

Offline Handwritten Signature Verification using Distance based Classifier

Alpana Deka

Assistant Professor, Department of Computer Science, NERIM Group of Institutions, Guwahati, Assam, India

Abstract

An offline handwritten signature verification system reduces number of occurrences of fraud events. In different document materials like credit cards, passport validation, banking transactions and different financial transactions, signatures are verified. Whether a signature is genuine or forgery is detected by comparing the training and testing data sets. This paper describes an offline handwritten signature verification system using global features. Here, signature verification is done by Euclidean distance which results False Rejection Rate (FRR), False Acceptance Rate (FAR) and Total Success Rate (TSR) as 6.66%, 26.66% and 93.3% respectively.

Keywords: Preprocessing, Feature Extraction, Euclidean Distance, FAR, FRR

1. Introduction

A handwritten signature verification system can be viewed from two perspectives. Firstly it verifies identification of a person. Secondly, it verifies a given signature itself. Signature of a person consists of some graphical marks on the surface where the signature is done [1]. Signature verification is so different with the character identification, because signature is often illegible and it seems to be just an image with some particular curves that represent the writing style of the person. Signature is just a special case of handwriting and often is just a symbol [2]. The offline and online are the two approaches in signature verification systems to verify a signature [3]. Again there are two types of variations like intra and inter personal variations are observed to present. The variation among signatures of same person is called intra personal variation. The variation between originals and forgeries is called inter personal variation. Less variation of intra personal variation and high variation of inter personal variation result an efficient signature verification system. Variation between training and testing signatures indicate three types of forgeries [4][5].

Random forgery: Random forgery is created by the person without having knowledge of the shape of original signature.

Simple forgery: Simple forgery is represented by a signature sample which written by the person who know the shape of original signature without much practice.

Skilled forgery: The last type called skilled forgery, which is represented by a suitable imitation of the genuine signature model.

2. Overview of proposed verification system

For signature verification, the basic steps are given below: Each of these steps are interrelated to verify a signature. For the proposed system, we have collected 30 and 45 signature samples in a white

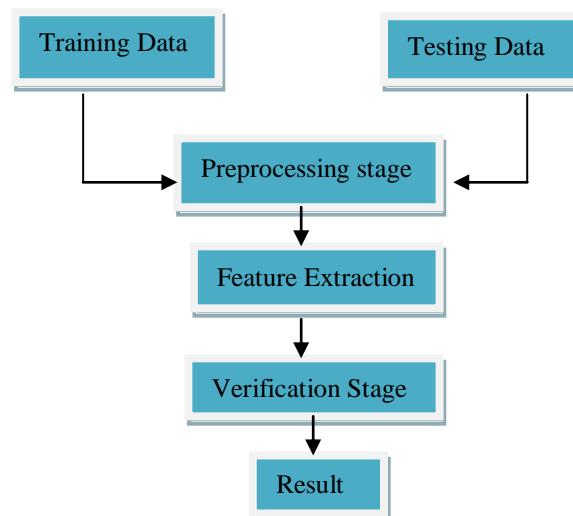


Fig. 1: Block Diagram of proposed system

paper sheet for training and testing database respectively. The testing database consists of 30 genuine and 15 forgery signatures. Then the signatures are extracted with the help of a scanner

with suitable resolution. In 2nd stage, samples are preprocessed such that noise, thickness of the pen, size of the signature etc. cannot degrade verification result of the system. Then features are extracted from the preprocessed signatures. Finally, decision is taken on the basis of Euclidean distance.

3. Preprocessing

To improve the efficiency of a proposed system, preprocessing is performed on both the training and testing signature samples. The collected RGB signature image is first converted to gray scale image. The gray scale image is then converted to binary image.

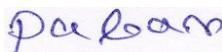


Fig. 2: A signature sample



Fig. 3: Grayscale image



Fig. 4: Complement binary image



Fig. 5: Thinned signature image

In a binary signature sample, foreground is black and background is white. Now complement operation is performed such that foreground becomes white and background becomes black. This is followed by thinning operation to convert thickness of the pen into one pixel i.e. to extract basic pattern of the signature. This is used to take care of the thickness variations so that the effects like change of pen etc should not affect the detection system [6]. Some preprocessing steps are displayed from Fig. 2 to Fig. 5.

