INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

HANDWRITTEN SIGNATURE VERIFICATION SYSTEM USING GEOMETRIC FEATURES

Dinesh Kumar Maurya[1], Lavi Tyagi[2]

[1,2] Department of Computer Science & Engineering
Monad University, Hapur (U.P.) India
erdinesh23@gmail.com, lavityagi15march@gmail.com

Abstract: *Signature verification has been a topic of interest for many years in the area of document authentication. This paper proposes a new technique to the problem of off-line signature verification and forgery detection. Off-line signature verification system work on the scanned image of a signature. In this paper, we present a new method for off-line verification of signatures using a set of geometric centres of the features. The feature that is used is the geometric centre of different parts of a signature image. Before signature is to be verified, pre-processing of a scanned image is required to isolate the signature part and to remove any noise present in the signature image. The system is initially trained using a database of signatures obtained from those persons whose signatures have to be verified by the system. For each person a mean signature is obtained integrating the above feature taken from a set of his genuine sample signatures. This mean signature acts as the reference for verification against a claimed test signature. Euclidian distance in the feature space between the claimed signature and the reference serves as a measure of similarity between the both signatures. If this difference is less than a pre-defined threshold, the test signature is verified to be that of the claimed person else detected as a forgery.*

Keywords: *Off-line, Authentication, Euclidian distance, Geometric center, Pre-processing, Threshold.*

1. INTRODUCTION

Handwritten signature is one of the most widely accepted personal attributes for identity verification. Signature verification is a research area that is to be used to create reliable off-line machines, which can verify or identify human signatures. Handwritten signature verification has been studied in last few decades. The various practical application domain included bank cheques authentication, credit card validation, security systems etc.

The signature verification system is categorizes into two main areas: Off-line signature verification and On-line signature verification. In Off-line signature verification, signature samples are scanned into image representation while in On-line signature verification, signature samples are collected from a digitizing tablet capable of recording pen movements during writing.

The process for offline signature verification can be divided into two stages: (i) Feature Extraction and (ii) Verification. In the feature extraction, some static features of the signature are extracted and in the verification, the authenticity of the unknown specimen is decided by comparing its features against those of the reference samples. Feature extraction is the process to extract various image features for identifying or interpreting meaningful physical objects from images. It is an area of image processing which are used to detect and isolate various desired portions of a signature image.

The various terms used for measuring accuracy are False Rejection Rate (FRR) which shows the percent of genuine signatures that were considered as a forgery, and False Acceptance Rate (FAR) which is the proportion of incorrectly accepted forgeries.

2. RELATED WORK

A lot of research has been conducted in handwriting signature verification and pattern recognition for a number of years. In the area of off-line handwritten signature verification, various methods have been used. In this section we review some of the recent papers on off-line handwritten signature verification. The techniques used by different researchers differ in the type of the training method adopted, image features extracted, the classification and verification model used. The categorization for these approaches done here is influenced by classification used in [1].

B.S Pawar [2] proposed an off-line signature verification system which is based on image processing and some global features using artificial neural network.

Ranjan Jana et al. [3] presented a technique which is used to extract features from signature image and classify the signature using Euclidian distance measurement. The experimental results provide a solution with FRR and FAR 2.86% and 17.1% respectively.

Javier Ruiz-del-Solar et al [4] proposed approach local interest points are detected in the signature images, then local descriptors are computed in the neighbourhood of these points, and then these descriptors are compared using local and global matching procedures. The final verification is performed using a Bayes classifier. The proposed algorithm is verified using the GPDS signature database, where it achieves a FRR of 16.4% and a FAR of 14.2%.

3. PROPSED SCHEME

3.1 Signature Acquisition

The handwritten signatures were captured at 300 dpi in 8-bit gray scale and stored in Portable Network Graphics (PNG)

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

format as shown in Fig. 1. The signature image can be taken from documents by means of scanning devices. This method can be applied to gather image from the different available sources in the form of signed forms because the signing on a paper is still the most common method for signature authentication.

