IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 13, Issue 3, Ver.III (May. - June. 2018), PP 53-59
www.iosrjournals.org

Offline signature verification based on geometric feature extraction using artificial neural network

Sumedha Tanajirao Panchal, V. V. Yerigeri
(Department of Post Graduation, MBES COE Ambajogai, Dr. B.A.M.University, India)
(Department of Post Graduation, MBES COE Ambajogai, Dr. B.A.M.University, India)

Abstract *— The fact that the signature is widely used as a means of personal verification emphasizes the need for an automatic verification system because of the unfortunate side-effect of being easily abused by those who would feign the identification or intent of an individual. A great deal of work has been done in the area of off-line signature verification over the past few decades. Verification can be performed either Offline or Online based on the application. Online systems use dynamic information of a signature captured at the time the signature is made. Offline systems work on the scanned image of a signature. In this paper, we present a method for Offline Verification of signatures using a set of simple shape based geometric features. The features that are used are Area, Euler's Number, Eccentricity, Standard deviation, Centroid, Skewness, Kurtosis and Orientation. Before extracting the features, preprocessing of a scanned image is necessary to isolate the signature part and to remove any spurious noise present. The system is initially trained using a database of signatures obtained from those individuals whose signatures have to be authenticated by the system.*
Then artificial neural network (ANN) is used in recognition and verification of signatures: genuine or forged, and efficiency is about 86.67% having threshold of 80%. Simulation results shows that the technique is robust and clearly differentiates between genuine and forgery signatures.

Keywords- *Offline signature; neural network; Geometric feature; False Acceptance Rate; False Rejection Rate*

Date of Submission: 02-07-2018 Date of acceptance: 18-07-2018

I. Introduction

Traditional bank checks, bank credits, credit cards and various legal documents are an integral part of the modern economy. They are one of the primary mediums by which individuals and organizations transfer money and pay bills. Even today all these transactions especially financial require our signatures to be authenticated. The inevitable side-effect of signatures is that they can be exploited for the purpose of feigning a document's authenticity. Hence the need for research in efficient automated solutions for signature recognition and verification has increased in recent years to avoid being vulnerable to fraud [1],[2],[3],[4].

Approaches to signature verification fall into two categories according to the acquisition of the data: *On-line* and *Off-line*. On-line data records the motion of the stylus while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time. Online systems use these data captured during acquisition. Online systems could be used in real time applications like credit cards transaction or resource access. While off-Line signature verification systems take as input the 2-D image of a signature**.** Offline systems are useful in automatic verification of signatures found on bank checks and documents [5],[6]. A robust system has to be designed which should not only be able to consider these factors but also detect various types of forgeries.

In signature verification, forged signatures can be broken up into *three* different categories. These categories are based on how similar a forgery is in relation to the genuine signature and are known as *random*, *simple* and *skilled*. *In random forgery* the forger does not know the signer's name or signature shape. In *simple forgery or unskilled forgery*, the forger knows the name of the original signer but not what his signature looks like. While in *skilled forgery*, a close imitation of the genuine signature is produced by a forger who has seen and practiced writing the genuine signature. It is these skilled forgeries that this paper will focus on for signature verification [7].

II Related Work

A great deal of work has been done in the area of offline signature verification for the detection of random forgeries. Earlier work on offline signature verification deals primarily with casual and random forgeries. Many searchers therefore found it sufficient to consider only the global features of a signature. As signature databases became larger and archers moved toward more difficult skilled forgery detection tasks, we

saw a progression not only to more elaborate classifiers, but also to the increased use of local features and matching techniques.

