International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 1– No.2, January 2012 – www.ijais.org

Handwritten Signature Verification using Neural Network

Ashwini Pansare
Assistant Professor in Computer Engineering
Department, Mumbai University, India

Shalini Bhatia
Associate Professor in Computer Engineering
Department, Mumbai University, India

ABSTRACT

A number of biometric techniques have been proposed for personal identification in the past. Among the vision-based ones are face recognition, fingerprint recognition, iris scanning and retina scanning. Voice recognition or signature verification are the most widely known among the non-vision based ones. As signatures continue to play an important role in financial, commercial and legal transactions, truly secured authentication becomes more and more crucial. A signature by an authorized person is considered to be the “seal of approval” and remains the most preferred means of authentication. The method presented in this paper consists of image prepossessing, geometric feature extraction, neural network training with extracted features and verification. A verification stage includes applying the extracted features of test signature to a trained neural network which will classify it as a genuine or forged.

Keywords

Biometrics, error back propagation algorithm, center of mass, neural network, and normalized area of signature.

1. INTRODUCTION

As signature is the primary mechanism both for authentication and authorization in legal transactions, the need for efficient auto-mated solutions for signature verification has increased [1].Unlike a password, PIN, PKI or key cards – identification data that can be forgotten, lost, stolen or shared – the captured values of the handwritten signature are unique to an individual and virtually impossible to duplicate. Signature verification is natural and intuitive. The technology is easy to explain and trust. The primary advantage that signature verification systems have over other type’s technologies is that signatures are already accepted as the common method of identity verification [2].

A signature verification system and the techniques used to solve this problem can be divided into two classes Online and Off-line [3].On-line approach uses an electronic tablet and a stylus connected to a computer to extract information about a signature and takes dynamic information like pressure, velocity, speed of writing etc. for verification purpose. Off-line signature verification involves less electronic control and uses signature images captured by scanner or camera. An off-line signature verification system uses features extracted from scanned signature image. The features used for offline signature verification are much simpler. In this only the pixel image needs to be evaluated. But, the off-line systems are difficult to design as many desirable characteristics such as the order of strokes, the velocity and other dynamic information are not available in the off-line case [4, 5]. The verification process has to wholly rely on the features that can be extracted from the trace of the static signature images only.

Vigorous research has been pursued in handwriting analysis and pattern matching for a number of years. In the area of Handwritten Signature Verification (HSV), especially offline HSV, different technologies have been used and still the area is being explored. In this section we review some of the recent papers on offline HSV. The approaches used by different researchers differ in the type of features extracted, the training method, and the classification and verification model used.

1.1 Hidden Markov Models Approach

Hidden Markov Model (HMM) is one of the most widely used models for sequence analysis in signature verification. Handwritten signature is a sequence of vectors of values related to each point of signature in its trajectory. Therefore, a well chosen set of feature vectors for HMM could lead to the design of an efficient signature verification system. These Models are stochastic models which have the capacity to absorb the variability between patterns and their similarities. In HMM stochastic matching (model and the signature) is involved. This matching is done by steps of probability distribution of features involved in the signatures or the probability of how the original signature is calculated. If the results show a higher probability than the test signatures probability, then the signatures is by the original person, otherwise the signatures are rejected.

In paper [6], a system is introduced that uses only global features. A discrete random transform which is a sinograph is calculated for each binary signature image at range of $0 - 360$, which is a function of total pixel in the image and the intensity per given pixel calculated using non overlapping beams per angle for X number of angles. Due to this periodicity, it is shift, rotation and scale invariant. A HMM is used to model each writer signature. The method achieves an AER of 18.4% for a set of 440 genuine signatures from 32 writers with 132 skilled forgeries.

1.2 Neural Networks Approach

The main reasons for the widespread usage of neural networks (NNs) in pattern recognition are their power and ease of use. A simple approach is to firstly extract a feature set representing the signature (details like length, height, duration, etc.), with several samples from different signers. The second step is for the NN to learn the relationship between a signature and its class (either “genuine” or “forgery”). Once this relationship has been learned, the network can be presented with test signatures that can be classified as belonging to a particular signer. NNs therefore are highly suited to modeling global aspects of handwritten signatures.

