Off-line Signature Verification Using Neural Network

Ashwini Pansare, Shalini Bhatia

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 ti 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 verifcation. 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.

Index Terms- Biometrics, Error back propogation algorithm, Geometric features, Horizontal and vertical splitting, Neural network

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 [6].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 [1].

A signature verification system and the techniques used to solve this problem can be divided into two classes Online and Off-line [5].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 [3,4]. The verification process has to wholly rely on the features that can be extracted from the trace of the static signature images only.

Contribution:
In this paper we present a model in which neural network classifier is used for verification. Signatures from database are preprocessed prior to feature extraction. The geometric features are extracted from preprocessed signature image. These extracted features are then used to train a neural network.In verification stage, on test signatures preprocessing 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 preprocessing 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 preprocessing 3) Feature extraction 4) Application of extracted features to a trained neural network 5) checking output generated from a neural network.

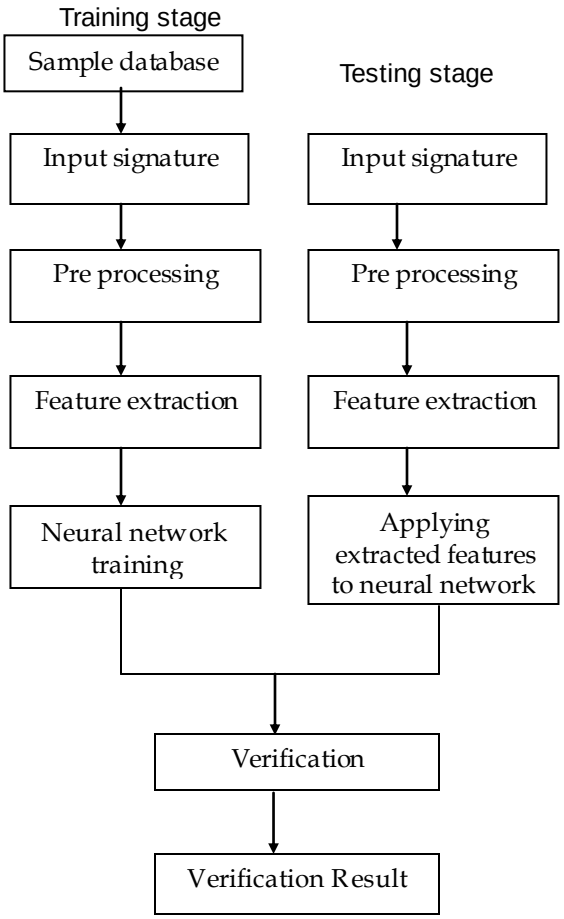


Fig. 1: Block Diagram of Offline Signature Verification using NN

Fig. 2 shows signature image taken from a database.

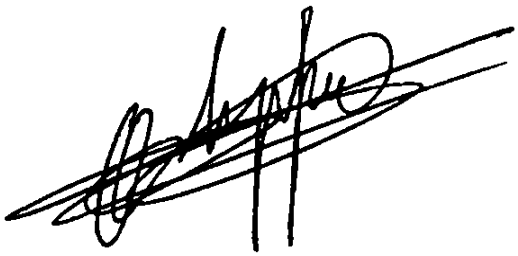


Fig. 2 Signature image from a database

2.1 Pre-processing

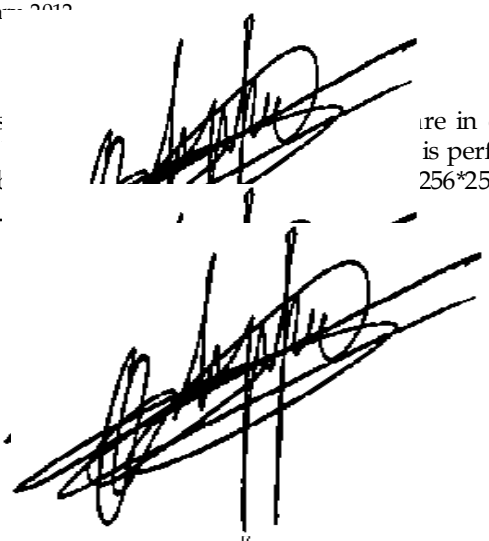
The pre processing step is applied both in training and testing phases. Signatures are scanned in gray. The purpose in this phase is to make signature standard and ready for feature extraction. The preprocessing stage improves quality of the image and makes it suitable for feature extraction [2]. The 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

The s ıre in different sizes so,to is performed, which will l 256*256 as shown in fig. 3.



:e 256*256

2.1.3

Thinı ures invariant to imag and paper. Thinning mean s to strokes that are singl ıature image.