A. Signature Database

I have taken "Grupo de Procesado Digital de Senales" (GPDS) signature database [5] to perform my experiments. In the GPDS database, there are 39 sets of signature (i.e. signatures of 39 persons). Each set have 24 genuine signature and 30 skilled forgery signature. Thus results provided in this research used a total of 2106 signatures.

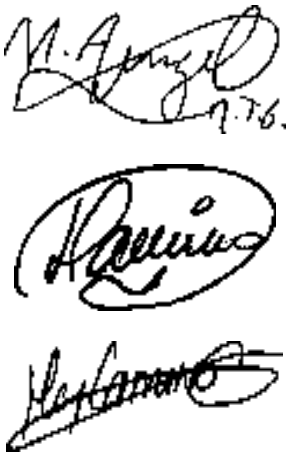

Figure 1: Examples of signature bitmaps

3.2 Pre-processing

Before a signature can be compared to any other signature, it undergoes some pre-processing operations. The pre-processing is performed in following four different stages: digitization image, width normalization, noise reduction and image thinning.

A. Digitization

Digitization is a process of converting signature image into binary image. For digitization, signatures are taken on white papers and acquired as binary images. The scanner scans the image that may be saved as a bitmap file. Further processing may be carried on the bitmap image [18].

B. Normalization

A writer may use an arbitrary baseline when writing the signature. We normalize the positional information of signature by computing an angle of θ corrective rotation about the geometric centre (x, y) such that rotating the signature by θ brings it back to a uniform baseline. We calculate θ by maximizing the deviation of the data, one direction, e.g. the x direction. The image size is to be changed so that the height reaches a default value while the height-to-width ratio remains unchanged. The size normalization in off-line signature verification is necessary to establish a common ground for signature image comparison. A low spatial resolution makes all signatures look like the same while a very high spatial resolution may highlighted the variability [6] [7].

C. Noise Removal

Dust on scanner or camera lens, may imperfections in the image resolution, etc introduces noises in the captured signature images. A filtering method is used to minimise the noises in the signature image. A noise reduction filter is applied to the binary scanned image. The goal is to eliminate single white pixels on black background and single black pixels on white back ground. We apply a 3 x 3 mask to the signature image with the following decision rule:

If the number of the 8-neighbors of a pixel that have the same colour with the central pixel is less than two, we reverse the colour of the central pixel [8][6].

D. Thinning

Thinning is a process that is used to remove selected foreground pixels from binary image. It is used in many applications, but is particularly useful for skeletonization. It is basically used to align the output of edge detectors by reducing all lines to single pixel thickness. It is mostly applied to binary image, and produces another binary image as output.

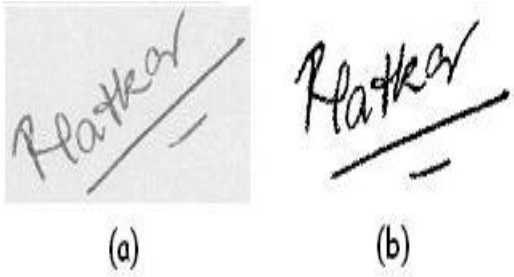

Figure 2: Pre-processing: (a) original (b) final.

3.3 Feature Extraction

The geometric features considered in my proposed plan are based on three sets of points in two-dimensional plane. Two sets having six feature points and one set having four feature points, which represent the distribution of signature pixels in image. These sixteen feature points are calculated by the following expression which is described in Geometric Centre [9]. Vertical Splitting, Horizontal Splitting and Diagonal Splitting are three steps to find out all these sixteen feature points. Before extracting these feature points we have to do some adjustments to the signature image. First, we move the signature image to the centre of the image window.