The proposed system in [7] uses structure features from the signatures contour, modified direction feature and additional features like surface area, length skew and centroid feature in which a signature is divided into two halves and for each half a position of the centre of gravity is calculated in reference to the horizontal axis. For classification and verification two approaches are compared the Resilient Back propagation (RBP) neural network and Radial Basic Function(RBF) using a database of 2106 signatures containing 936 genuine and 1170 forgeries. These two classifiers register 91.21% and 88 % true verification respectively.

1.3 Template matching approach

Fang et al. [8] proposed two methods for the detection of skilled forgeries using template matching. One method is based on the optimal matching of the one-dimensional projection profiles of the signature patterns and the other is based on the elastic matching of the strokes in the two-dimensional signature patterns. Given a test signature to be verified, the positional variations are compared with the statistics of the training set and a decision based on a distance measure is made. Both binary and grey-level signature images are tested. The average verification error rate of 18.1% was achieved when the local peaks of the vertical projection profiles of grey-level signature images were used for matching and with the full estimated covariance matrix incorporated.

1.4 Statistical approach

Using statistical knowledge, the relation, deviation, etc between two or more data items can easily be found out. To find out the relation between some set of data items we generally follow the concept of Correlation Coefficients. In general statistical usage refers to the departure of two variables from independence. To verify an entered signature with the help of an average signature, which is obtained from the set of, previously collected signatures, this approach follows the concept of correlation to find out the amount of divergence in between them.

A unique method is introduced in [9]. In this approach various features are extracted which include global features like image gradient, statistical features derived from distribution of pixels of a signature and geometric and topographical descriptors like local correspondence to trace of the signature. The classification involves obtaining variations between the signatures of the same writer and obtaining a distribution in distance space. For any questioned signature the method obtains a distribution which is compared with the available known and a probability of similarity is obtained using a statistical Kolmorogorv-Smirnov test. Using only 4 genuine samples for learning, the method achieves 84% accuracy which can be improved to 89% when the genuine signature sample size is increased. This method does not use the set of forgery signatures in the training/learning.

1.5 Support Vector Machine

Support Vector Machines (SVMs) are machine learning algorithms that uses a high dimensional feature space and estimate differences between classes of given data to generalize unseen data. The system in [10] uses global, directional and grid features of the signature and SVM for classification and verification. The database of 1320 signatures is used from 70 writers. 40 writers are used for training with each signing 8 signatures thus a total of 320 signatures for training. For initial testing, the approach uses 8 original signatures and 8 forgeries and achieves FRR 2% and FAR 11%.

Contribution:

In this paper we present a model in which neural network classifier is used for verification. Signatures from database are pre-processed prior to feature extraction. Features are extracted from pre-processed signature image. These extracted features are then used to train a neural network. In verification stage, on test signatures pre-processing and feature extraction is performed. These extracted features are then applied as input to a trained neural network which will classify it as a genuine or forged signature.

Organization of the paper: The rest of the paper is organized as follows. In section 2, the signature verification model is described. In section 3, the algorithm is presented .Results generated by the system is presented in section 4 and concluded in section 5.

2. METHODOLOGY

In this section, block diagram of system is discussed. Fig. 1 gives the block diagram of proposed signature verification system which verifies the authenticity of given signature of a person. The design of a system is divided into two stages:

1) Training stage 2) Testing stage

A training stage consist of four major steps 1) Retrieval of a signature image from a database 2) Image pre-processing 3) Feature extraction 4) Neural network training

A testing stage consists of five major steps 1) Retrieval of a signature to be tested from a database 2) Image pre-processing 3) Feature extraction 4) Application of extracted features to a trained neural network 5) Checking output generated from a neural network.

