NOVEL FEATURE EXTRACTION TECHNIQUE FOR OFF-LINE SIGNATURE VERIFICATION SYSTEM

DR. DARAMOLA SAMUEL
Department of Electrical and Information Engineering, College of Science and Technology, Covenant University, Canaan-land, Ogun State, Nigeria. dabaslectcu@yahoo.com

PROF. IBIYEMI SAMUEL
Department of Electrical Engineering, Faculty of Engineering, University of Ilorin, Ilorin, Kwara-State, Nigeria. tsibiyemi@yahoo.com

Abstract: Feature extraction stage is the most vital and difficult stage of any off-line signature verification system. The accuracy of the system depends mainly on the effectiveness of the signature features use in the system. Inability to extract robust features from a static image of signature has been contributing to higher verification error-rates particularly for skilled forgeries. In this paper, we propose an off-line signature verification system that incorporates a novel feature extraction technique. Three new features are extracted from a static image of signatures using this technique. From the experimental results, the new features proved to be more robust than other related features used in the earlier systems. The proposed system has 1% error in rejecting skilled forgeries and 0.5% error in accepting genuine signatures. These results are better in comparison with the results obtained from previous systems.

Keywords: Off-line Signature Verification, Feature Extraction, Euclidean distance model.

1. Introduction

Handwritten signature is accepted widely as biometric characteristic for personal and document authentication; this makes automatic signature verification an important research area in the field of pattern recognition. Automatic signature verification system can be classified into two categories called on-line and off-line. In an off-line technique, signature is signed on a piece of paper and scanned to a computer system. In an on-line technique, signature is signed on a digitizer and dynamic information like speed, pressure is captured in addition to a static image of signature. Verification decision is usually based on local or global features extracted from signature under processing. Excellent verification results can be achieved by comparing the robust features of the test signature with that of the user’s signature using appropriate classifier [1], [2].

Researches in on-line signature verification have been reported with high success rates. However, off-line signature verification researches are relatively unexplored; this apathy can be attributed to the inherent limitation of available features from a static image of signatures. Nevertheless, off-line signature verification systems are still largely in use; major areas of application of off-line signature verification systems include: authentication of bank cheques, attendance register monitoring and visa application [3], [4].
Different features extraction techniques have been reported for off-line signature verification systems. Discrete Radon Transform (DRT) method [5], Discrete Wavelet Transform (DWT) technique [6] and Inverse Fourier Transform (IFT) [7] are used to extract global features from a static image of signature in previous systems. Also graphometrics features: Axial slant angle, pixel distribution, pixel density, centre of gravity and stroke curvature are extracted from a static image of signature using grid segmentation method [8],[9],[10],[11],[12],[13],[14]. In [15], vertical and horizontal centre points are extracted from a static image of signature using vertical and horizontal points splitting technique whereas in [16], gradient, structural and concavity features are extracted from a binary signature image for verification.

The feature extraction techniques used in previous off-line signature verification systems discussed above have some limitations that make it difficult for them to detect skilled forgeries effectively. Therefore many of the previous techniques are only meant to detect simple and random forgeries. In this paper, off-line signature verification system that incorporates a new feature extraction techniques in order to overcome the deficiencies arose from previous systems is proposed. Three robust features are extracted from a static image of signature using this new method, they are image cell size, image centre angle relative to the lower cell corner and pixel normalized angles relative to the lower cell corner.

This paper is organized into eight sections. Following an introduction of the topic in section 1, section 2 describes the proposed system and data acquisition procedure; in section 3 the preprocessing stage is presented; section 4 introduces the new feature extraction method; training strategy and threshold selection are discussed in section 5; section 6 describes signature classification process; section 7 shows the experimental results and finally, conclusion is presented in section 8.

2. System Description and Data Acquisition

The off-line signature verification system proposed in this study is basically divided into five stages as shown in figure 1.

![Block diagram of the proposed system](image)
The first stage deals with collection of signatures followed by pre-processing and the novel feature extraction process as the second and third stage respectively. The fourth stage describes the training process where the aim is to obtain the user’s signature templates. And the final stage describes the signature classification process between the test signature and the user’s signature template.

Genuine signatures were collected from 100 students at Covenant University Ota Nigeria; each student contributed 7 genuine signature samples. 200 forgeries made of 100 simple forgeries and 100 skilled forgeries were collected from 20 forgers. Each forger contributed 10 forgeries. The genuine signatures were collected over a period of three months to account for variations in the signatures with time. The forgeries were also collected over a similar time period. The simple forgeries were obtained by given only the names of the users to the forgers who did not have any knowledge about the user’s genuine signatures. The skilled forgeries were obtained by given users genuine signatures to the forgers who were allowed to practice for a while before imitating them to create the forgeries. Figure 2 shows the example from the database of genuine signatures in first column with their corresponding skilled and simple forgeries in second and third column respectively.