4. Features Extraction

Features are some scalar properties with which one object can be differentiated from another one. Feature selection is the process of identifying characteristics or features that remain inherent within an object. Since a single feature is not sufficient for judgment of object, therefore a feature vector is constructed by combining a number of features [7]. A particular signature sample can be verified by analyzing features extracted from preprocessed training as well as testing samples. Therefore, features are extracted from both training and testing samples. Here, we have considered global features which are given below [1][8][9][10]:

Image area: Image area is the number of on pixels in the signature. It is calculated by summing these on pixels.

Aspect ratio: For height-width ratio of a signature, first maximum length of columns and maximum

length of rows of a cropped image are taken. Maximum length of column gives height and maximum length of rows gives width of a signature. Variation may occur in height and width of different signature samples collected from same person but height-width ratio of the samples of the same person approximately remains constant.

Normalized area of signature: Normalized area of a signature is calculated by taking the ratio of area of signature image to the area of signature enclosed in a bounding box. Area of bounding box is obtained by multiplying height and width of the bounding box.

Maximum vertical projection: For vertical projection calculation, signature is scanned horizontally to find the number of foreground pixels in each column. Here maximum vertical projection is obtained by observing the column with maximum value.

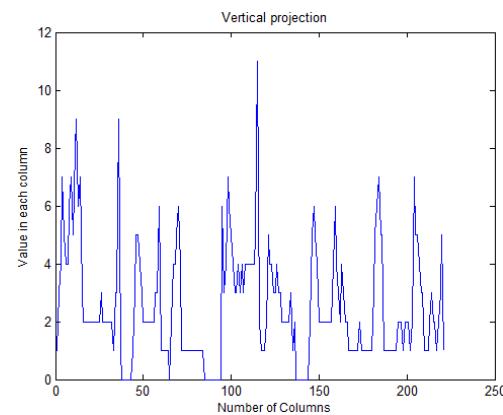


Fig. 6: Vertical projection

Maximum horizontal projection: The operation of horizontal projection is same as vertical projection but done vertically. Here, signature is scanned in vertical direction. Then the row with maximum number of white pixels is selected as maximum horizontal projection.

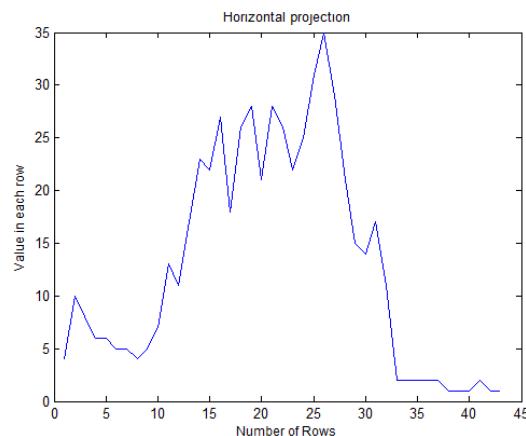


Fig. 7: Horizontal projection

Table 1: Features values of 5 genuine signature samples collected from same person

Image area	Aspect ratio	Normalized area	Maximum vertical projection	Maximum horizontal projection
1082	0.3556	0.0281	17	30
910	0.3836	0.0255	21	28
895	0.3754	0.0215	17	29
962	0.3312	0.0289	26	28
1037	0.3316	0.0220	17	29

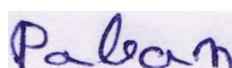


Fig. 8: A simple forgery signature



Fig. 9: Thinned image

Now, a forgery signature sample is shown in Fig. 8 and its extracted features from Fig. 9 are given in Table 2.

Table 2: Features values extracted from image displayed in Fig. 9

Features	Values
Image Area	639
Aspect ratio	0.5156
Normalized Area	0.0148
Maximum Vertical Projection	14
Maximum Horizontal Projection	20

5. Verification

Here, Euclidean distance is used as a classifier to verify a signature. For this, two feature vectors of same size (training and testing feature vector) are computed to apply the distance measure. Therefore, when a signature is to be verified, first the features will be extracted from preprocessed one, which gives testing feature vector. Then Euclidean distance is applied between this feature vector and each of the feature vectors of 30 signature samples which are already in database (training feature vector). Thus 30 Euclidean distance measures are computed for each of the testing dataset. The Euclidean distance is obtained by

$$\sqrt{\sum_{i=1}^n (a_i - b_i)^2}$$

Here, a_i and b_i are two feature vectors of same size. Since we have considered 5 numbers of features for training and testing samples, therefore a_i and b_i are training and testing feature vector respectively with equal size 5.