Geometric centre are calculated using the formulas given below:

$$Center_x = \frac{\sum_{x=1}^{x_{max}} x \sum_{y=1}^{y_{max}} b\,[x]\,[y]}{\sum_{x=1}^{x_{max}} \sum_{y=1}^{y_{max}} b\,[x]\,[y]} \quad \ldots\ldots (1)$$

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

$$Center_y = \frac{\sum_{y=1}^{y_{max}} y \sum_{x=1}^{x_{max}} b[x][y]}{\sum_{x=1}^{x_{max}} \sum_{y=1}^{y_{max}} b[x][y]} \quad \ldots\ldots (2)$$

A. Moving signature image to the centre of image window

In this step signatures image are moving to the centre of image window. Because of this we can reduce intra-personal variations. Here first we have to find out the geometric centre of the image signature and move the signature pixels such that the geometric centre should reside at centre of image window. Fig. 3(a) and 3(b) shows the signature images before moving and after moving signature to the centre of image window respectively.

Figure 3(a): Before moving signature to the centre of image

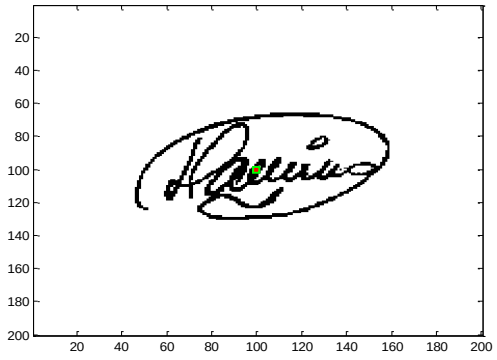

Figure 3(b): After moving signature to the centre of image

B. Horizontal splitting

Six feature points will be finding out by horizontal splitting. Here feature points are nothing but geometric centres. The steps for finding feature points by horizontal splitting are as follows: First we divide the image with horizontal line passing through the centre of image then we will get upper and lower parts of image. Find geometric centres h1 and h2 for upper part and lower part respectively. Then divide upper part with vertical line passing through the h1 and find out geometric centres h3 and h4 for left part and right part of upper part respectively. Similarly divide lower part with vertical line passing through the h2 and find out geometric centres h5 and h6 for left part and right part of lower part respectively.

Fig. 4 shows the feature points (h1, h2,..… h6) retrieved from signature image. These six feature points we have to find out for all signature images in both registration phase and verification phase.

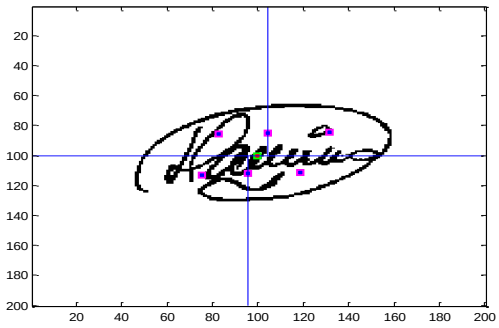

Figure 4: Feature points based on horizontal splitting

C. Vertical splitting

Six feature points will be finding out by vertical splitting. Here feature points are nothing but geometric centres. The steps for finding feature points by vertical splitting are as follows:

First we divide the image with vertical line passing through the centre of image then we will get left part and right part of image. Find geometric centres v1 and v2 for left part and right part respectively. Then divide left part with horizontal line passing through the v1 and find out geometric centres v3 and v4 for upper part and lower part of left part respectively. Similarly divide right part with horizontal line passing through the v2 and find out geometric centres v5 and v6 for upper part and lower part of right part respectively.

Fig. 5 shows the feature points (v1, v2,……v6) retrieved from signature image. These six feature points we have to calculate for all signatures image in both registration phase and verification phase.

