A Comparative Analysis of Offline Signature Verification using Zernike Moment and Minutiae using Artificial Neural Network Approach

Divyot Singh Puri
Research Scholar
Department of Computer Sc.
National Institute of Technical Teachers Training & Research

Maitreyee Dutta, Ph.D
Professor & Head
Department of Computer Sc.
National Institute of Technical Teachers Training & Research

ABSTRACT
Signature verification is the oldest and widely used biometrics offering offline (static) and online (dynamic) verification schemes. It has been observed that offline scheme is more complex because of the absence of stable dynamic characteristics and factors like stylish and unconventional writing styles but still it is more into use as it does not require signer’s attendance as it is already stored in the database. The paper presents an offline handwritten signature verification system using ANN classifier. In this paper we attempt to compare the performance of two feature extraction schemes such as Zernike Moment and Minutiae feature in terms of Accuracy, False Acceptance Rate (FAR) and False Rejection Rate (FRR) to recognize the signature. Despite of substantial research in the field of signature verification involving Zernike Moment, almost no attention has been dedicated to Minutiae feature although it has been widely used as a means of biometrics to recognize fingerprints. The proposed method comprises of image enhancement techniques like Power Law Transformation, Ripplet II Transformation and Fractal Dimension. Using a database of 40 signatures it has been observed that Zernike Moment feature shows an encouraging accuracy of 95.5596115 and FRR of 4.336188 over Minutiae feature with accuracy of 95.2241 and FRR of 4.792331 on applying rotations of 30 and 45 degrees respectively as Zernike Moment is scale and rotation invariant. Also it has also been observed that Minutiae feature slightly exceeds in terms of FAR of 0.025335 over Zernike Moment with FAR of 0.093571 respectively.

Keywords
Offline Signature Verification and recognition techniques used ,feature extraction ,image processing.

1. INTRODUCTION
A Biometric system is a pattern recognition system which determines a user by assuring the legitimacy of a specific feature or behavioral characteristic possessed by the user. The signature verification has an advantage over other forms of biometric techniques like fingerprint, voice and iris recognition, heart sound etc. A Signature is a hand written depiction of someone’s name, nickname or any other identifying mark that proof his or her identity. It will have some intrapersonal variation even when it comes from a same person due to geographical factors, age, emotional state, illness or due to any other reason as well as interpersonal variation means differences between originals and forgeries. Forgeries are then further classified into three different categories namely Random, Simple and Skilled.

2. RELATED WORK
Large amount of work has been done in the field of signature verification using Zernike Moment and also Minutiae feature in fingerprints recognition. In this section we will discuss many approaches [1-15]. Srikanta pal et al. performed an off-line signature verification system involving Hindi signatures. The gradient and Zernike moment features were employed and Support Vector Machines (SVMs) were considered for verification. The Hindi signature database employed for experimentation consisted of 840(35x24) genuine signatures and 1050 (35x30) forgeries. An encouraging accuracy of 7.42% FRR and 4.28% FAR were obtained following experimentation when the gradient features were employed [1]. SriKanta Pal et al. used the signatures of English, Hindi and Bangla for identification. Zernike Moment and Histogram of gradient are employed as two different feature extraction techniques, Support Vector Machines (SVMs) are used as classifiers and a database of 2100 English 2100 Bangla and 2100 Hindi signatures are used for experimentation. Two different results based on two different feature sets are calculated and analyzed. The highest accuracy of 92.14% is obtained based on the gradient features using 4200 (1400 Bangla + 1400 English + 1400 Hindi) samples for training and 2100 (700 Bangla + 700 English + 700 Hindi) samples for testing. Different feature sets for offline signature identification were utilized, and encouraging results (92.14% and 91.23%) were obtained [2]. Srikanta Pal et al. proposed foreground and background based technique for identification
of scripts from bi-lingual (English/Roman and Chinese) off-line signatures. This system will identify whether a claimed signature belongs to the group of English signatures or Chinese signatures. The identification of signatures based on its script is a major contribution for multi-script signature verification. Two background information extraction techniques are used to produce the background components of the signature images. Gradient-based method was used to extract the features of the foreground as well as background components. Zernike Moment feature was also employed on signature samples. Support Vector Machine (SVM) is used as the classifier for signature identification in the proposed system. A database of 1120 (640 English+480 Chinese) signature samples were used for training and 560 (320 English+240 Chinese) signature samples were used for testing the proposed system. An encouraging identification accuracy of 97.70% was obtained using gradient feature from the experiment [3]. SriKanta Pal et al. investigated the performance of an off-line signature verification system involving Hindi signatures, whose style is distinct from Western scripts. The gradient feature, Zernike moment features and SVMs were considered for verification. To the best of the authors’ knowledge, Hindi signatures investigated as part of a large dataset have never been used for the task of signature verification, and this research work is only the second important report using Hindi signatures in this area. An encouraging accuracy of 90.69% was obtained using gradient feature. The Hindi signature database employed for experimentation consisted of 2400 (100 × 24) genuine signatures and 3000 (100 × 30) forgeries. The error rates of 11.50% FRR and 7.12% FAR were obtained through experimentation using gradient features [4]. Md. Iqbal Quraishi et al. proposed method which comprises spatial and frequency domain techniques for transformation. After extracting the Region of Interest Ripplet- II Transformation, Fractal Dimension and Log Polar Transformation are carried out to extract descriptors of the concerned signature to be verified as well as authenticated. In decision making stage Feed Forward Back Propagation Neural Network is used for verification and authentication purpose. This system has been tested with large sample of signatures to show its verification accuracy and the results have been found around 96.15%. Also forgery detection rate has been found 92% which is very encouraging. False Acceptance Rate and False Rejection rate of our system has been determined 5.28% and 2.56% respectively [5].