Now applying above equation, the distance which is the smallest distance from training feature vector to the testing feature vector is considered as desired one. Now, if this distance reflects the desired training sample in the database then the tested signature is accepted as genuine signature otherwise it is recognized as forgery signature.

6. Experimental result

False Rejection Rate (FRR) and False Acceptance Rate (FAR) give performance measurement of signature verification system. FRR gives number of rejected original signatures out of total number of original signature tested. Similarly, FAR indicates number of accepted forgery signature to the total number of tested forgery signatures. System performance can also be calculated in terms of Total Success Rate (TSR). TSR is the ratio of number of correctly accepted signatures to the total number of signatures tested by the system [11]. Thus we have obtained 6.66%, 26.66% and 93.3% as FRR, FAR and TSR respectively.

6. Conclusion

The system given above uses distance classifier on global features to differentiate signatures. The verification is done on genuine and simple forgery signatures. Here signatures are collected at different time intervals since physical and psychological state of a person, writing surface, surrounded environment may affect a signature which produces intra personal variation [12]. The performance of the existing system can be improved by applying other classifiers such as neural network, fuzzy logic.

References

- [1] Alamoudi, O. O. and Mohammed, S. E. F.: "Offline Signature Verification using Machine Vision", Journal of Science & Technology, Vol. 14 (No. 2): pp: 3-35, (2009).
- [2] Ashok, K. D. and Dhandapani, S.: "Offline Signature Verification System for Bank Cheques Using Zerinke Moments, Circularity Property and Fuzzy Logic", International Journal of

- Engineering and Computer Science, Vol. 6 (Issue 9): pp: 22442-22449, (2017).
- [3] Baltzakis , H. and Papamarkoz, N.: "A new signature verification technique based on a two-stage neural network classifier", Engineering Applications of Artificial Intelligence, Vol. 14, pp:95-103, (2001).
- [4] Biswas, S., Kim, T.H. and Bhattacharyya, D.: "Features Extraction and Verification of Signature Image Using Clustering Technique", International Journal of Smart Home, Vol. 4 (No. 3), pp: 43-56, (2010).
- [5] Deka, A. :"A Study of Features Data in Offline Handwritten Signatures", International Journal of Scientific Research in Computer Science Applications and Management Studies, Vol. 8 (Issue 2), (2019).
- [6] Fotak, T., Baca, M. and Koruga. P.: "Handwritten Signature Identification using Basic Concepts of Graph Theory", Wseas Transactions on Signal Processing, Vol. 7 (Issue 4), pp: 117-129, (2011).
- [7] Kumar, P., Singh, S., Garg, A. and Prabhat, N. : "handwritten Signature Recognition and verification using Neural Network", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3 (Issue 3), pp: 558-565 (2013).
- [8] Maheswaran, S.: "Fuzzy Logic Based Off-line Signature Verification and Forgery Detection System".
- [9] Majhi, B., Reddy, Y. S. and Babu, D. P.: "Novel Features for Off-line Signature Verification", International Journal of Computers, Communications & Control, Vol. I (No. 1), pp. 17-24, (2006).
- [10] Panchal, S. T. and Yerigeri, V. V.: "Offline Signature Verification based on Geometric Feature Extraction using Artificial Neural Network", IOSR Journal of Electronics and Communication Engineering, Vol. 13 (Issue 3), pp: 55-59. (2018).
- [11] Ravi, J. and Raja, K. B.: "Concatenation of Spatial and Transformation Features for Off-Line Signature Identification", International Journal of Innovative Technology and Exploring Engineering, Vol. 1, pp: 102, 108, (2012).
- [12] Tiwari, D. and Sharma, B.: "Development of Intelligent Network for Offline Signature Verification Using Pixel Density, Directional Method and Both Method Together", International Journal of Computer Trends and Technology, Vol. 3 (Issue 3), pp: 403-411, (2012).