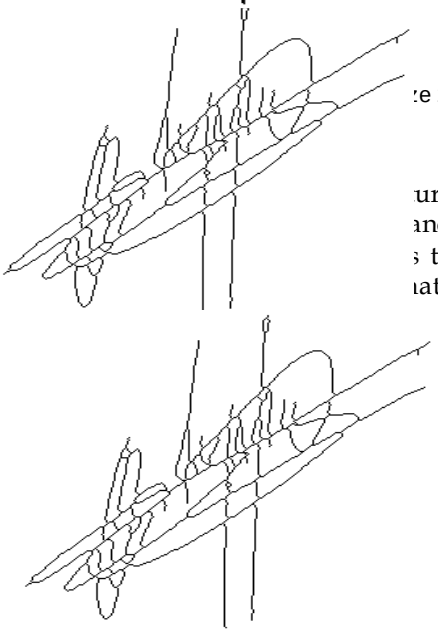


Fig.4 signature image after thinning

2.1.4 Bounding box of the signature:

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

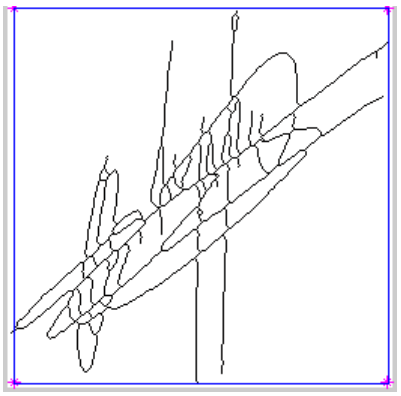


Fig.5 Signature image with a bouding box

2.2 Feature Extraction

The choice of a powerful set of features is crucial in signature verification systems. The features that are extracted from this phase are used to create a feature vector. We use a feature vector of dimension 60 to uniquely characterize a candidate signature. These features are geometrical features which mean they are based on the shape and dimensions of the signature image. These features are extracted as follows:

2.2.1 Geometric Centre:

Traverse a signature image to find a point (row and column number in the image) at which no of black pixels is half of the total no of black pixels in the image [7].

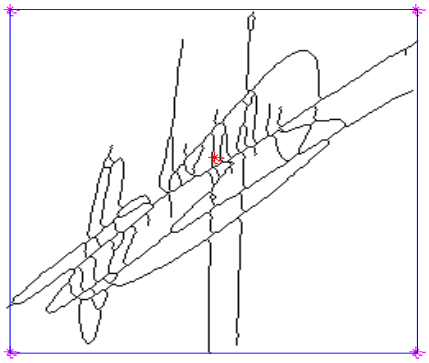


Fig.6 Geometric center in signature image is represented by red marker(*).

2.2.2 Feature extracted using vertical splitting:

Split the signature image with vertical line passing through its geometric centre to get left and right part of signature .Find geometric centre for left and right part. Divide the left part with horizontal line passing through its geometric center to get top and bottom part. Find the geometric centers for top and bottom parts of left part correspondingly. Similarly, the right part is split with a horizontal line at its geometric center to get top and bottom parts of right part correspondingly. Find geometric center for the top and bottom of the right part. Each part of the image is again split using same method to obtain thirty vertical feature points as shown in Figure 7.

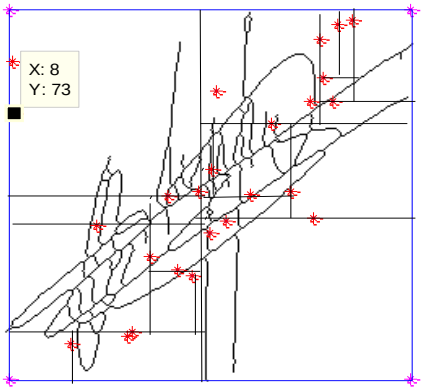


Fig. 7 Signature image after vertical splitting

2.2.3 Feature extracted using horizontal splitting

Split the signature image with horizontal line passing through its geometric centre to get top and bottom part of signature. Find geometric centre for top and bottom part. Divide the top part with vertical line passing through its geometric center to get left and right part. Find the geometric centers for left and right parts of top part correspondingly. Similarly, the bottom part is split with a vertical line at its geometric center to get left and right parts of bottom part correspondingly. Find geometric center for the left and right of the bottom part. Each part of the image is again split using same method to obtain thirty horizontal feature points as shown in Figure 8.