Shan Li et al. performed an analysis on the amount of visual information captured by ZM phase and the amount captured by ZM magnitude. They formed a new shape descriptor, known as invariant ZM descriptor (IZMD), followed by pre-normalization of image using geometrical moments for obtaining scale and translation invariance of IZMD. A phase correction method was performed while extracting IZMD features to make the phase invariant to rotation. This method outperforms the commonly used magnitude-only ZMD feature in terms of noise robustness and object discrimination [6]. G. Y. Chen et al. proposed a method of combining wavelet based de-noising enhancement technique with Zernike moment feature extraction in order to achieve improved classification rates. For this purpose they first segmented the unknown pattern image from the background then normalized the pattern to make it scale and translation invariant followed by de-noising using wavelet method and at last Zernike moment features are extracted for classification purpose. The average recognition rate of 98.17% with de-noising method was reported over average recognition rate of 97.26% without de-noising [7]. T. Shivanand et al. proposed a new method for the detection and recognition of object using image preprocessing and image enhancement techniques then connected component analysis procedure was performed followed by bounding box method to achieve rotation and scaling invariance. Each object is then described by Zernike moments. They had utilized modified SVM for utilizing decision tree for solving multiclass problems for recognition purposes. This algorithm performs the task of object detection and recognition even in the presence of shadows, partial occlusion and non-uniform illuminations at an efficient rate. The recognition rates of 95.31% were reported for partial occlusion [8]. N. Sridevi et al. performed a classification of handwritten ancient scripts in Tamil using ELM (Extreme Learning Machine) trained by Zernike moments and Regional features which is then compared with Probabilistic Neural Networks claiming that ELM gives highest accuracy rate of 95% taking less time for training and testing. The algorithm was applied for about 300 samples containing scripts belonging to four classes of ancient Tamil scripts [9]. Karbhari V. Kale et al. proposed simple and compound character recognition for Marathi derived Devanagari script using Zernike moment approach followed with classification and recognition using SVM and K-NN approach. They tested it on 27000 images for basic and compound characters and obtained 98.37% and 98.32% accuracy respectively. The overall recognition rate of proposed system using SVM and K-NN classifier is up to 98.37%, and 95.82% respectively [10]. Yang Zhanlong et al. proposed an automatic image mosaics technique by using the pseudo- Zernike moments defined on the feature point’s neighborhood. Firstly using the Harris corner detector gain the feature points, compute the pseudo Zernike moments defined on these feature point’s neighborhood, through comparing the Euclidean distance of these pseudo- Zernike moments to extract the initial feature points pair, then eliminate spurious feature points pair by geometric transform model obtained from RANSAC, finally transform the input image with the correct mapping model for image fusion and complete image stitching. Experimental results demonstrate that the proposed algorithm is robust to translation, rotation, noise and slight scaling [11].

