Offline Signature Verification System using a Set of Simple Shape Based Geometric Features

AMIT KISHORE SHUKLA
COMPUTER SCIENCE DEPARTMENT
MNNIT ALLAHABAD, INDIA

SHREYAS SINGH
COMPUTER SCIENCE DEPARTMENT
MNNIT ALLAHABAD, INDIA

***Abstract*— Signature is mostly used as a means of personal verification focused the need for an automatic verification system. Verification can be categorized either Offline or Online it depends on the application which is used. Online systems uses information which are dynamic in nature information are captured at the time the signature is performed. Offline systems work on the scanned image of a signature. In this paper we present a prototype for the Offline Verification of signatures using a set of simple shape based geometric features. The features that are used in this paper are The Baseline Slant Angle Of The Signature Sample, The Aspect Ratio Of The Signature Sample, The Normalized Area Of The Signature Sample, The Center of Gravity Of The Signature Sample and The Slope Of The Line Joining The Center Of Gravity Of The Vertical Splitting Of The Signature Sample . Before extracting the features of signature we have to perform, the preprocessing of a scanned image because we have to remove any spurious noise present in the signature sample. The system is initially trained using a database of signatures obtained from those individuals whose signatures have to be authenticated by the system. For every object a mean signature is obtained by integrating the above said features which are derived from a set of sample of genuine signatures. This mean signature acts as the template for verification against a claimed test signature. Euclidian distance which is in the feature space between the claimed signature and the template serves as a measure of similarity between the two. If this distance is less than a predefined threshold & the test signature is verified to be that of the claimed subject else detected as a forgery**

Keywords— Offline Signature Verification, Forgery, Feature Extraction, FAR, FRR.

I. INTRODUCTION

Signature has been a distinguishing feature for person identification throughout ages. Even today a large number of transactions, particularly financial ones, are being authorized via signatures, therefore methods which are used for automatic signature verification needs to be developed whenever authenticity requires to be verified. There are two approaches of signature verification which are categorized according to the acquisition of the data: It can be On-line or Off-line. In case of On-line the data records the motion of the stylus while the signature is being produced, and it includes location, preferable velocity, pen pressure and the acceleration taken as a function of time. Systems which are online use this information which is captured during the acquisition process. These dynamic characteristics are specific to each individual and sufficiently stable as well as repetitive in nature. The data that are Off-line is represented as a 2-D image of the signature. Processing Off-line data is complex because of the absence of stable characteristics which are not found in dynamic characteristics. Problem also lies in the fact that it is very hard to segment signature strokes because of highly stylish and unconventional writing styles. Also the non-repetitive nature of variation of the signatures, due to age, illness, geographic location and perhaps to some extent the emotional state of the person, makes hard to achieve the purpose. All these coupled together cause large intra-personal variation. A strong and reliable system has to be designed which should not only be able to tackle these factors but should also detect various types of forgeries [3]. The system should not be too sensitive and not too loose. There should exist an acceptable trade-off between a low False Acceptance Rate (FAR) and a low False Rejection Rate (FRR).

We tackle the problem in two steps. Firstly the scanned copy of signature is preprocessed which is required for suitably extracting features. After that the preprocessed image is used to extract related and relevant geometric parameters that can distinguish signatures of different persons. Section II deals with the steps required during preprocessing and Section III explains the features that are extracted. Section IV contains procedure for the verification. A detail of implementation and simulation results are written in Section V. Section VI contains the conclusion.

II. Pre-processing

The scanned copy of the signature image may contain false noise and that is supposed to be removed in order to avoid errors in the further processing steps. The gray image I_o of size M*N is inverted to obtain an image I_i in which the signature part which consist of higher gray levels forms the foreground.

$$I_i(i,j)=I_{o,max}-I_o(i,j) \qquad \ldots(1)$$

Where Io,max is the maximum grey-level.

