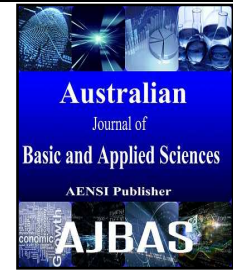




ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Signature Verification Using Neural Networks And Image Processing

Rahul Rao and Dr. Jagadish S Kallimani

M.S Ramaiah Institute of Technology, Bangalore, Karnataka, India.

ARTICLE INFO

Article history:

Received 1 December 2015

Accepted 31 December 2015

Available online 10 January 2016

Keywords:

Biometric Authentication, Center of Mass, Neural Networks, Normalized Area.

ABSTRACT

Signature verification is a long standing biometric authentication technique used to determine the identity of a human being. It's a non-vision based technique. Face recognition, iris recognition are among the vision based techniques. Signature is the easiest and simplest method of authentication. The method used in this paper includes the image pre-processing, feature extraction, training and testing the neural network. Image with minimum error will be classified as genuine or else it is forged.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: Rahul Rao and Dr. Jagadish S Kallimani., Signature Verification Using Neural Networks And Image Processing. *Aust. J. Basic & Appl. Sci.*, 9(36): 490-494, 2015

INTRODUCTION

Signature as aforementioned is a primary mechanism to authenticate and authorize a person. Unlike passwords, PIN etc. a signature cannot be forgotten, stolen or copied very easily (Prasad, A.G., V.M. Amaresh.). The advantage of signatures is that they are already an accepted method to identify a person (Jain, A.K., A. Ross and S. Pankanti, 2006).

Signatures are mainly used in banks, financial institutions etc., and hence the signature verification techniques are needed in these fields mostly. Pixel matching is also another technique but the efficiency of the neural technique is much more, hence we have chosen the former in our venture. Signature verification is of 2 types: Online and offline. Online technique uses a specialized biometric device which takes into account the pressure, velocity, timestamp and the amount of pen-ups while signing. The Off-line technique are less efficient as features such as velocity, order of strokes, timestamp cannot be calculated (Prashanth, C.R., *et al.*, 2009; Plamondon, R. and S.N. Srihari, 2000). Different models such as Hidden Markov Model and Dynamic Time-Warping is present to design an algorithm for analysis. This approach wholly depends on the feature such as the normalized area extracted from the images to compare and conclude.

1.1 Hidden Markov Model:

Hidden Markov Model (HMM) is the most widely used models for image analysis in signature recognition. It converts the handwritten signature into a set of feature vectors using which the image

will be tested. Therefore, a good feature selector will yield good results.

HMM is considered as sequence generator. When we visit a state, we emit a residue from the state's emission probability distribution. Later we choose which state to visit next according to the state's transition probability distribution. The model thus generates two strings of information (Edson, J., *et al.*, 2000) One is the underlying *state path* (the labels), as we transition from state to state. Another is the *observed sequence* (the DNA), each residue being emitted from one state in the state path. The state path is a Markov chain and the state path is hidden, hence it's a *Hidden Markov Chain*.

1.2 Statistical Approach:

Using statistics, the deviation, relation etc. can be calculated between two or more datasets which are in comparison (Herbst, B., J. Coetzer, and J. Preez, 2004). To implement this method we find out the Correlation coefficient mostly. A set of signatures are used as primary dataset and its data is calculated. Later the amount of divergence between the set of previously tested images and the image under consideration is calculated. This method yields promising results.

This paper aims to give the best possible recognition rate with the available database. Signatures are pre-processed and the features are extracted from the images. These features are then used to train the neural network. The verification phase compares the above features with the testing image and the image with minimum deviation is considered as recognized.

The paper is organized as: section 2 describes the system using a flow chart and existing systems. Section 3 which provide information about the pre-processing stages, followed by section 4 which describes feature extraction. Section 5 and Section 6 are results generated and the conclusions respectively.

2. Overview of the System:

A block diagram is used to describe the system. There are 2 stages:

- 1) Training stage
- 2) Testing stage

In the training stage, 1) Signature is retrieved from database 2) Pre-processing 3) Feature extraction 4) Training the neural network

In testing stage, we have 1) Retrieval of the image to be tested 2) Pre-processing 3) Feature extraction 4) Comparison of the values obtained by the neural network.