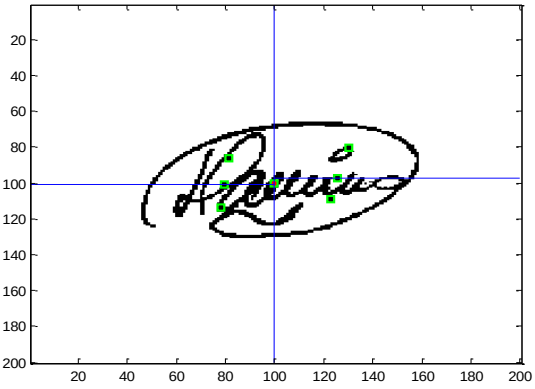

Figure 5: Feature points based on vertical splitting

D. Diagonal splitting

Four feature points will be finding out by diagonal splitting. Here feature points are nothing but geometric centres. The steps for finding feature points by diagonal splitting are as follows: First we divide image with diagonal line (lower left corner to upper right corner) at the centre of image then we will get left upper part and right lower part of image. Find out geometric centres d1 and d2 for left upper part and right lower part respectively. Similarly divide image with diagonal line (upper left corner to lower right corner) at the centre of image

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

then we will get left lower part and right upper part of image. Find out geometric centres d3 and d4 for left lower part and right upper part respectively.

Fig.6 shows the feature points (d1, d2,…….d4) retrieved from signature image. These four feature points we have to calculate for all signatures image in both registration phase and verification phase.

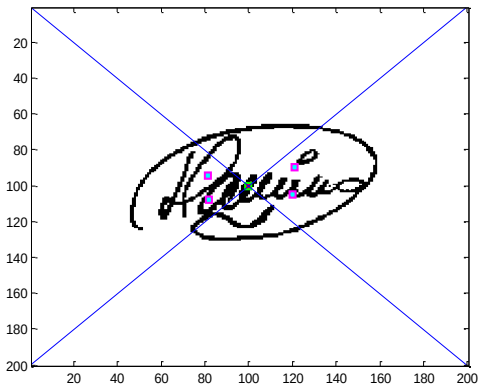

Figure 6: Feature points based on diagonal splitting

Now total sixteen feature points (v1, v2…….v6; h1, h2…….h6; d1, d2……..d4) are calculated by horizontal, vertical and diagonal splitting.

3.4 Classification

Since in my proposed work the signature image features are based on geometric properties. Therefore we can use Euclidean distance model for classification. Euclidean distance is the simple distance between a pair of vectors of any size. Here vectors are nothing but feature points. Now we will describe how to calculate distance using Euclidean distance model. These distances are useful in threshold calculation.

A. Euclidean distance model

A method for finding the similarity or differences between two signatures in feature space is essential for classification. Let A(x1, x2,,……..…xn) and B(y1, y2……..yn) are two vectors of size n. We can calculate distance (d) by using equation:

$$distance\ (d) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \quad \ldots\ldots (3)$$

In our application, vectors are points on plane. So d is the simple distance on a plane between two points.

3.5 Threshold selection

Since nobody can make same signature every time, there may be some deviation from one another, therefore a threshold value must be calculated for each user, which is maximum allowable deviation. If the difference is less than threshold value then signature will be classified as guanine signature and if the difference is greater than threshold value then signature will be classified as forgery signature. Here we calculate individual threshold value for horizontal, vertical and diagonal splitting.

Consider n is the number of reference (or registered) signatures and x1, x2, …, xn are corresponding sigle feature points of reference signatures (taking one corresponding feature point from each signature). Let xmedian is the median of n features from n signatures and D1, D2,…..,Dn are distances defined here:

$$D_1 = distance(x_{median}, x_1)$$

$$D_2 = distance(x_{median}, x_2) \quad \ldots\ldots (4)$$

$$\ldots\ldots$$

$$D_n = distance(x_{median}, x_n)$$

Now we use two main parameters for threshold calculation one is average distance (d_{avg}) and other standard deviation (σ). Equations 5 and 6 represent the calculation of these two above parameters.

$$d_{avg} = \frac{(D_1 + D_2 + \ldots\ldots + D_n)}{n} \quad \ldots\ldots (5)$$

$$\sigma = SD(D_1, D_2, \ldots\ldots, D_n) \quad \ldots\ldots (6)$$

Like this total six different feature points are there for both horizontal and vertical splitting while four different feature points are there for diagonal splitting based on average distance (davg) and standard deviation (σ).