The background, which should be preferably dark, may comprise of pixels or group of pixels with gray values between background and foreground. These can be removed by doing a row averaging process which generate the averaged (row) image I_{ra}, which is given by,

$$I_r(i,j) = I_i(i,j) - \sum_{l=1}^{M} I_i(l,j)/M$$

$$I_{ra}(i,j) = \begin{cases} I_r(i,j) & \text{if } I_r(i,j) > 0 \\ 0 & \text{otherwise} \end{cases} \qquad \ldots(2)$$

More noise removal and greater smoothening is achieved by using an n*n averaging filter which generates a cleaned image I_a.

$$I_a(i,j)=1/9\left(\sum_{l=i-1}^{i+1}\sum_{k=j-1}^{j+} I_{ra}(l,k)\right) \quad \text{…(3)}$$

The gray image is converted into binary image by threshold decomposition, hence isolating the foreground which consists of the signature from the background of the image. This binary image is again used in the future for feature extraction. Most of the thresholding techniques which are based on histogram work on the assumption that foreground area is comparable to that of background area. Usually in a signature image the mode of foreground is much less compared to that of the background. Therefore in order to make foreground mode comparable to that of the background, attenuation of the background mode is performed on the histogram H of the cleaned image I_a. To perform this Global mode Gm and the Foreground mode Fm are determined.

G_m = Max Hi, i in the dynamic range.
F_m = Max Hi, i in the upper half of the dynamic range.

An empirically determined factor γ (<=1.0) is used to attenuate the lower half of the range between the start of the histogram and the foreground mode. Thresholding is performed on this background attenuated image I_{ba} using Discriminate Analysis method as suggested in [1]. Here the image pixels are divided into two classes:

- Background Class with gray levels between 0 and t.
- Object Class with gray levels between t+1 and G-1, on a gray scale of 0 to G-1.

The probability of occurrence of a particular gray level g is given by

$$p_g = H_g/T \text{ where } T = \sum_{i=0}^{G-1} H_i \quad \text{… (4)}$$

The optimum threshold is that value of t that maximizes the between-class- variance.

$$\sigma_B^2(g) = \omega_1(\mu_o)^2 + \omega_1(\mu_1)^2$$
$$\omega_0 = \sum_{i=0}^{t} p_i$$
$$\omega_1 = 1- \omega_0$$
$$\mu_T = \sum_{i=0}^{G-1}(i^* p_i)$$
$$\mu_o = \sum_{i=0}^{t}(i^* p_i)$$
$$\mu_1 = \mu_T - \mu_o \quad \text{… (5)}$$

Using the threshold t we obtain a binary image I_T with signature pixels made to 1.

III. FEATURE EXTRACTION

In the feature extraction we use a set of five features to define & characterize a candidate signature. These features are defined as the geometrical features based on the shape and dimensions of a signature sample. The various shape based are described are shown below:

1. The Baseline Slant Angle of the Signature Sample

Baseline is the imaginary line about which the signature is assumed to rest. The angle of inclination of this line to the horizontal is called the Slant Angle Θ. To determine the slant angle the ratio of the maximum horizontal projection to the width of the projection is maximized over a range of values of angle of rotation θ.

$$P_H(i) = \sum_{j=0}^{N-1} I_T(i,j)$$
$$\rho(\theta) = H(\theta)/W(\theta) \qquad -\theta_1<\theta<\theta_2$$
$$H(\theta) = \text{Max } P_H(i)$$
$$W(\theta) = \text{number of non-zero elements in } P_H(i) \quad \text{…(6)}$$

Θ is the value of θ at which $\rho(\theta)$ attains maximum. The ratio $\rho(\theta)$ is smaller at every angle other than the baseline slant angle. The threshold image I_T is rotated by this angle to obtain the slant normalized signature image I_R. The rotated image I_R contains a lot of blank spaces, which are removed using area close operation [5] that involves dilation followed by erosion.