Yin Li-qiang et al. proposed fingerprint feature extraction, using an algorithm for minutiae extraction based on tracing the thin ridge line, expressing the type of current point and the states of its 8-neighborhood pixels by 8-neighbor coding, and makes the further processing to the fingerprint minutiae extracted, namely, eliminating the false minutiae and retaining the real minutiae [12]. Sangita Bharkad et al. proposed the discrete wavelet packet transform based feature extraction method for fingerprint matching. The performance of proposed method is compared with the DWT, minutiae and Gabor filter based feature extraction method. The performance proposed method with reduced redundancy gives good GAR (Genuine Acceptance Rate) at low FAR (False Acceptance Ratio). The proposed method is computationally fast as compared to Gabor filter based feature extraction method. The length of the feature vector is reduced by a factor ~20 with the DWPT with reduced redundancy which improves the matching speed [13]. Bindu Garg et al. proposed a method involves combination of Gabor filter and Frequency domain filtering for enhancing the fingerprint. With eight different orientations of Gabor filter, features of the fingerprint extracting are combined. In Frequency domain filtering, the fingerprint image is subdivided into $32 \times 32$ small frames. Features are extracted from these frames in frequency domain. Final enhanced fingerprint is obtained with the
results of Gabor filter and frequency domain filtering. Binarization and Thinning follows next where the enhanced fingerprint is converted into binary and the ridges are thinned to one pixel width. This helps in extracting the Minutiae parts (ridge bifurcation and ridge endings). The overall recognition rate for the proposed method is 95% which is much better than histogram method where the recognition rate is 64% [14]. Roli Bansal et al. presented a review of a large number of techniques present in the literature for extracting fingerprint minutiae. The techniques are broadly classified as those working on binarized images and those that work on gray scale images directly. Further, more emphasis is to be laid on defining the local criteria, in order to establish the validity of a minutia point, which is particularly useful during fingerprint matching and adopting more sophisticated identification models, for instance extending minutiae definition by including trifurcations, islands, bridges, spurs etc. Also, the paper leads to the further study of the statistical theory of fingerprint minutiae. In particular approaches can be investigated to determine the number of degrees of freedom within a fingerprint population which will give a sound understanding of the statistical uniqueness of fingerprint minutiae [15].

3. PROCESS METHODOLOGY

There are three major steps used for signature verification and recognition and each of these steps consists of many methods that contribute to improved results. Following steps are:

a) **Data acquisition:** Paper based signature is first converted into a digital image by scanning and then it is used for verification purpose. In this implementation we have used a database of forty images.

b) **Preprocessing of image:** It is the most important step in signature verification and recognition system that is performed for the manipulation and modification of images. Its successful implementation produces improved results and higher accuracy rates.

Different levels of processing are:

1. **Binarization:** It converts an image of up to 256 gray levels to a black and white image Threshold method is used to extract the signature from the background of a signature. All pixels of signature are converted to “1” and rest of pixels those are belongs to background of signature convert to “0”.

2. **Image enhancement:** Prior doing image enhancement a gray scale conversion has been done. This step is performed to enhance image quality. For this purpose three different techniques have been performed namely Power Law Transformation, Ripplet II Transformation and Fractal Dimension.

a) **Power Law Transformation:** It includes nth power and nth root transformation. These transformations can be given by the expression:

\[ s = cv^\gamma \]

This symbol \( \gamma \) is called gamma, because of this it is also known as gamma transformation. Variation in the value of \( \gamma \) varies the enhancement of the images. Different display devices / monitors have their own gamma correction, that’s why they display their image at different intensity. Here the value of Gamma has been taken as 1.