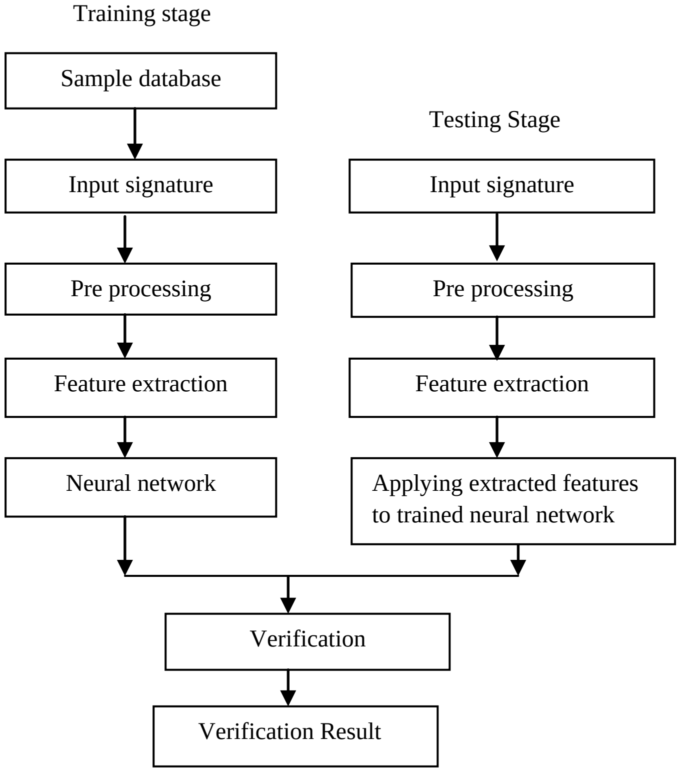

Fig 1: Block Diagram of Handwritten Signature Verification System using NN.

Fig. 2 shows one of the original signature image taken from a database and all the subsequent figures show the resultant signature image obtained after performing the steps mentioned in an algorithm.

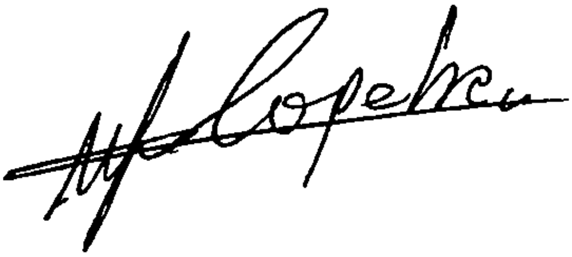

Fig 2: Signature image from the database

2.1 Pre-processing

The pre processing step is applied both in training and testing phases. Signatures are scanned in gray. The purpose in this phase is to make signature standard and ready for feature extraction. The pre-processing stage improves quality of the image and makes it suitable for feature extraction [11]. The prepossessing stage includes

2.1.1 Converting image to binary

A gray scale signature image is converted to binary to make feature extraction simpler.

2.1.2 Image resizing

The signatures obtained from signatory are in different sizes so, to bring them in standard size, resizing is performed, which will bring the signatures to standard size 256*256 as shown in Fig. 3.

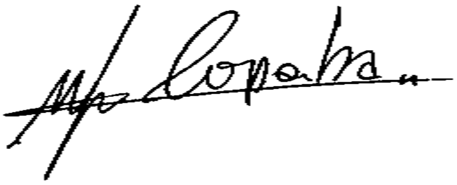

Fig. 3 Signature image after resizing

2.1.3 Thinning

Thinning makes the extracted features invariant to image characteristics like quality of pen and paper. Thinning means reducing binary objects or shapes to strokes that are single pixel wide. Fig. 4 shows thinned signature image.

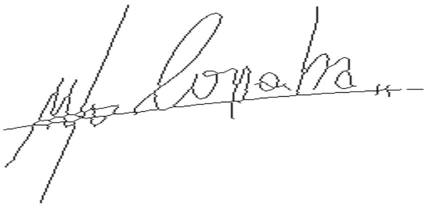

Fig 4: Signature image after Thinning

2.1.3 Bounding box of the signature:

In the signature image, construct a rectangle encompassing the signature. This reduces the area of the signature to be used for further processing and saves time. Fig. 5 shows signature enclosed in a bounding box.