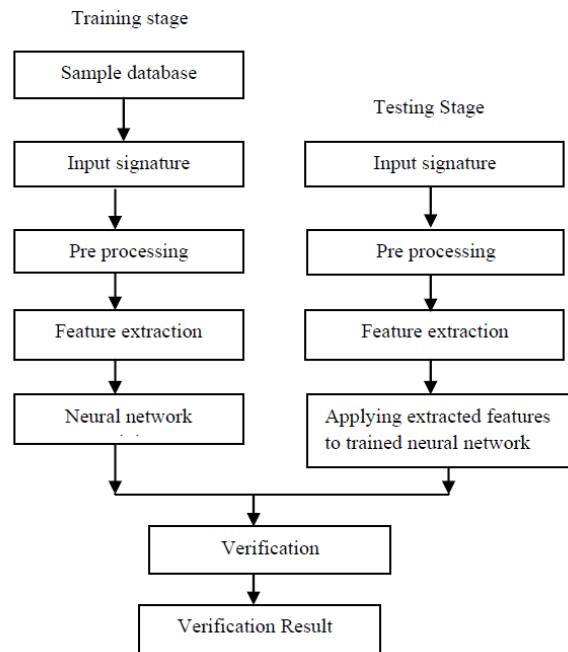


Fig. 1: Overview of the Signature Verification System

An example of a signature taken from the database will be used to explain the pre-processing and the feature extraction steps.



Fig. 2: An Example Image from the Database

3. Pre-processing:

There are many steps involved in pre-processing. They are:

Image Resizing:

The image retrieved from the database has to be resized to a standard size so that the comparison will be uniform (Ramachandra, A.C., 2009). We have resized the image to 256*256.



Conversion to Binary:

The image is converted to grayscale first and then converted to binary format for further processing.

Thinning:

The image from the database will be obtained using pen and paper hence some irrelevant features might be present. Thinning removes these features and makes the image ready for feature extraction.



Cropping of the Image:

The obtained image after thinning is cropped neatly so as to remove the unnecessary white spaces which take precious computation time. A box is constructed around the cropped image.

4. Feature Extraction:

The Extraction and selection of features play a very important role in the deciding the efficiency of the neural system (Viswanath, K. and R. Gunasundari, 2015). We consider a set of 30 features.

Center of Mass:

The center of mass of the whole image is calculated and it is noted down as a feature.

Normalized Area:

Normalized area is defined as the ratio of the area of the signature to the area of the bounded box.

$$\text{Normalized area} = \frac{\text{Area of the signature}}{\text{Area of the bounded image}} \quad (1)$$

Aspect Ratio:

Aspect ratio is the ratio of the width of the signature to the height of the signature. It generally remains uniform for a persons signature.

$$\text{Aspect Ratio} = \frac{\text{width of the signature}}{\text{height of the signature}} \quad (2)$$

Quadruple Partiton Area:

The signature in the bounding box is split into 4 parts and the normalized area of each part is calculated using Eq(1).

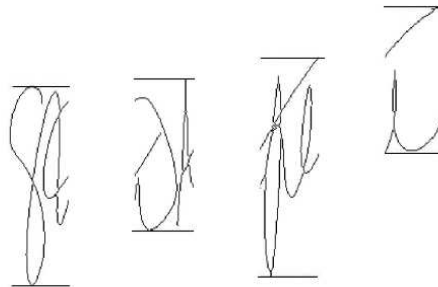


Fig. 3: Quadruple Partition Area

Eight fold Surface Area:

The signature which is split into four parts is now split into eight by using the center of mass. The

normalized area of each fold is calculated using Eq(1).



Fig. 4: Finding Center of Mass and Partitioning the Image

Transition Ratio:

The signature image is traversed from right to left. Whenever there is a pixel transition from 1 to 0 or 0 to 1, calculated the Transition ratio using Eq(3). Traverse the image from right to left, top to bottom and bottom to top and calculate the Transition ratio in each case. This gives us 16 more features.

$$\text{Transition Ratio} = \frac{\text{Position of pixel tansition}}{\text{width of the image traversed}} \quad (3)$$

These feature extraction mechanisms give 30 feature points for us to test the images.

Training of the neural system:

The aforementioned feature points are extracted for each image in the training set and the neural network is trained.

Testing of the neural system:

The values obtained by the training mechanism will be used to test and find out the error. The image with the minimum error will be identified as recognized.

Algorithm:

We conclude the pre-processing and feature extraction by writing an algorithm.

Input: Signature from database

Output: Verified signature classified as genuine or forged

Steps:

Retrieval of signature image from a database

Preprocessing of signatures

Image Resizing

Converting to image to binary

Thinning

Cropping of Image

Feature Extraction

Center of mass

Normalized area

Aspect ratio

Quadruple partition area

Eight fold surface area

Transition Ratio

Formulating a feature vector by combining extracted features

Standardizing a feature vector

Training a neural network with the standardized feature network

Repeat steps 1 to 5 with a standardized feature vector

Applying standardized feature vector of test signature to trained neural network

Using the result generated by the output neuron of the neural network declaring a signature as genuine or forged.