1. Baltzakis developed a neural network-based system for the detection of random forgeries. The system uses global features, grid features, and texture features to represent each signature. For each one of these feature sets, a special two-stage perceptron one class one network classification structureis implemented. In the first stage, the classifier combines the decision results of the neural networks and the Euclidean distance obtained using the three feature sets.
2. Kaewkongka uses the Hough transform to extract the parameterized Hough space from a signature skeleton as a unique characteristic feature of a signature. A back propagation neural network is used to evaluate the performance of the method.
3. Quek used global baseline features (the vertical and horizontal position in the signature image which corresponds to the peak in the frequency histogram of the vertical and horizontal projection of the binary image, respectively), pressure features (that correspond to high pressure regions in the signature), and slant features (which are found by examining the neighbours of each pixel of the thinned signature). He then conducts two types of experiments. The first group of experiments uses genuine signatures and forgeries as training data, while the second group of experiments uses only genuine signatures as training data. These experiments are conducted on the signatures of 15 different writers, that is, 5 writers from 3 different ethnic groups. For each writer, 5 genuine signatures and 5 skilled forgeries are submitted. When genuine signatures and forgeries are used as training data, the average of the individual EERs is 22.4%.
4. El-Yacoubi uses HMMs and the cross-validation principle for random forgery detection. A grid is superimposed on each signature image, segmenting it into local square cells. From each cell, the pixel density is computed so that each pixel density represents a local feature. Each signature image is therefore represented by a sequence of feature vectors, where each feature vector represents the pixel densities associated with a column of cells. The cross-validation principle forgeries, subsets of other writers training sets are used for impostor validation. Two experiments are conducted on two independent data sets, where each data set contains the signatures of 40 and 60 writers, respectively .Both experiments involves the use of a subset (validation set) of each writer straining set for validation purposes. Since this system aims to detect only random use 20 genuine signatures for training and 10 for validation

II. Proposed Methodology

In this paper, the recognition and verification of offline signature samples using artificial neural network is relevant as it follows a paradigm which models human learning patterns.

1. Data Acquisition/Signature Database

In offline signature verification signatures from individual person are taken on paper and then scanned with scanner. In this paper we have used standard MCYT-75 offline signature corpus database [3]. The database contains data from individuals, including genuine signatures and forgeries signatures. The signatures are collected by acquisition device using WACOM Intuos (Inking pen). Each signature image having dimension of 850 x 360 pixels.

2. Preprocessing

Image pre-processing represents a wide range of techniques that exist for the manipulation and modification of images. It is the first step in signature verification and recognition. A successful implementation of this step produces improved results and higher accuracy rates. After an image is acquired, it goes through different levels of processing before it is ready for the next step of feature extraction. The following are the reasons why image preprocessing is important:

- It creates a level of similarity in the general features of an image, like the size aspect. This enhances the comparison between images.
- Signatures vary according to the tool that was used in writing; the type of pen/pencil, the ink, the pressure of the hand of the person making the signature, and so on. In off-line signature recognition, these facts are not important, and have to be eliminated and the matching should be based on more important offline features.
- Noise reduction, defects removal and image enhancement.
- Improves the quality of image information.
- It eases the process of feature extraction, on which the matching depends mainly.

The prepossessing stage includes following steps.

2.1 RGB to gray scale conversion:

In this step RGB image is converted into gray scale intensity signature image to eliminate the hue and saturation information while retaining the luminance.

2.2 Binarization:

A gray scale signature image is converted into binary to count the number of black pixels which make feature extraction simpler.

2.3 Thinning:
Thinning is a morphological operation that is used to remove selected foreground pixels from binary_images, somewhat like erosion or opening. It can be used for several applications, but is particularly useful for skeletonization. In this mode it is commonly used to tidy up the output of edge detectors by reducing all lines to single pixel thickness. Thinning is normally only applied to binary images, and produces another binary image as output.

2.4 Cropping:
We cropped the image by the value returned by bounding box calculation method. This reduces the area of signature to be used for further processing

3. Feature Extraction
Features Extraction is the key to develop an offline signature recognition system. We use a set of eight global features that cannot be affected by the temporal shift. These features are geometrical features based on the shape and dimensions of a signature image. The various shape features that we use are: Area, Euler's Number, Eccentricity, Standard deviation, Centroid, Skewness, Kurtosis and Orientation.

- Area : Total number of black pixels present in the binary image

- Euler's Number: The Euler number is the total number of objects in the image minus the total number of holes in those objects.

- Eccentricity: The eccentricity is the ratio of the distance between the foci of the ellipse and its major axis length. The value is between 0 and 1

- Standard Deviation: It is a most widely used measure of variability or diversity used in statistics. It gives the how much variation or dispersion exists from the average (mean or expected value) The low standard deviation indicates that the data points tend to be very close to the mean and high standard deviation indicates that the data points are spread over a large range values.