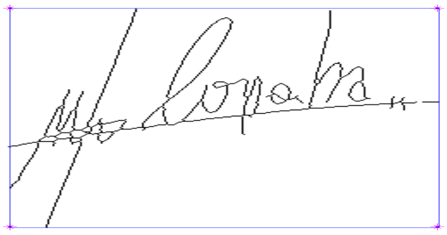

Fig 5: Signature image with a bounding box

2.2 Feature Extraction

The choice of a powerful set of features is crucial in signature verification systems. The features that are extracted in this phase are used to create a feature vector. A feature vector of dimension 24 has been used to uniquely characterize a candidate signature. These features are extracted as follows:

1) Maximum horizontal and vertical histogram

Horizontal histogram is calculated by going through each row of the signature image and counting number of black pixels. A row with maximum number of black pixels is recorded as maximum horizontal histogram. Similarly, a vertical histogram is calculated by going through each column of the signature image and finding a column with maximum number of black pixels.

2) Center of mass

Split the signature image in two equal parts and find center of mass for individual parts.

3) Normalized area of signature

It is the ratio of area of signature image to the area of signature enclosed in a bounding box. Area of a signature is the number of pixels comprising it.

$$Normalized\ area = \frac{Signature\ \ Area}{Area\ \ enclosed\ \ in\ a\ bounding\ \ box} \qquad \text{Eq. (1)}$$

4) Aspect Ratio

It is the ratio of width of signature image to the height of the image. This is done because width or height of person’s signature may vary but its ratio remains approximately equal.

$$Aspect\ Ratio = \frac{width\ of\ signature\ \ in\ a\ bounding\ \ box}{Height\ \ of\ signature\ \ in\ a\ bounding\ \ box} \qquad \text{Eq. (2)}$$

5) Tri surface feature

Two different signatures may have same area .so; to increase the accuracy of the features three surface feature has been used. In this, a signature is divided into three equal parts and area for each part is calculated. Eq. (1) is then used to calculate normalized area of each part. Figure (6) shows tri surface feature.

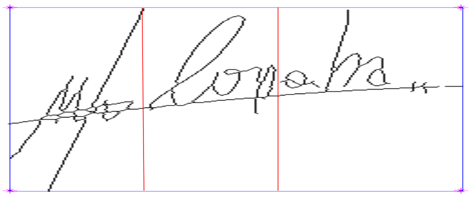

Fig 6: Tri surface feature

6) The six fold surface feature

Divide a signature in three equal parts and find bounding box for each part. Then calculate centre of mass for each part. Draw a horizontal line passing through centre of mass of each part and calculate area of signature above and below centre of mass within a bounding box. This provides six features.

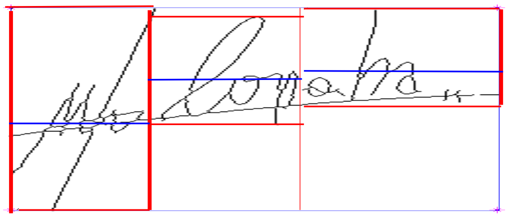

Fig 7: Six fold surface feature

7) Transition feature

Traverse a signature image in left to right direction and each time there is a transition from 1 to 0 or 0 to 1, calculate a ratio between the position of transition and the width of image traversed and record it as a feature. Repeat a same process in right to left, top to bottom and bottom to top direction. Also calculate total number of 0 to 1 and 1 to 0 transitions. This provides ten features.

2.2.4 Creation of feature vector

A feature vector of size 24 is formed by combining all the extracted features as discussed in section 2.2.

2.2.5 Training a neural network

Extracted 24 feature points are normalized to bring them in the range of 0 to 1.These normalized features are applied as input to the neural network.

2.3 Verification

In the verification stage, a signature to be tested is pre-processed and feature extraction is performed on pre processed test signature image as explained in section 2.2 to obtain feature vector of size 24. After normalizing a feature vector it is fed to the trained neural network which will classify a signature as a genuine or forged.

3. ALGORITHM

Table 1 gives algorithm for the handwritten signature verification system in which neural network is used for verifying the authenticity of signatures.

