International Journal of Scientific Research and Management (IJSRM)
||Volume||5||Issue||05||Pages||5327-5330||2017||
Website: www.ijsrm.in ISSN (e): 2321-3418
Index Copernicus value (2015): 57.47 DOI: 10.18535/ijsrm/v5i5.07

Signature Verification Using Support Vector Machine (SVM)

Ravinder kumar[1], Poonam singhal[2]

Deenbandhuchhotu Ram University of Science and Technology, Murthal (Sonipat)

Abstract

Automated signature verification has many applications in our daily life like Bank-cheque processing, document authentication, ATM access etc. Handwritten signatures have proved to be important in authenticating a person's identity, who is signing the document. In this paper we present an off-line signature verification and recognition system using the global, directional and grid features of signatures. Support vector machine (SVM) was used to verify and classify the signatures. As there are unique and important variations in the feature elements of each signature, so in order to match a particular signature with the database, the structural parameters of the signatures along with the local variations in the signature characteristics are used. The artificial neural networks are trained by these characteristic. The system uses the features extracted from the signatures such as centroid, height – width ratio, total area, first and second order derivatives, quadrant areas etc. After the verification of the signature the angle features are used in fuzzy logic based system for forgery detection and the performance is increases approximately (80%) when using SVM as a classifier

Keywords—.Forgery detection; Support Vector Machine (SVM); Signature verification; Artificial Neural Network (ANN); Fuzzy Logic; Computer Vision

I INTRODUCTION

Handwritten signature has long been established as the most diffuse mean for personal verification in our day to day life. It is generally, in all kind of legal transaction and documents. Therefore, the signature is probably the widest acceptance in all the biometric modalities. We can also say that the signature is a behavioural characteristic of individual, and therefore it is considered being weaker against fraud. Signature verification is the process in which, we verify a given signature who belongs to a user, a genuine signature, or has been made by another user, a forgery signature,and decision is made whether the signature has been made by that user [1].The main application of signature verification including use in financial transaction, providing electronic signatures for documents and in providing additional securities measure for computer system authentication [2].

In signature verification systems, firstly the user enrolment is provided by a number of signature samples. If when a user give a new signature then firstly the signature compared with the reference signatures for that individuals. There are certain threshold values are given to find out the dissimilarity between the both signature, if the value is below this value then the user is authenticated, otherwise denied [3]

There are following two approach to detect the signature is genuine or forgery.

(i) Offline Approach

(ii) Online Approach

Online approaches means weuse a digitizing surface to capture dynamic features like pressure, speed, direction etc. which result in higher accuracies. Off-line verification means us deals with signatures that have been written on paper and digitized by scanning them. Off line approach is less accurate as compared to the online approach. But in many situation we use the offline approach. The forgeries related to handwritten signatures are classified into three types.

A .*Skilled Forgery*

This forgery is created by some professional forger and they are well trained for a long time to forge other's signatures. These are very tough and challenging for detection.

B .*Casual Forgery*

In this type of forgery the signer observes the signatures of others closely for a very brief time and then puts them in his own style without any prior practice.

C .*Random Forgery*

The signer or the forger creates it by using the name of the victim in his own style to create a forgery known as the simple forgery or random forgery [4].

In this paper, we proposed an off-line signature verification system using support vector machine (SVM). The SVM is introduced by Vapnik et al. [4,5], tries to find an optimal hyper plane for separating two classes.Basically, SVM is used to separating linearly two

classes. A kernel function is used as radial basic function (RBF) or multilayer perception, when the data is none linearly separable. In order to define if a signature is genuine or forgery, a rule is performed on the outputof the SVMs where values are positive or negative.Hence, the output of the SVMs should be transformed to the objective evidences expressed as the membership degree. In practice, for membership degree no standard form is defined. The only constraint is that it must be limited in the range of 0,1 whereas SVM produce a single output [6].

There are various method that are used for offline signature verification like template matching, minimum distance classifiers, elastic image matching and neural networks and others. These all methods are summarized in a survey articles [7], [8], [9], [10], [11], [12].

This paper is arranged as follows: section II presents the proposed method. Section III shows the pre-processing, Section IV shows the methodology, Section V shows the result and conclusion and VI is conclusion.