  Standard Deviation is mathematically represented as

$$\sigma = \sqrt{\sum_{i=0}^{L-1} (r_i - \mu)^2 \, p(r_i)} \quad (1)$$

where, [0,L-1] is range of intensity value, r_i is i^{th} intensity value, $p(r_i)$ is probability of intensity r_i.

$$p(r_i) = \frac{n_i}{m \times n} \quad (2)$$

where, n_i is number of pixels in the signature with intensity r_i,m x n is size of signature, μ is average intensity value.

$$\mu = r_i \times p(r_i) \quad (3)$$

- Centroid: It denotes to the center point of vertical and horizontal of the signature.
- Skewness: It measure the asymmetricity of the probability distribution of a real valued random variable having positive, negative or may have undefined value.
  Skewness is mathematically represented as

$$s = \sigma^{-3} \sum_{i=0}^{L-1} (r_i - \mu)^3 \, p(r_i) \tag{4}$$

Where, σ is standard deviation, , [0,L-1] is range of intensity value, r_i is i^{th} intensity value, $p(r_i)$ is probability of intensity r_i, μ is average intensity value.

- Kurtosis: It measures the structure of probability distribution function of a real valued random variable and is related to the fourth moment of a mean.

$$K = \sigma^{-4} \sum_{i=0}^{L-1} (r_i - \mu)^4 \, p(r_i) \tag{5}$$

where, σ is standard deviation, , [0,L-1] is range of intensity value, r_i is i^{th} intensity value, $p(r_i)$ is probability of intensity r_i, μ is average intensity value.

- Orientation: Angle between the *x*-axis and the major axis of the ellipse that has the same second-moments as the region, returned as a scalar. The value is in degrees, ranging from -90 degrees to 90 degrees..

4. Training and Verification:

4.1 ANN Training

Artificial Neural Network or ANN resembles the human brain in learning through training and data storage. The ANN is created and trained through a given input/ target data training pattern. During the learning process the neural network output is compared with the value and a network weight correction via a learning algorithm is performed in such a way to
Minimize an error function between the two values.
The mean-squared error (MSE) is a commonly used error function which tries to minimize the average error between the network's output and the target value. And the training is successfully done as shown in Fig.1.

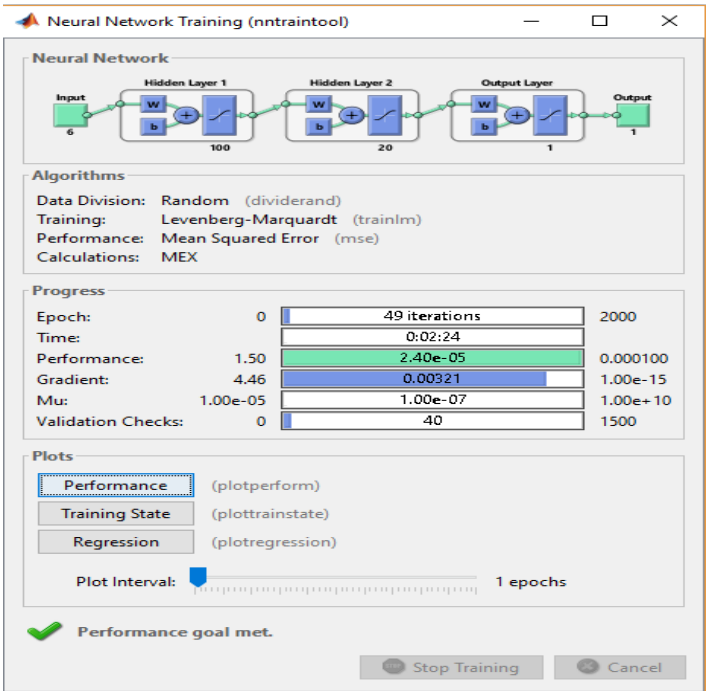

Figure 1: Neural Network Training

4.2 ANN Testing

The system has been tested for its accuracy and effectiveness on a database of about 120 signatures, which contains both their genuine and skilled forged signature sample counterparts. Our database consists of signatures done with different pens. All the samples of our database were pre-processed and the geometric features were extracted out. After features extraction, testing is done and the result is displayed,

IV. Result And Discussion

1. Performance measure:

The performance measure of the signature verification is measured in terms of false rejection rate (FRR) and false acceptance rate (FAR). False acceptance occurs when forgeries signatures are accepted as genuine while in case of false rejection genuine signature are accepted as forgery.