3. Static Signature Image Preprocessing

Off-line signature image preprocessing presented here can be broken down into three stages as follows: (1) Spatial Smoothing (2) Binarization and (3) Morphological filtering.

4. Novel Feature Extraction Technique

In this paper, a new feature extraction technique based on signature image splitting is presented. The centre of gravity of the signature image is used for the splitting. The signature images are partitioned into rectangular cells at moderate resolution in such way that all gradient information of the signature strokes is acquired. Three robust features are extracted from the signature image. The extracted features are able to capture invariant signature characteristic at local, intermediate and global level. The features are image cell size (F1), image centre angle relative to the cell lower right corner (F2) and pixels normalized angle relative to the lower right corner (F3). The feature extraction algorithm is stated as follows:

1. Locate signature image bounding box.
   (i) Scan the binary image from top to bottom to obtain the signature image height.
   (ii) Scan the binary image from left to right to obtain the signature image width.

2. Centralization of the signature image.
   (i) Calculate centre of gravity of the signature image using Eq. (1).

Fig2: Example of genuine signatures and forgeries from the database.
\[
\bar{x} = \frac{1}{N} \sum_{i=1}^{N} x(i), \\
\bar{y} = \frac{1}{N} \sum_{j=1}^{N} y(j).
\]

(ii) Then move the signature image centre to coincide with centre of the predefined image space.

3) The image is partitioned into four sub-image parts as shown in figure 3a.
   (i) Through point \(\bar{x}\) make a horizontal splitting across the signature image.
   (ii) Through point \(\bar{y}\) make a vertical splitting across the signature image.

4) Partition each sub-image part into four rectangular parts as shown in figure 3b
   (i) Locate the centre of each sub-image part using Eq. (1).
   (ii) Repeat step 3(i) and 3(ii) for each sub-image part, to obtain a set of 16 sub-image parts.

5) Partition each of the sub-image parts in figure 3b into four signature cells
   (i) Locate the centre of each of the sub-image part using equation (1).
   (ii) Repeat step 3(i) and 3(ii) for each sub-image part, to obtain a set of 64 sub-image cells.

6) Find the size of each of the 64 cells and normalize them with the number of the black pixels in the cells,
   (i) Calculate the height and width of each cell and use this value to obtain the cell size.
   (ii) Count the number of black pixels in each cell.
   (iii) Divide cell size by the number of black pixels.

   The feature extracted at stage 6; constitutes the set of the first feature (F1).

7) Calculate the angle of inclination of each sub-image centre in each cell to lower right corner of the cell.
   (i) Locate the centre of each of the 64 sub-image cells using equation (1).
   (ii) Calculate the angle that each centre point makes with the lower right corner of the cell.

   The features extracted at stage 7; constitutes the set of the second feature (F2).

Fig 3: Feature extraction diagrams
(8) Calculate the summation of the angle of inclination of each black pixel to the lower right corner in each cell and normalize by the number of black pixels.

(i) Calculate the angle of inclination of each black pixel point in each cell to the lower right corner of the cell.

(ii) Sum the angles in each cell.

(iii) Normalize the sum of the angles with the number of black pixels.

The feature extracted at stage 8; constitutes the set of the third feature (F3).

The three robust feature sets (F1, F2 and F3) obtained from this new feature extraction; are the feature representation of each user’s signature. Each feature set has 64 vector components (f₁, f₂, f₃,………..f₆₄).

5. Training and Threshold Selection

In the training stage, threshold value for each registered user is calculated independently based on each feature. Five out of the seven signatures collected from each user are used to determine this threshold value. Given that five training signature samples are represented as S₁, S₂, S₃, S₄, S₅ and the corresponding feature vector components of each signature are represented as t₁, t₂, t₃,………..t₆₄. That is:

\[
S₁ = [t₁₁, t₁₂, t₁₃, \ldots, t₁₆₄] \\
S₂ = [t₁₂, t₂₂, t₂₃, \ldots, t₂₆₄] \\
S₃ = [t₁₃, t₃₂, t₃₃, \ldots, t₃₆₄] \\
S₄ = [t₁₄, t₄₂, t₄₃, \ldots, t₄₆₄] \\
S₅ = [t₁₅, t₅₂, t₅₃, \ldots, t₅₆₄] 
\]  

The mean values (t mean) of each corresponding feature vector components are obtained. These values constitute the template feature vector (T) as represented by Eq. (3).

\[
T = [\text{t mean}_{f₁}, \text{t mean}_{f₂}, \ldots, \text{t mean}_{f₆₄}] .  
\]  