Equation 7 represents the formula for threshold calculation for horizontal and vertical splitting and equation 8 shows for diagonal splitting.

$$threshold\ (t) = \sqrt{\sum_{i=1}^{6} (d_{avg}, i + \sigma_i)^2} \quad \ldots (7)$$

$$threshold\ (t) = \sqrt{\sum_{i=1}^{4} (d_{avg}, i + \sigma_i)^2} \quad \ldots. (8)$$

4. EXPERIMENTAL RESULTS

Signature database is a set of binary images from a set of persons. Algorithms are designed and validated with, and tested against this database. The database is divided into a reference set and a validation or test set.

In our proposed system 24 genuine signatures were taken from 39 different persons. Out of which we select 5 signatures for reference (training) purpose and remaining 19 signatures for validation purpose. We also have taken 30 forgery signatures corresponding to each signer. Thus total 1911 signatures (39×19 originals and 39×30 forgeries) were used to test our algorithm.

A. Result

The effectiveness of a system is most commonly described with its "false rejection rate" (FRR), and its "false acceptance rate" (FAR). The false rejection rate is the percentage of

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

original signatures the system rejects. The false acceptance rate is the percentage of forgeries the system accepts as original.

FAR and FRR are calculated by following equation:

$$FAR = \frac{number\ of\ \ forgeries\ accepted}{number\ of\ \ forgeries\ tested} x100 \quad .....(9)$$

$$FRR = \frac{number\ of\ \ originals\ rejected}{number\ of\ \ originals\ tested} x100 \quad .....(10)$$

Table 1: Performance of proposed scheme

Type of signature	Total number of signature tested	Number of signature accepted/ rejected	FAR	FRR
Original Signature	39 × 19 = 741	694/47	---	6.34%
Skilled Forgery signature	39 × 30 = 1170	161/1009	13.76%	---

5. CONCLUSION

My proposed method uses geometric features to classify the signatures that effectively serve to distinguish signatures of different persons. The algorithm is effective and can detect random, simple and skilled forgeries. As an off-line signature verification process could be beneficial and efficient for the banking system particularly for cheque signature forgeries. In this paper a powerful mechanism has been proposed in which a complete off-line signature verification system has been designed.

REFERENCES

[1] H. Hammandlu and V. M. Krishna, " Off-line Signature Verification and Forgery detection using Fuzzy modeling", Pattern Recognition, vol. 38, pp. 341–356, 2005.

[2] B.S PAWAR "Offline Signature Verification And Recognition Using ANN", International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-3, Issue-9, Sept.-2015.

[3] Ranjan Jana, Saptashwa Mandal And Kunal Chhaya " Offline Signature Verification For Authentication", International Journal Of Computer Applications (0975 – 8887) Volume 126 – No.6, September 2015.

[4] Javier Ruiz-del-Solar, Christ Devia, Patricio Loncomilla, and Felipe Concha "Offline Signature Verification Using Local Interest Points and Descriptors", Springer-Verlag Berlin Heidelberg LNCS 5197, pp. 22–29, 2008.

[5] L.E. Martinez, C.M. Travieso, J.B. Alonso, and M. Ferrer, "Parametrization of a forgery Handwritten Signature Verification using SVM", IEEE 38th Annual International Carnahan Conference on Security Technology, pp. 193-196, 2004.

[6] H. Baltzakis, N. papamarkos, "A new signature verification technique based on a two-stage neural network classifier", PII: S0952-1976, 2001.

[7] T. Wessels, C.W. Omlin, "A Hybrid System for Signature Verification", International Joint Conference on Neural Networks IEEE-INNS, 0-7695-0619-4, 2000.