$$\text{FAR} = \frac{\text{Number of genuine accepted}}{\text{Number of forgery tested}} \times 100 \tag{6}$$

$$\text{FRR} = \frac{\text{Number of genuine rejected}}{\text{Number of genuine tested}} \times 100 \tag{7}$$

The overall accuracy of the system is the mean between percentage of genuine signatures verified as genuine and percentage of forgery signature is verified as forgery.

$$\text{Accuracy} = \frac{(100 - \text{FAR}) + (100 - \text{FRR})}{2} \tag{8}$$

2. Results

For the signature verification we were used different 10 users each having 20 genuine and 20 forgery signatures. This signature database taken from MCYT-75 offline Signature Corpus database hence total number of 450 Signatures were taken each having dimension of 850x360 pixels, these signature images were pre-processed and different geometric features were extracted by image processing and this was performed on matlabR2017a, after that we train the data through neural network, then select signature from test database.

The result is demonstrated on a database of 10 users each having 20 signatures, some of them are genuine and forgery signature shown in fig 2 and fig 3,shows FAR and FRR of each users. Thus the total accuracy obtained from the proposed method is 86.67, the accuracy for training and testing is shown in below table

Thus the total accuracy obtained from the proposed method is 86.67, the accuracy for training and testing is shown in table 1.

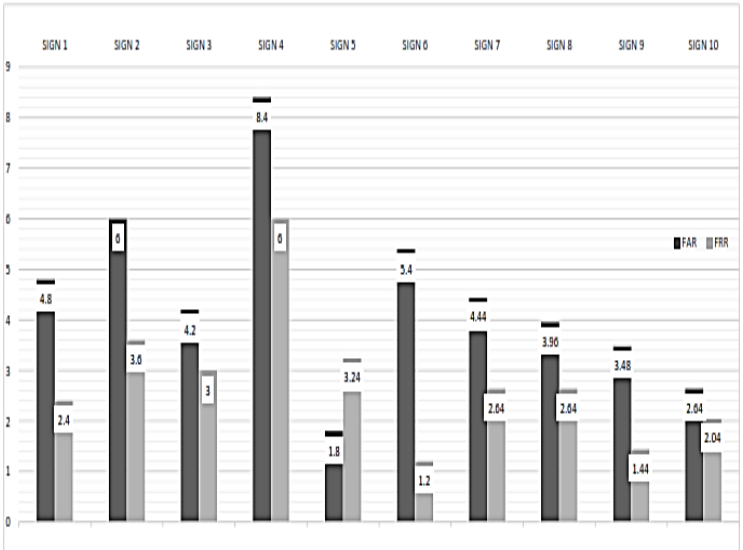

Figure 2: FAR and FRR of each user

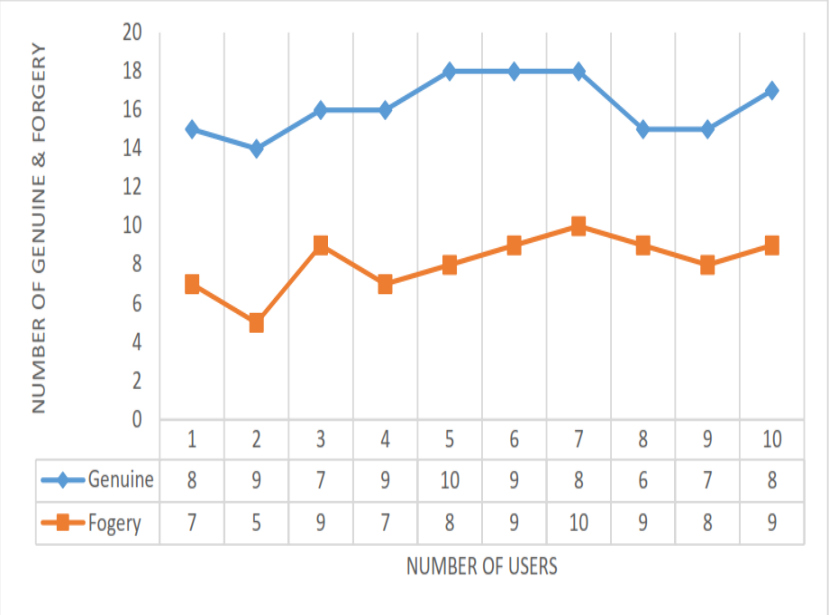

Figure 3: Number of Genuine and Forgery signature recognized

Table 1: Result of BPNN

	Accuracy rate	**Error rate**
Training	72.81%	21.19%
Test	80.00%	20%

V. Conclusion and Future Works

The main objective of the project is to verify a signature using neural networks. An offline signature recognition system using back propagation neural network is implemented in this project. The results show that the BPNN gives a good accuracy which is 86.67% in terms of FRR and FAR rates. This indicates that our approach and the features are working well with a good optimization of 'verification the offline signature'.