b) **Ripplet II Transformation:** Currently there is a very limited scope for representing 2D singularities that can be addressed more efficiently on using curvelet and ridgelet when compared with wavelet transform. Thus, to enhance the performance of 2D singularities Ripplet II has been carried out for efficient representation of texture and edges. The latent qualities like image de-noising, image restoration and image compression are preserved by ripplet transform. For this purpose Ripplet II function must be defined. If \( \phi \) is a univariate wavelet function then function \( \phi: R \rightarrow R \) and \( \int \phi(t) dt = 0 \), then bivariate function would be \( \Psi_{x,y,x,\theta}: R^2 \rightarrow R^2 \), in the polar coordinate system

\[ \Psi_{x,y,x,\theta}(\rho, \Phi) = x^{-1/2}\rho \cos((\theta - \Phi)/\gamma - \gamma/\rho) \]

Where \( x > 0 \) signifies scale, \( y \in \mathbb{R} \) signifies translation, \( x \in \mathbb{R} \) signifies degree, and \( \theta \in [0, 2\pi) \) signifies orientation. Function \( \Psi_{x,y,x,\theta}(\rho, \Phi) \) is called ripplet-II function. Here, we have taken \( z > 0 \) (i.e. positive curves), as positive curves are only considered for their open curve nature. Applying ripplet-II transform standard deviation and mean have been calculated from transformation values.

![The enhanced image after Ripplet II Transformation](image)

3c) **Fractal Dimension:** Fractal can be addressed as a scale invariant irregular shape of geometric object that comprises of an infinite nesting or we can say that it is a curve or regular figure that’s every part has as a whole invariant statistical characteristics. Fractal dimension (D) is explained as below. If the linear size of the boxes \( s_{id} = 1/N \). \( N_{box}(L) \) be the number of boxes of size \( L \). Then

\[ D = \lim_{N \to \infty} \frac{\log N_{box}(1/N)}{\log N} = \lim_{L \to 0} \frac{\log N_{box}(L)}{\log (1/L)} \]

Also we can state that \( N_{box}(L) \) obeys Power Law, as above equation can be written as

\[ N_{box}(L) \sim 1/L^D \]
Fig 2 The enhanced image after Fractal Dimension Transformation

3. **Thinning:** Thinning removes the thickness differences at each image pixel that can occur because of different pens. Several researchers have conducted thinning process to improve the accuracy rate.

c) **Feature Extraction:** Feature extraction techniques play vital role to improve the accuracy of signature verification system. This process identifies and differentiates an individual signature from another. It can be achieved by employing different type features such as global features, geometric features, texture features. The features which we have extracted in our proposal are namely Zernike Moment and Minutiae. These features are based on the shape and dimension of a signature image.

1. **Zernike Moment:** Zernike polynomials are an orthogonal set of complex valued polynomials. These are scaling and orientation invariant. It can be described as:

   \[ V_{nm}(x, y) = R_{nm}(x, y) \exp \left( j m \ \tan^{-1} \left( \frac{y}{x} \right) \right) \]

   Where,

   \[ x^2 + y^2 \leq 1, j = \sqrt{-1}, n \geq 0, |m| \leq n \]

   And \( n - |m| \) is even and Radial polynomials \( \{ R_{nm} \} \) are defined as:

   \[ R_{nm}(x, y) = \sum_{s=0}^{n-|m|} B_{nm}^{s} (x^2 + y^2)^{n-2s} \]

   Where,

   \[ B_{nm}^{s} = \frac{(-1)^{s}(S-1)!}{S! \left( \frac{n + |m|}{2} - S \right) \left( \frac{n - |m|}{2} - S \right)!} \]

   The complex Zernike moments of order \( n \) and repetition \( m \) are given by:

   \[ A_{nm} = \frac{n + 1}{n} \sum_{x} \sum_{y} f(x, y) V_{nm}^{*}(x, y) \]

   Where \( x^2 + y^2 \leq 1 \) and symbol * denotes the complex conjugate operator.

   The Zernike moments can be computed by the scale invariant Central moments as follows:

   \[ A_{nm} = \sum_{k, n-m|/n-\text{even}} \sum_{a, d} b(a) B_{nm}^{a} G_{k-2a, d} \]

Where

\[ b = \frac{n - |m|}{2} - S \text{ and } j = \sqrt{-1} \]

1. **Minutiae feature:** From the binary thinned image, the minutiae are detected by using 3x3 pattern masks. Samples of masks used for identifying the ridge ending and bifurcations point are shown in Fig 4 and Fig 5. Although the process seems to be simple, it is necessary to consider the elimination of false detected minutiae.