II PROPOSED METHOD

There are two major part of this system: (1) training signature, (ii) Testing of given signature. The block diagram of the system is given in Figure 1.

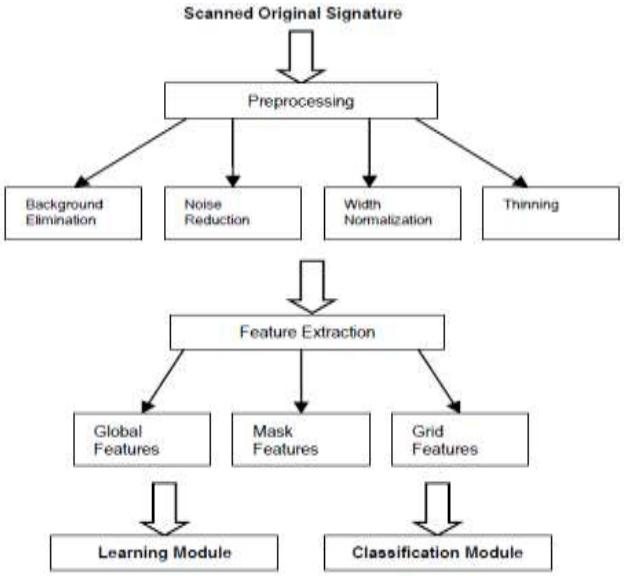

Figure 1. Block diagram of proposed system [13]

III PREPROCESSING

Training and testing both phases are applied to the pre-processing step. In gray the signature is scanned. The main purpose in thisphase is to make signatures standard and ready for feature extraction. The pre-processing stage includes four steps: Background elimination, noise reduction, width normalization and skeletonization. The pre-processing steps of an example signature are shown in Figure 2.

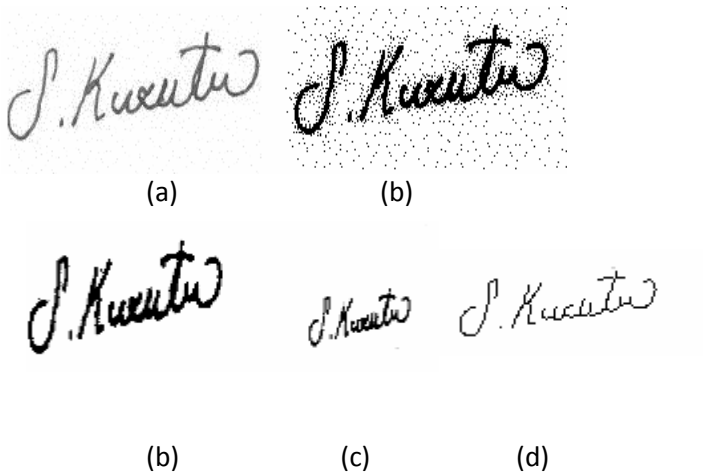

Figure 2. Pre-processing steps: (a) scanning (b) background (c) noise reduction (d) width normalization, (e) thinning applied signature [13]

For extracting features the data areas are cropping. To capture the signature from the background, we use p-tile threshold. After thresholding the signature would be "1" and the other pixels which belongs to the background would be "0"

For noise reduction we use noise reduction filter which is applied to the binary image for eliminating single black pixels on white background. There are two types of differences intrapersonal and interpersonal, which exists in signature dimension. So the image width is adjusted to a default value and height will change without any change on height-to-width ratio. Width dimension is finally normalized and adjusted to 100. The main moto of thinning is to eliminate the thickness differences of pen by making the image one pixel thick. Hilditch's algorithm is used in this system.

IV METHODOLOGY

These systems are divided into three parts: (i) signature's feature extraction (ii) Signature alignment (iii) Enrollment. The block diagram of the system is shown in Figure 3.

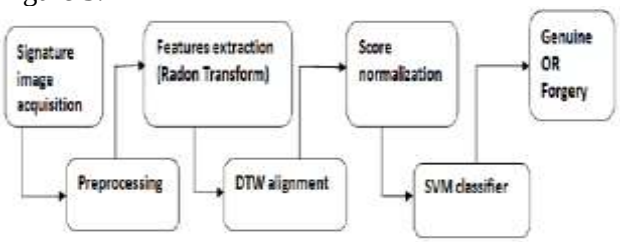

Figure 3. Signature verification system [14]

Enrollment phase means a set of reference signatures are used to determine user dependent parameter characterizing the variance within the reference signature. The signature reference sets, together with these parameters, are stored with unique identifier.

