off-line systems, signatures written on paper are converted to electronic form with the help of a camera or a scanner and obviously, the dynamic information is not available. To classify two signatures as belonging to the same class or two different classes, the intraclass scatter should be as low as possible whereas the interclass scatter should be high as possible [5]. We can monitor the variability by extracting feature in any recognition and classification systems. Marianne P. et al. [6] presented offline signature verification system that uses simple voting scheme in classifier fusion. Each classifier uses a different feature set namely global, grid gray, and intensity distribution. In voting, the classifier determines whether the query signature does not exceed its corresponding threshold. Emre Özgündüz[7] developed system they used features sets namely global, mask and grid features for learning and classification process. In [8] another method for the classification and verification using feature point is presented. The scheme is based on selecting 60 feature points from the geometric center of the signature and compares them with the already trained features points. Structural approach includes neural networks [9, 10], Hidden Morkov Model [11], Euclidean distance classifier [12] and elastic image [13]. In this paper, we also extracted features using the structural approach.

2. PROPOSED METHOD
Machine recognition and verification of signatures is a very special and difficult problem. Based on the feature sets of the mentioned papers we extract only the end points of the signature for the classification and based on that we calculate different measurements from the drawn shape. Our proposed solution involves:

- Acquire Signature from Camera or Scanner
- Signature Preprocessing
- Feature Extraction
- Signature Classification

2.1 Signature Preprocessing
Any image-processing application suffers from noise like touching line segments, isolated pixels and smeared images results in poor recognition and verification rate. Therefore, a preprocessor is used to remove noise. Thinning of the signature images are performed using morphological operators to get one-pixel thin lines of the signatures.

2.2 Feature Extraction Phase
The structural features have been extracted from the geometry of the signatures. Structural features are easier to extract and are more representative of the shape as compared to statistical features. Signature image is scanned from left to right pixel by pixel and we marked endpoints.

Algorithm
Input: A Signature Image
Output: A Polygonal shape formed by joining Endpoints.

Begin
While (end pixel is not encountered )
   Scan image from left to right
   
if ((current pixel belong to signature) AND (has 1 Neighbor Pixel atmost) )
   then
      Begin
         endpoints_count ++
         Save (x, y) coordinates of the endpoint encountered
      End
   END WHILE

   Join all end points whose coordinates were stored in above loop
End

By applying the above described algorithm we got different shapes that are

![Fig. 3 Shapes drawn from original signatures](image)

1. Perimeter
2. Area
3. Circularity Measure
4. Rectangularity Measure
5. Minimum enclosing rectangle
6. Form factor

![Thinning and Endpoints](image)

![Joined Points](image)

![Polygon Extracted](image)

Fig. 2. various stages for extracting polygon

2.3 Signature Classification
Euclidean distance is the most common measure of dissimilarity and is used by our system. It is defined as:

\[
d(S_i, x) = \sqrt{\sum_{n} (a_i - b_i)^2}
\]

Where \( d \) is the distance between signatures \( S_a \) and \( S_b \), and \( a_i \) and \( b_i \) are feature vector elements. The feature vectors are of length \( n \). The NNR is formulated as:

\[
d(S_i, x) = \text{MIN}_i \{ d(S_i, x) \}
\]

Where \( d \) is the distance measure, the set of samples \( \{S_1, S_2, S_3, ..., S_i, ..., S_N\} \) is called the learning set, and \( x \) is the unknown sample to be classified. Two signatures are similar if the Euclidean distance of their feature vectors is relatively small.

3. RESULTS AND DISCUSSION
False Acceptance Rate (FAR) and False Rejection Rate (FRR) are the two parameters used for measuring performance of any signature verification method. FAR is calculated by equation 6 and FRR is calculated by equation 7.

\[
FAR = \frac{\text{number of forgeries accepted}}{\text{number of forgeries tested}} \times 100
\]

\[
FRR = \frac{\text{number of originals rejected}}{\text{number of originals tested}} \times 100
\]

The database comprised of 450 signatures that were collected from 25 people. Among the 25 people, 15 were asked to provide signatures for building the authentic signature database.
Five of the people were asked to produce a set of simple forgeries, and the other five were asked to produce a set of skilled forgeries to the signature of the 15 subjects. The performance of each verification function was evaluated using the verification error rate. We compared our algorithms with 60 feature points Scheme [8]. The accuracy of detecting genuine was 92%. The proposed algorithm with structural feature got better results than geometric features. The suggested algorithm successfully rejected skilled forgeries with good rate and was perfect in rejecting simple forgeries as shown in table 1. Our method showed the FAR and FRR much less as compared to the FAR and FRR of the other feature points based scheme (see table 2).

| Table 1: Comparative analysis of FAR |
|-----------------|-----------------|-----------------|
| Forgery Type    | 60 feature points Scheme [8] | Proposed method |
| Simple          | 0.98            | 0.73            |
| Skilled         | 2.08            | 1.57            |

<table>
<thead>
<tr>
<th>Table 2: Comparative analysis of FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>False Rejection Rate (FRR)</td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td>60 feature points Scheme [8]</td>
</tr>
<tr>
<td>Proposed method</td>
</tr>
</tbody>
</table>

4. CONCLUSION
In this paper a new offline signature verification scheme has been proposed. The scheme is based on extracting endpoints from the geometry of the signature. A closed shape is drawn by joining the endpoints extracted from the signature. Various measurement have been calculated from the shape that are parameter, area, minimum enclosing rectangle, rectangularity measure, circularity measure and form factors. It require less effort to find end points in the target signature than those who extracts different feature sets as the grid features, global features, grid features etc. The scheme differentiates between originals and forged signatures. This scheme discriminates between simple and random forgeries.

5. REFERENCES