2. The Aspect Ratio of the Signature Sample

The aspect ratio (A) is defined as the ratio of width to height of the signature. The coordinates of the bounding box of the signature are determined and the width (D_x) and height (D_y) are computed with the help of these coordinates.

$$A. \; A = D_x/D_y \quad \text{...(7)}$$

3. The Normalized area of the signature sample

Normalized area (NA) is the ratio of the area occupied by signature pixels to the area of the bounding box.

$$N_A = \Delta/(D_xD_y) \quad \text{…(8)}$$
Where Δ is the area of signature pixels.

4. The Center of Gravity of the Signature Sample

The Center of Gravity is the 2-tuple (X,Y) given by,

$$X = \sum_{j=0}^{N-1} P_V(j)^*j/\Delta$$
$$Y = \sum_{i=0}^{M-1} P_H(i)^*i/\Delta \quad \text{...(9)}$$

Where P_V and P_H are the vertical and horizontal projections respectively.

5. *The Slope of the line joining the Centers of Gravity of the vertical splitting of the signature sample*

We divide the signature sample within its bounding box into left and right halves and separately to calculate the center of gravity of the two halves to distinguish signature samples.

IV. VERIFICATION

The above described features are extracted from a sample group of signature images of different persons. The values derived from each sample group are used in deriving a mean signature for each subject. The mean values and standard deviations of all the features are computed and used for final verification. Let μ_i and σ_i denote the mean and standard deviation for the i^{th} feature and F_i denote its value for the query image. The Euclidian distance δ in the feature space measures the proximity of a query signature image to the mean signature image of the claimed person.

$$\delta = (1/n) \sum_{i=1}^{n} [(F_i - \mu_i)/\sigma_i]^2 \qquad \ldots(10)$$

If this distance is below a certain threshold then the query signature is verified to be that of the claimed person otherwise it is detected as a forged one.

V. IMPLEMENTATION DETAILS AND SIMULATION RESULTS

A database of about 140 signatures with 7 signatures per person was used for training stage. The signatures were scanned with a precision of 300 dpi. It was found experimentally that a value of 0.85 for γ gave good results. Here, we used a threshold value of 1.5 for the distance δ. The training images for a subject are shown in Fig.1. For a sample signature image shown in Fig. 2, the threshold image is shown in Fig. 3. Fig.4 shows the baseline rotated image and the image obtained after elimination of spurious noise is shown in Fig. 5. Also a signature of the same subject signed by a different person, shown in Fig. 6, was detected as forged. The results of our simulation for forged and genuine signatures are as shown in the table below.

TABLE 1

Nature of Signature	No. of Samples	False Acceptance Rate	False Rejection Rate
Original	80	-----	8.90%
Forged	55	23.33%	------

VI. Conclusions and Scope for Future Work

This algorithm uses simple geometric features to distinguish the signatures of different persons. The system is defined as robust and can detect the random, simple and semi-skilled forgeries but the performance deteriorates in case of skilled forgeries. A larger database can minimize false acceptances as well as false rejections performed by the different samples of the signatures of the different persons. With the help of highly dimensional feature space & dynamic information collecting at the time of signature can also improve the performance level of the system. The concepts of Neural Networks as well as Wavelet transforms will define a high accuracy in the verification of the signature samples.

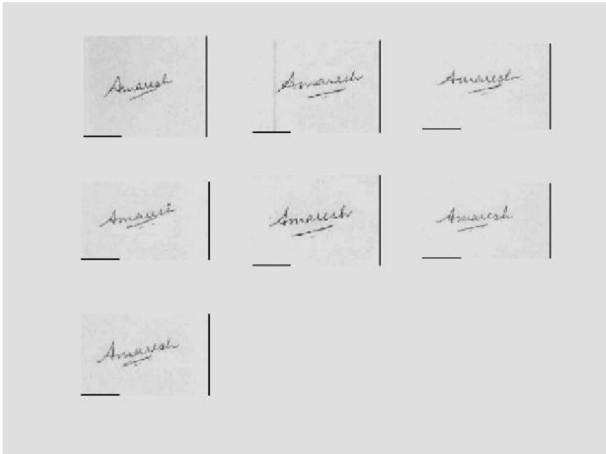

Fig. 1 Training Images

Fig. 2 Original Image

Fig. 3 Threshold Image

Fig. 4 Baseline Rotated Image

Fig. 5 Cleaned Image

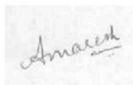

FIG. 6 A FAKE SIGNATURE DETECTED AS FORGED

REFERENCES

[1] Ostu N., 'A Threshold Selection Method from Gray Level Histogram, Man and Cybernetic, SPC-8, 1978 pp. 62-69.