In training phase we select a number of genuine and a forged signature for training the SVM classifier. And in the verification phase, a test signature is input to the system, it compared to the reference signatures of the claimed person. If the person is authentic then the dissimilarity measure is below or equal a threshold value of the classifier, otherwise denied. The signature verification system are described in the following sections.

A. SIGNATURE'S FEATURE EXTRACTION

Matrix is a discrete random transform (DRT), where each column represents a projection or shadow of the original image at a certain angle. DRT can be expressed as follows [15], [16]:

$$R_j = \sum_{i=1}^{\Psi} w_{ij} I_i ; \; j = 1,2,\ldots, \; N_\varphi N_\theta \qquad 1$$

Where:R_j = the cumulative intensity of the pixels that lies within the j^{th}beam.
Ψ= image total pixel.
W_{ij} = the i^{th}pixel to j^{th} beam-sum contribution
I_i = the intensity of the I_{th} pixel.
N_Φ =non-overlapping beams per angle.
N_Θ =number of total angles.

For extracting signature, firstly the background of the signature image is mapped to zero. After that, median filtering is applied to remove speckle noise. Immediately the DRT of the signature image is calculated. DRT is calculated at angle N_Θ. These angles are equally divided between "0^0 to 180^0" [17], [18].

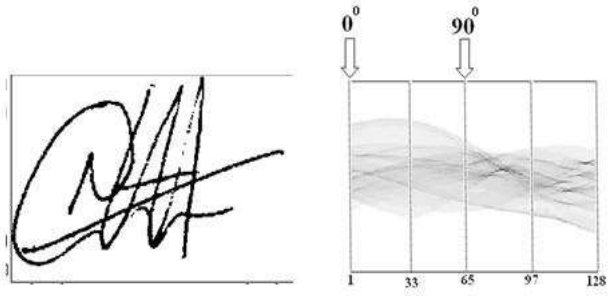

Figure 4.A signature and its DRT. The DRT is displayed as a gray-scale image. This image has N_Θ =128 columns, where each columns represents a projection [14].

B. SIGNATURE ALLIGNMENT

We use a dynamic time warping (DTW) algorithm to compare two signature of different length [9]. The best linear alignment of two vectors are found by DTW, and the overall distance between them is reduced (see in figure 5).

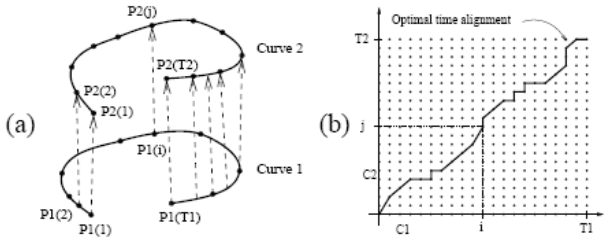

Figure 5. Two curves with the correspondence points indicated. (b) Warping plane and Warping path.

The rotation occurs in the observation sequence, and the rotation invariant representation corresponding to the signature image and the observation sequence is necessary. Iiteratively shifts the observation sequences with respect to each other. During any iteration the distances between the corresponding observations (feature vectors) are calculated.

C. ENROLLMENT

We use a number of signature during the enrollment of the system, all signature are aligned in pair wise to find out the distance between pair, using DTW algorithm. From these alignment, the following references sets are calculated:

i. The farthest signature 's average distance (d_{max})
ii. The nearest signature 's average distance (d_{min})

V EXPERIMENT AND RESULTS

A dataset is used for this experiment, which is called as "MCYT-100 signature CORPUS" [19]; a static signature images are contain in this dataset. The dataset contains 1320 signatures from 70 persons.In which 15 genuine signature and 15 skilled signature. For training 40 persons signatures are used. Each of these persons signed 8 original signatures andrest 30 persons imitated the signatures. In which 4 forgery signatures are signed for each 4 person.

In each individual enrollment 5 genuine signatures are used as a reference set and remaining signatures are used for training and testing. We conform that the training data is different from both the reference set of genuine signatures and the test data used in experiments.

By using this method we can get a performance of approximately (80%) when using SVM as a classifier.