TABLE 1 Algorithm for Handwritten Signature Verification using Neural Network

```
Input: signature from a database
Output: verified signature classified as genuine or forged.
1. Retrieval of signature image from a database.
2. Preprocessing the signatures.
    2.1 Converting image to binary.
    2.2 Image resizing.
    2.3 Thinning.
    2.4 Finding bounding box of the signature.
3. Feature extraction
    3.1 Maximum horizontal and vertical histogram
    3.2 Centre of mass
    3.3 Normalized area of signature
    3.4 Aspect ratio
    3.5 The tri surface feature
    3.6 The six fold surface feature
    3.7 Transition feature
4. Creation of feature vector by combining extracted features.
5. Normalizing a feature vector.
6. Training a neural network with a normalized feature vector.
7. Steps 1 to 5 are repeated for testing signatures.
8. Applying normalized feature vector of test signature to
   trained neural network.
9. Using a result generated by the output neuron of the neural
   network declaring a signature as a genuine or forged.
```

4. RESULTS AND DISCUSSION

For training and testing of the system many signatures are used. The results given in this paper are obtained using the “Grupo de Procesado Digital de Senales” (GPDS) signature database [12]. The results provided in this research used a total of 1440 signatures. Those 1440 signatures are comprised of 30 sets (i.e. from 30 different people) and, for each person there are 24 samples of genuine signatures and 24 samples of forgeries. Figure 6 shows some of the signatures in the GPDS database. To train the system, a subset of this database was taken comprising of 19 genuine samples taken from each of the 30 different individuals and 19 forgeries made by different person for one signature. The features extracted from 19 genuine signatures and 19 forged signatures for each person were used to train a neural network. The architecture of neural network used has input layer, hidden layer and output layer [13]. Number of neurons in the input layer are 24, 24 neurons in the hidden layer and one neuron in the output layer. After applying a feature vector of test signature if the output neuron generates value close to +1 test signature is declared as genuine or if it generates value close to -1 it is declared as forged.Fig.8 shows performance graph of the training a two layer feed forward neural network using Error Back Propagation Algorithm (EBPTA).

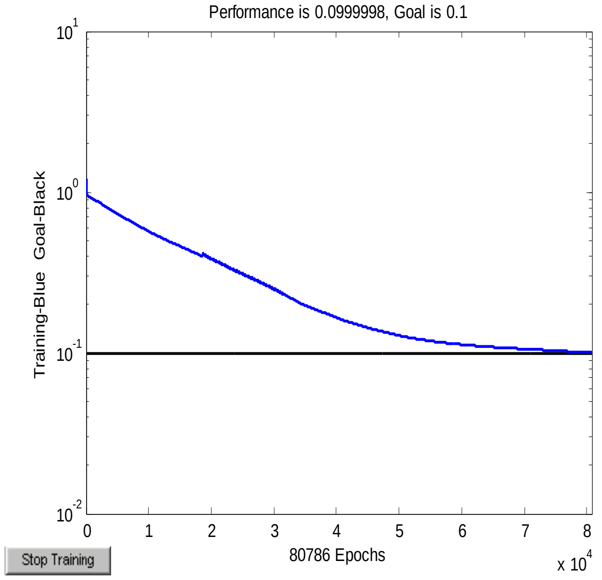

Fig. 8 Performance graph of handwritten signature verification using neural network.

4.1 Performance Analysis

False Acceptance Rate (FAR), False Rejection Rate (FRR) and Correct Classification Rate (CCR) are the three parameters used for measuring performance of system. FAR is calculated by eq. (3), FRR is calculated by eq. (4) and CCR is calculated by eq. (5).

$$FAR = \frac{Number\ \ of\ forgeries\ \ accepted}{Number\ \ of\ forgeries\ \ tested} * 100 \qquad \text{Eq. (3)}$$

$$FRR = \frac{Number\ \ of\ originals\ \ rejected}{Number\ \ of\ originals\ \ tested} * 100 \qquad \text{Eq. (4)}$$

$$CCR = \frac{Number\ \ of\ \ samples\ \ correctly\ \ recognized}{Number\ \ of\ samples\ \ tested} * 100 \qquad \text{Eq. (5)}$$

4.2 Results of Testing Neural network with trained samples

The genuine and forged signature samples used for training neural network is applied in the testing phase to check whether neural network classifies it correctly as genuine or forged. This is called Recall. The result of recall is as shown in Table 2.

TABLE 2 Result of Testing Neural Network with Trained Signature Samples.