[2]. Gonzalez R.C., Woods E., 'Digital Image Processing', Addison-Wesley, 1993

[3]. Larkins and Mayo, Adaptive Feature Thresholding for offline signature verification, 23rd International Conference In Image and Vision Computing New Zealand (2008), pp. 1-6.

[4]. Coetzer, Herbst and Preezp , Offline Signature Verification Using the Discrete Radon Transform and a Hidden Mar Model,EURASIP Journal on Applied Signal Processing 2004.

[5]. Almudena, Fernandez, Pecharroman and Fierrez , Off-line signature verification ystem based on contour features, 11th International Conference on Frontiers in Handwriting Recognition,2008.

[6]. Debasish, Banshidhar and Jena, Improved Offline Signature Verification Scheme Using Feature Point Extraction, 7th IEEE International Conference on Digital Object Identifier .

[7]. Hanmandlu, Mohd. Hafizuddin, Vamsi, Offline Signature Verification and forgery detection using fuzzy modeling, Pattern Recognition, Volume 38, March 2005, Pages 341-356.

[8]. Piyush and Rajagopalan, Offline signature verification using DTW,Pattern Recognition Letters, Volume 28, 1 Sep. 2007.

[9]. Bradley, Serestina, An off-line signature verification system, Signal and mage Processing Applications (ICSIPA), 2009.

[10]. Prakash and Guru, Geometric Centroids and their Relative Distances for off-line Signature Verification, 10th International Conference on Digital Object Identifier: 2009, Page(s): 121 125.

[11]. Yu Qiao, Jianzhuang Liu and Xiaoou Tang, Offline signature verification using online handwriting registration, Computer Vision and Pattern Recognition, 2007. IEEE Conference on Digital Object Identifier, 2007, Page(s): 1 - 8.

[12]. Weiping HOU, Xiufen Ye and Kejun Wang, A Survey of Off-line Signature Verification , Intelligent Mechatronics and

[13]. Automation,International Conference on Digital Object Identifier, 2004.

[14]. Bence Kovari, Istvan Albert and Hassan Charaf, Current Challenges in Off-line Signature Verification.

[15]. Daramola Samuel and Ibiyemi Samuel, Novel Feature Extraction Technique for Off-Line Signature Verification System ,International Journal of Engineering Science and Technology Vol.2(7), 2010.

[16]. Jose F. Velez, Angel Sanchez and A. Moreno, Robust Off-line Signature Verification Using Compression Networks and Positional Cuttings, Neural Networks for Signal Processing, 2003. IEEE 13thWorkshop on Digital Object Identifier, Page(s): 627 636.

[17]. Ibrahim S. I. ABUHAIBA, ”Offline Signature Verification Using

[18]. Graph Matching”, Turk J Elec Engin, VOL.15, NO.1 2007.

[19]. E. J. R. Justino, , Of-line signature verification using HMM for random, simple and skilled forgeriesin International Conference on Document Analysis and Recognition, vol. 1, pp. 105110.

[20]. Vu Nguyen; Blumenstein, M.; Muthukkumarasamy V.; Leedham G., Offline Signature Verification Using Enhanced Modified Direction Features in Conjunction with Neural Classifiers and Support Vector Machines, in Proc. 9th Int Conf on document analysis and recognition, vol. 02, pp. 734-738, Sep 2007.

[21] www2.engr.arizona.edu/~pgsangam