VI CONCLUSION

In this paper we present an offline signature verification system, which is based on a two-class pattern recognition problem using SVM classifier.

For global feature extraction system we used a DRT system and we can say that this method is stable and robust method. We create a model for a signature with DTW by using DRT simulated time evolution from one features to the next.

We use SVM classifier and obtained 80% overall performance for the data sets of 70 persons and 1320 signatures.

REFERENCES

1. A. M Ormaza, o.m. hurtado, and R.A Moreno, "On-line Signature Biometrics using Support VectorMachine" international journal of pattern recognition and artificial intelligence, vol 15, no.4, pp. 357-641, 2001.
2. C. E. Pippin, "Dynamic signature verification using local and globalfeatures", Georgia Institute of Technology July 2004.
3. AHMED ABDELRAHMAN, AHMED ABDALLAH, "Signature Verification System Based on Support Vector Machine" in The conference of International Arab, vol.4, no.2, pp.521-555, 2013.
4. Anjali.R1, Manju Rani Mathew, "Offline Signature Verification Based on SVMand Neural Network" in international Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering" vol. 2, special issue 1, dec 2013.
5. V. N. Vapnik, the Nature Of Statistical Learning Theory, Springer,1995.
6. T. Mitchell, Machine Learning, McGraw-Hill, 1997.
7. V. Nguyen; Blumenstein, M.; Muthukkumarasamy V.; Leedham G.,"Off-line Signature Verification Using Enhanced Modified DirectionFeatures in Conjunction with Neural Classifiers and Support VectorMachines", in Proc. 9th IntConf on document analysis and recognition,vol 02, pp. 734-738, Sep 2007.
8. R. Plamondon and G. Lorette, "Automatic signature verification andwriter identification—the state of the art," Pattern Recognition, vol. 22,no. 2, pp. 107–131, 1989.
9. R. Sabourin, R. Plamondon, and G. Lorette, "Off-line identification withhandwritten signature images: survey and perspectives," in StructuredDocument Image Analysis, H. Baird, H. Bunke, and K. Yamamoto,Eds., pp. 219–234, Springer-Verlag, NY, USA, 1992.
10. F. Leclerc and R. Plamondon, "Automatic signature verification: thestate of the art, 1989–1993," International Journal of Pattern Recognitionand Artificial Intelligence, vol. 8, no. 3, pp. 643–660, 1994.
11. J. Gupta and A. McCabe, "A review of dynamic handwritten signatureverification," Tech. Rep., James Cook University, Australia, 1997.
12. R. Plamondon and S. N. Srihari, "On-line and off-line handwritingrecognition: a comprehensive survey," IEEE Trans. On Pattern Analysisand Machine Intelligence, vol. 22, no. 1, pp.63–84, 2000.
13. J. K. Guo, D. Doermann, and A. Rosenfeld, "Forgery detection by localcorrespondence," International Journal of Pattern Recognition andArtificial Intelligence, vol. 15, no. 4, pp. 579–641, 2001.
14. *EmreÖzgündüz,TülinŞentürk and M. ElifKarslıgil, "*OFF-LINE SIGNATURE VERIFICATION AND RECOGNITIONBY SUPPORT VECTOR MACHINE" in international conference on documents analysis and recognition, vol 1, pp.103-115, 2001.
15. A. A. Abdalla Ali, A. A. MohmmedEmam, K-Nearest NeighborClassifier For Signature Verification System, International Conferenceon Computing, Electrical and Electronic Engineering ICCEE 2013.
16. R. N. Bracewell, Two-Dimensional Imaging, Prentice-Hall, EnglewoodCliffs, NJ, USA, 1995.
17. T. Peter, The Radon Transform - Theory and Implementation, Ph.D.thesis, Technical University of Denmark, June 1996.
18. A. A. Abdalla Ali, V.F. Zhirkov, "Off line signature verification usingradon transform and svm/knn classifiers", TSTU Trans. Vol. 15. № 1.pp. 62-69, Весник ТГТУ. Том 15. No 1, 2001.
19. J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M.Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C.Vivaracho, D. Escudero and Q.-I. Moro, "MCYT baseline corpus: abimodal biometric database", IEE Proc.-Vis. Image Signal Process., Vol.150, No. 6, December 2003