Samples presented	Genuine	Forged	CCR in Recall
570 genuine	570	0	100%
570 forged	0	570	100%

When the neural network was presented with 570 genuine signatures from 30 different persons, it classified all 570 genuine signatures as genuine and when 570 forged signatures from 30 different persons were applied it recognized all 570 signatures as forgeries. Thus FAR and FRR of the system is 0%.Hence, Correct Classification Rate (CCR) is 100% for Recall.

4.3 Result of testing neural network with new signature samples from database

When the signatures samples not used for training neural network are applied as test signatures to the trained neural network, it is called Generalization. The result of generalization is shown in Table 3.

TABLE 3 Result of Testing Neural Network with New Signatures Samples from Database.

Samples presented	Genuine	Forged	FAR	FRR	CCR In Generalization
150 genuine	120	30	-	20%	82.66%
150 forged	22	128	14.66 %	-	

The neural network when presented with 150 genuine signatures from 30 different persons classified 120 signatures out of 150 as genuine and 30 signatures as forgeries. Thus FRR of the system is 20% .When 150 forged signatures were given as input to neural network, it classified 22 signatures as genuine and 128 as forgeries. Thus FAR of the system is 14.66%. And hence the Correct Classification Rate is 82.66% for generalization.

5. CONCLUSION

This paper presents a method of handwritten signature verification using neural network approach. The method uses features extracted from preprocessed signature images. The extracted features are used to train a neural network using error back propagation training algorithm. As shown in Table 2 CCR in recall is 100%. The network could classify all genuine and forged signatures correctly. When the network was presented with signature samples from database different than the ones used in training phase, out of 300 such signatures (150 genuine and 150 forged) it could recognize 248 signatures correctly. Hence, the correct classification rate of the system is 82.66% in generalization as shown in Table 3.

6. REFERENCES

[1] Prasad A.G. Amaresh V.M. "An offline signature verification system"

[2] Prashanth CR,KB Raja,KR Venugopal, LM Patnaik,"Standard Scores Correlation based Offline signature verification system", International Conference on advances in computing, control and telecommunication Technologies 2009

[3] R. Plamondon and S.N. Srihari, "Online and Offline Handwriting Recognition: A Comprehensive Survey", IEEE Tran. on Pattern Analysis and Machine Intelligence, vol.22 no.1, pp.63-84, Jan.2000.

[4] J Edson, R. Justino, F. Bortolozzi and R. Sabourin, "An off-line signature verification using HMM for Random,Simple and Skilled Forgeries", Sixth International Conference on Document Analysis and Recognition, pp.1031-1034, Sept.2001. 211-222, Dec.2000.

[5] J Edson, R. Justino, A. El Yacoubi, F. Bortolozzi and R. Sabourin, "An off-line Signature Verification System Using HMM and Graphometric features", DAS 2000

[6] B. Herbst. J. Coetzer. and J. Preez, "Online Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model," *EURASIP.Journal on Applied Signal Processing,* vol. 4, pp. 559–571, 2004.

[7] M. Blumenstein. S. Armand. and Muthukkumarasamy, "Off-line Signature Verification using the Enhanced Modified Direction Feature and Neural based Classification," *International Joint Conference on Neural Networks*, 2006.

[8] 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.

[9] H. S. Srihari and M. Beall, "Signature Verifcation Using Kolmogrov Smirnov Statistic,"*Proceedings of International Graphonomics Society,Salemo Italy* , pp. 152–156, june,2005.

[10] T.S. enturk. E. O¨ zgunduz. and E. Karshgil, " Handwritten Signature Verification Using Image Invariants and Dynamic Features," *Proceedings of the 13*th *European Signal Processing Conference EUSIPCO 2005,Antalya Turkey*, 4th-8th September, 2005.

[11] Ramachandra A. C ,Jyoti shrinivas Rao"Robust Offline signature verification based on global features" IEEE International Advance Computing Conference ,2009.

[12] Martinez, L.E., Travieso, C.M, Alonso, J.B., and Ferrer, M. *Parameterization of a forgery Handwritten Signature Verification using SVM.* IEEE 38thAnnual 2004 International Carnahan Conference on Security Technology ,2004 PP.193-196

[13] "An Introduction to Artificial Neural Systems" by Jacek M. Zurada, West Publishing Company 1992.