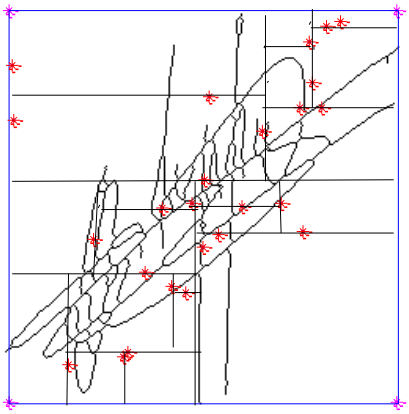


Fig. 8 Signature Image after horizontal splitting

2.2.4 Creation of feature vector:

A feature vector of size 60 is formed using 30 features extracted from vertical and horizontal splitting each.

2.3 Training a neural network

Extracted 60 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.

2.4 Verification

In the verification stage, a signature to be tested is preprocessed and feature extraction is performed on pre processed test signature image as explained in 2.2 to obtain feature vector of size 60. 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 offline signature verification system in which neural network is used for verifying the authenticity of signatures.

TABLE 1
Algorithm for Offline Signature Verification using Neural Network

Input: signature from a database
Output: verified signature classified as genuine or forged.
1. Retrieval of signature image from 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 Extracting features using vertical splitting.
   3.2 Extracting features using horizontal splitting.
4. Creation of feature vector by combining extracted features Obtained from horizontal and vertical splitting.
5. Normalizing a feature vector.
6. Training a neural network with 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 result generated by the output neuron of the neural network declaring signature as genuing 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 [8]. 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 [9]. Number of neurons in the input layer are 120 for 60 feature points as each feature point has a row and a column number, 120 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 Propogation Algorithm (EBPTA).

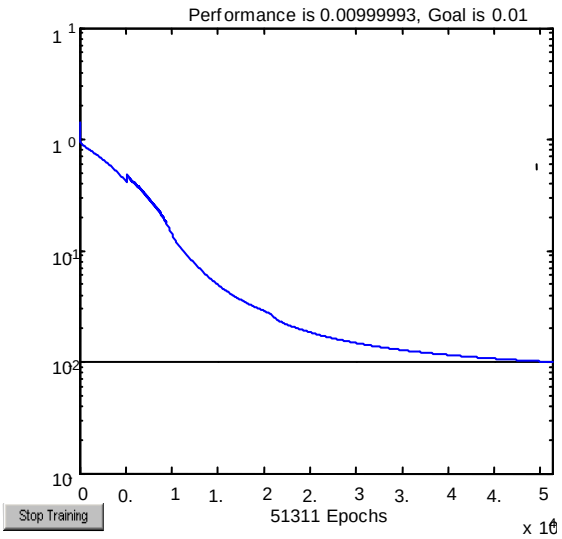


Fig.8 Performance graph of trainning a NN using EBPTA.

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 (1), FRR is calculated by (2) and CCR is calculated by (3).

$$FAR = \frac{\text{Number of forgeries accepted}}{\text{Number of forgeries tested}} * 100 \quad (1)$$

$$FRR = \frac{\text{Number of originals rejected}}{\text{Number of original tested}} * 100 \quad (2)$$

$$CCR = \frac{\text{Number of samples correctly Recocgnized}}{\text{Number of samples tested}} * 100 \quad (3)$$

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.

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.

TABLE 2
Result of Testing Neural Network with Trained Signatue Samples

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

4.3 Result of testing neural network with new 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 Signtaure Samples from Database.

Samples prsented	Genuine	Forged	FAR	FRR	CCR In Generalization
150 genuine	125	25	-	16.7 %	85.7%
150 forged	18	132	12%	-	

The neural network when presented with 150 genuine signatures from 30 different persons classified 125 signatures out of 150 as genuine and 25 signatures as forgeries. Thus FRR of the system is 16.7% .When 150 forged signatures were given as input to neural network, it classified 18 signatures as genuine and 132 as forgeries. Thus FAR of the system is 12%. And hence the Correct Classification Rate is 85.7% for generalization.

5. Conclusion

This paper presents a method of offline signature verification using neural network approach. The method uses geometric 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 257 signatures correctly. Hence, the correct classification rate of the system is 85.7% in generalization as shown in Table 3.

REFERENCES

[1] Bradley Schafer, Serestina Viriry "An Offline Signature Verification system" IEEE International conference on signals and image processing application, 2009.

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

[3] 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.

[4] 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*

[5] 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.

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

[7] B. Fang, C.H. Leung, Y.Y. Tang, K.W. Tse, P.C.K. Kwok and Y.K. Wong, "Off-line signature verification by the tracking of feature and stroke positions", *Pattern Recognition* 36, 2003, pp. 91–101.

[8] 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

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