[8] Jalal Mahmud, Chwdry Mofizur Rahman, "On the Power of Feature Analyzer for Signature Verification", Proceedings of the Digital Imaging Computing: Techniques and Applications, 0-7695-2467, 2005.

[9] J. J. Brault and R. Plamondon, "Segmanting Handwritten Signatures at Their Perceptually Important Points", IEEE Trans. Pattern Analysis and Machine Intelligence, vol.15, no. 9, pp.953-957, Sept.1993.

[10] R. M. Samant, Mahendra Shilwant, Bhojraj Sarsambi and Mahesh Shelke "Signature Verification System", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 4, April 2017

[11] Luiz G. Hafemann, Robert Sabourin and Luiz S. Oliveira "Offline Handwritten Signature Verification Literature Review", 978-1-5386-1842-4/17/$31.00 c 2017 IEEE.

[12] S. Srihari. K. M. Kalera. and A. XU, "Offline Signature Verification and Identification Using Distance Statistics", International Journal of Pattern Recognition And Artificial Intelligence ,vol. 18, no. 7, pp. 1339–1360, 2004.

[13] Ashok Kumar. D, Dhandapani. S "Offline Signature Verificationsystem For Bank Cheques Usingzernike Moments, Circularity Property And Neural Network", International Journal of Artificial Intelligence and Applications (IJAIA), Vol. 7, No. 5, September 2016.

[14] S. Reddy. B. Maghi. and P. Babu, "Novel Features for Offline signature verification", Journal of Computer, Communication and Control., vol. 1, pp. 17–24, 2006

[15] Weiping HOU, Xiufen Ye and Kejun Wang "A Survey of Off-line Signature Verification", International Conference on intelligent Mechatronics and Automation Chengdu China, August 2004.

[16] S. N. Srihari and A. Xu., "Learning Strategies and Classification Methods for Offline Signature Verification", Proceedings of the 7th International Workshop on Frontiers in handwriting recognition, 2004.

[17] Madhuri R. Deore and Shubhangi M. Handore,"A survey on offline signature recognition

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

and verification schemes", International Conference on Industrial Instrumentation and Control (ICIC), 2015.

[18] Jingbo Zhang, Xiaoyun Zeng, Yinghua Lu, Lei Zhang, Meng Li, "A Novel Off-line Signature Verification Based on One-class-one-network", Third International Conference on Natural Computation, ICNC 2007, vol. 2, pp. 590-594, Aug. 2007.

[19] Snehil G. Jaiswal and Abhay R Kasetwar,"Offline signature verification using global & local features with neural networks", IEEE International Conference on Advanced Communications, Control and Computing Technologies, 2014.

[20] Debasish Jena, Banshidhar Majhi and Sanjay Kumar Jena,"Improved Offline Signature Verification Scheme Using Feature Point Extraction Method", Journal of Computer Science 4 (2): 111-116, ISSN 1549-3636 © Science Publications, 2008.

[21] Pradeep Kumar, Shekhar Singh, shwani Garg, Nishant Prabhat "Hand Written Signature Recognition & Verification using Neural Network", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, ISSN: 2277 128X, March 2013.

[22] Hemanta Saikia and Kanak Chandra Sarma " Approaches and Issues in Offline Signature Verification System", International Journal of Computer Applications (0975 – 8887) Volume 42– No.16, March 2012.

[23] H. N. Prakash, D. S. Guru, "Geometric Centroids and their Relative Distances for Off-line Signature Verification", 10th International Conference on Document Analysis and Recognition ICDAR '09', pp. 121-125, July 2009.

[24] R. Larkins, M. Mayo, "Adaptive Feature Thresholding for off-line signature verification", 23rd International Conference on Image and Vision Computing New Zealand, IVCNZ 2008, pp.1-6, Nov. 2008.

[25] H. N. Prakash, D. S. Guru, "Geometric Centroids and their Relative Distances for Off-line Signature Verification", 10th International Conference on Document Analysis and Recognition ICDAR '09', pp. 121-125, July 2009.