The future work of this project is to verify the signature database using other efficient verification methods like Conic Section Function Neural Network (CSFNN), Multi Layer Perception (MLP) Neural Network, RBF Neural Network method etc and compare the results of Back propagation Neural Network with these results.

The signature verification can also be changed by changing the features that can be extracted from a signature. So, the future work of the verification of signature can be done with the same Neural Network methods but using different signature features and compares the results with results of the present project.

Acknowledgements

We convey our sincere thanks to the Principal Dr. B. I. Khadakbhavi, Dean of P. G. Department Dr. B. M. Patil and staff of MBES's College of Engineering, Ambajogai for help in carrying out this research work at the institute.

References

[1]. Bajaj R., Chaudhary S., "Signature Verification using multiple neural classifiers", Pattern recognition society 30,(1996),1-7
[2]. Baltzakis H., Papamarkos N., "A signature verification technique based on two stage classifier," Engineering applications of artificial science 14, (1998), 95-103.
[3]. Brault J., Plamondon R., "Segmenting handwritten signatures at their perceptually important points," IEEE sanctions on pattern analysis and machine intelligence (1993),Vol 15.,pp. 953-957.
[4]. Hanmandlu M., Madasu V.K.,Madasu S. "Neuro Fuzzy approaches to signature verification," Second national analysis on Document analysis and recognition (2003)
[5]. Haykin S., "Neural Networks A comprehensive foundation," Macmillan college publishing (1994)
[6]. Huang K.,Yan H. "Online signature verification based on Geometric Feature Extraction and Neural Network Classification," Pattern Recognition society , (/1996),9-17.

[7]. Kiet T.H., Palaniappan R.,Raveendran P.,Takeda F. "Signature verification system using Pen Pressure for internet and E-commerce applications," ISSRE (2001), International symposium on software reliability engineering, Hong Kong,(2001)23
[8]. Murshed N.A.,Bortolozzi F.,Sabourin R. "Online signature verification using fuzzy ARTMAP neural network," International Conference on neural networks,(1995),Perth,Australia,(1995)
[9]. Oz C.,Ercal F.,Demir Z. "Signature recognition and verification with an ANN," Inter-national Conference on Electrical and Electronics Enmgineering ,(2003), Bursa
[10]. Parizeu M., Plamondon R., "A comparative analysis of regional correlating dynamic time warping and skeletal tree matching for signature veri_cation," IEEE transaction on pattern analysis and machine intelligence (1990), pp. 710-717.
[11]. Yildirim T.,Ozyilmaz L., "Dimensionality reduction in conic section Function neural network ," Sadhana academy proceedings in Engineering sciences, 2 (2002),675-683.
[12]. Yildirim T., "Development of conic section function Neural network in software and analogue hardware," Ph.D.Thesis,(1997).
[13]. Qui Y.,Hunt B., "Signature verification using global and grid features", Pattern recognition 27, 1 (1994), 1621-1629.
[14]. Han K.,Sethi I. "Handwritten signature retrieval and identification," Pattern recognition letters (1996), pp. 83-90.
[15]. Akban M., Lim Y., "online signature verification using thickened templates," COM-CON, 3 (1995).
[16]. Droughard j.,Sabourin R.,Godbout M. "A neural network approach to online Signature verification using directional pdf," Pattern Recognition , 11 (1996), 415-424.
[17]. Lee L., Berger T. "Reliable online signature verification system," IEEE transactions on Pattern Analysis and Machine learning 18 (1996), 643-647.
[18]. Pandya A., Robert B. M., "Pattern recognition in neural networks," CRC Press and IEEE press (1995),

Sumedha Tanajirao Panchal "Offline signature verification based on geometric feature extraction using artificial neural network. "IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) 13.3 (2018): 53-59.