(3)

Standard deviations (σₕ) of training sample components from template samples components are calculated and these values are used to obtain individual threshold (θ) value for each user based on each feature as given by Eq (4).

\[
\text{Threshold } \theta = \sqrt{\sum_{f_i} \sigma^2_f} . 
\]  

(4)

6. Off-line Signature Verification

The last stage is the verification stage; this stage compares the incoming test signature with the user’s signature templates in the database. The Euclidean distance model is one of the most suitable classifier used to obtain distance measurement between two vectors of equal size on a two dimensional plane [15]. In this paper, given that \( T_f \) is the template feature vector of size \( f \), \( T_f \) and \( I_f \) is the incoming feature vector of size \( f \).

Euclidean distance (d) between the template feature vector and the incoming signature feature vector is calculated by using Eq. (5).

\[
(d) = \sqrt{\sum_{f_i} (T_f - I_f)^2} .  
\]  

(5)

The Euclidean distance (d) of equation (5) and threshold (θ) of equation (4) is compared based on each feature for each user. If (d) is less than or equal to (θ) then the incoming signature is accepted and a pass mark is assigned to the signature otherwise the signature is rejected with no pass mark assign to it. The final decision of accepting or rejecting incoming test signature is based on total accumulated pass marks acquired using the three features.
7. Experimental Results

Experiments have been conducted to evaluate the discriminative ability of the new features in comparison with related features used in previous systems. Total number of 160 signatures made up of 80 genuine signatures and 80 skilled forgeries are tested. Table 1 shows the results of the performance of these new features in comparison with previous related features. The performance evaluation is based on False Acceptance Rate (FAR) and False Rejection Rate (FRR). Also the proposed system is tested based on the three new features. Total numbers of 500 signatures made up of 200 genuine signatures, 100 random forgeries, 100 simple forgeries and 100 skilled forgeries are tested. FRR and FAR are calculated for our testing purpose. Table 2 shows the FAR for random, simple and skilled forgeries and table 3 shows the FRR for genuine signatures.

8. Conclusion

An efficient Off-line verification system is needed to detect all kinds of forgeries particularly in paper documentation environment, like banks, schools and government ministries. The achievement made in this work will go a long way to improve the current situation in this research area. The three new features extracted in this work are robust enough to prevent signature forgeries. The experimental results have shown the ability of the proposed system against all kinds of forgeries.

<table>
<thead>
<tr>
<th>Type</th>
<th>Feature</th>
<th>FRR</th>
<th>FAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some previous related features</td>
<td>Pixel density</td>
<td>17.50</td>
<td>18.75</td>
</tr>
<tr>
<td></td>
<td>Pixel distribution</td>
<td>16.25</td>
<td>16.25</td>
</tr>
<tr>
<td></td>
<td>Axial slant.</td>
<td>2.50</td>
<td>3.75</td>
</tr>
<tr>
<td></td>
<td>Vertical centre points</td>
<td>7.50</td>
<td>8.75</td>
</tr>
<tr>
<td></td>
<td>Horizontal centre points</td>
<td>6.25</td>
<td>7.50</td>
</tr>
<tr>
<td>Proposed features</td>
<td>Image cell size (F1)</td>
<td>2.50</td>
<td>3.75</td>
</tr>
<tr>
<td></td>
<td>Image centre angle relative to the cell lower right corner (F2)</td>
<td>2.50</td>
<td>2.50</td>
</tr>
<tr>
<td></td>
<td>Pixels normalized angle relative to the cell lower right corner (F3)</td>
<td>1.25</td>
<td>2.50</td>
</tr>
</tbody>
</table>
Table 2: False Acceptance Rate (FAR) Result

<table>
<thead>
<tr>
<th>Type of Forgery</th>
<th>Number of Signatures</th>
<th>Number of Signatures Accepted</th>
<th>Number of Signatures Rejected</th>
<th>FAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random</td>
<td>100</td>
<td>0</td>
<td>100</td>
<td>0%</td>
</tr>
<tr>
<td>Simple</td>
<td>100</td>
<td>0</td>
<td>100</td>
<td>0%</td>
</tr>
<tr>
<td>Skilled</td>
<td>100</td>
<td>1</td>
<td>99</td>
<td>1%</td>
</tr>
</tbody>
</table>

Table 3: False Rejection Rate (FRR) Result

<table>
<thead>
<tr>
<th>Type of Signature</th>
<th>Number of Signatures</th>
<th>Number of Signatures Accepted</th>
<th>Number of Signatures Rejected</th>
<th>FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genuine</td>
<td>200</td>
<td>199</td>
<td>1</td>
<td>0.5%</td>
</tr>
</tbody>
</table>

References