   ![Fig 4 Masks for bifurcation detection](image)

   ![Fig 5 Masks for termination detection](image)

Now as the minutiae is successfully extracted they are now stored in a template containing the minutiae position(x, y), minutiae direction (angle), minutiae type (bifurcation or termination). During the enrollment process extracted templates that are stored in the database will be used in the matching process as a reference template or database template. During recognition process the extracted minutiae are also stored in a template and they are used as a query template during the matching process. There are certain techniques like Crossing Number (CN) and Morphological based which are used for minutiae extraction. In our proposal we have used CN method as it is widely used for its computational efficiency and inherent simplicity. The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3x3 window as shown in figure below.
Fig 6 shows the local neighborhood of each pixel

The CN value is then computed as follows:

\[ \text{CN} = 0.5 \sum_{i=1}^{n} |P_i - P_{i+1}| \]

It is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood. Table 1 shows the Properties of Crossing Number.

<table>
<thead>
<tr>
<th>CN</th>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Isolated Point</td>
</tr>
<tr>
<td>1</td>
<td>Ridge Ending Point</td>
</tr>
<tr>
<td>2</td>
<td>Continuing Ridge point</td>
</tr>
<tr>
<td>3</td>
<td>Bifurcation Point</td>
</tr>
<tr>
<td>4</td>
<td>Crossing Point</td>
</tr>
</tbody>
</table>

Table 1 Properties of Crossing Number

False minutiae may be introduced into the image due to factors such as noisy images, and image artifacts created by the thinning process. Hence, after the minutiae are extracted, it is necessary to employ a post processing stage in order to validate the minutiae.

- **Procedure to remove false minutiae**
  
  We have employed an algorithm that incorporates the validation of different types of minutiae. It tests the validity of each minutiae point by scanning the skeleton image and examining the local neighborhood around the minutiae. The algorithm is then able to cancel out false minutiae based on the configuration of the ridge pixels connected to the minutiae point. The preprocessing is done which includes the vertical oriented image followed by the core point detection and region of interest selection. Then feature extraction is done in the extracted region of interest image and then a multilayer perceptron network of three layers is trained to extract the minutiae from the thinned image.

Then the extracted features are fed into a Neural Network Classifier which computes the performance metrics.

**4. RESULT AND ANALYSIS**

In this section we compare and analyze the performance of two extracted features on calculating Accuracy, FAR, FRR.

Table 2 Average values of Zernike Moment feature

<table>
<thead>
<tr>
<th></th>
<th>Average values of all parameters for Zernike Moment feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>FAR</td>
</tr>
<tr>
<td>at 30</td>
<td>at 45</td>
</tr>
<tr>
<td>95.4102</td>
<td>95.559612</td>
</tr>
</tbody>
</table>

Fig 8 The comparison of Accuracy metrics for Zernike Moment at 30 degrees and 45 degrees.

Fig 9 The comparison of FAR metrics for Zernike Moment at 30 degrees and 45 degrees.

Fig 10 The comparison of FRR metrics for Zernike Moment at 30 degrees and 45 degrees.
Table 3 Average values of Minutiae feature

| Average values of all parameters for Minutiae feature |
|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| Accuracy at 30  | Accuracy at 45  | FAR at 30       | FAR at 45       | FAR AT 30       | FAR AT 45       |
| 94.60008        | 95.2241         | 0.025335        | 0.033690339     | 5.3246835       | 4.792331       |

It is evident that on increasing the orientation the value of accuracy metrics increases and at the same time the value of FAR metrics decreases in cases of both features thereby addressing the improvement in signature recognition rate but there is a slight improvement in FAR also.

5. CONCLUSION

The proposed method to authenticate offline signature verification using concepts of preprocessing including binarization, thinning and image enhancement techniques like Power law Transformation, Ripplet II and Fractal Dimension followed by feature extraction yields the average accuracy rate of 95.5596115 and 95.2241 for Zernike Moment and Minutiae feature respectively. FRR of 4.336188 and 4.792331 has also been observed for Zernike Moment and Minutiae feature respectively which proves that Zernike Moment feature is showing more encouraging performance over Minutiae feature which makes it best suited for signature recognition.

6. REFERENCES