Table 1: Results of testing the neural network with trained signature samples

Samples considered	Genuine	Forgery	FAR	FRR	CRR
300 genuine	279	21	N/A	7%	93%
300 forgery	29	271	9.6%	N/A	90.3%

Results:

The training and testing is done using the database "SVC20EU", "COLLECTION2" database is used to do it. It consists of 20 genuine samples, 20 skilled forgeries and 40 genuine samples of 40 people respectively. Once a set of images are trained their values are used to calculate the error and this error classifies the image into whether it is a forgery or a genuine sample (LLLee, 1995).

Performance Parameters:

The False Acceptance Rate (FAR), False Rejection Rate (FRR) and Correct Classification Rate (CCR) are the three performance parameters that are used to determine the efficiency of a system (Ashwini Pansare).

$$FAR = \frac{\text{Number of forgeries accepted}}{\text{Number of forgeries tested}} * 100$$

$$FRR = \frac{\text{Number of originals rejected}}{\text{Number of originals tested}} * 100$$

$$CCR = \frac{\text{Number of samples correctly recognized}}{\text{Number of samples tested}} * 100$$

Results of testing the neural network with sample trained with Neural Network:

The system was trained with 600 samples consisting of both skilled forgeries as well as genuine signatures. The neural network classified all the 600 signatures correctly as genuine or forged.

Table 2: Results of testing the neural network with new signatures from the database

Samples considered	Genuine	Forgery	CCR
300 genuine	300	0	100%
300 forged	0	300	100%

Results of testing the neural network with new signatures from the database:

Signatures which were not used for training the neural network are applied as testing signatures to the trained neural network. 600 samples were of new signatures were considered. The results are as follows:

The total recognition rate of the neural network when signatures which were not trained are applied to the already trained neural network is 91.67%.

Conclusion:

This paper tries to give a way of extracting features from a given signature and recognize whether it's a forgery or not. Due to the database limitations we couldn't achieve a perfect recognition

rate but the methodology is implemented in a proper fashion.

The features are extracted and the samples are trained using the features. With a database which gives information about the timestamp, pressure would give perfect results (Martens, R. and L. Claesen, 1996).

Future Enhancements:

More features can be extracted so that the recognition rate of this method can be increased. Nowadays, IRIS recognition has replaced signature as it is more valid. So that can be implemented to provide better biometric analysis (Li Ma, et al., 2004). An online verification can be implemented so that we can use DCT to get a more

efficient system (Lejtman, D.Z. and S.E. George, 2001).

REFERENCES

- Ashwini Pansare, Shalini Bhatia, *Handwritten Signature Verification using Neural Network*, Edson, J., R. Justino, A. El Yacoubi, F. Bortolozzi and R. Sabourin, 2000. *An off-line Signature Verification System Using HMM and Graphometric features*, DAS.
- Herbst, B., J. Coetzer, and J. Preez, 2004. *Online Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model*, EURASIP Journal on Applied Signal Processing, 4: 559-571.
- Jain, A.K., A. Ross and S. Pankanti, 2006. *Biometrics: a tool for information security*, IEEE Transactions on Information Forensics and Security, 1(2): 125-143.
- Lejtman, D.Z. and S.E. George, 2001. *On-line handwritten signature verification using wavelets and back-propagation neural networks*, in Proceedings of 6th International Conference Document Analysis and Recognition (ICDAR-6), Seattle, WA, pp: 992-996.
- Li Ma, Tieniu Tan, Yunhong Wang and Dexin Zhang, 2004. *Efficient Iris Recognition by Characterizing Key Local Verifications*, IEEE Transactions on Image Processing, 13(6): 739-750.
- LLLee, 1995. *Neural approaches for human signature verification*, in proceedings of 3rd International Conference Document Analysis Recognition (ICDAR-3), IEEE Computer Society, Montreal, Canada, 1: 1055-1058.
- Martens, R. and L. Claesen, 1996. *On-line signature verification by dynamic time-warping*, in Proceedings of 13th International Conference on Pattern Recognition (ICPR96), Vienna, Austria, pp: 38-42.
- Plamondon, R. and S.N. Srihari, 2000. *Online and Offline Handwriting Recognition: A Comprehensive Survey*, IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(1): 63-84.
- Prasad, A.G., V.M. Amaresh, *An offline signature verification system*.
- Prashanth, C.R., K.B. Raja, K.R. Venugopal, L.M. Patnaik, 2009. *Standard Scores Correlation based Offline signature verification system*, International Conference on Advances in Computing, Control and Telecommunication Technologies.
- Ramachandra, A.C., 2009. *Jyoti Srinivas Rao Robust Offline signature verification based on global features*, IEEE International Advance Computing Conference.
- Viswanath, K. and R. Gunasundari, 2015. "Modified Distance Regularized Level Set Segmentation Based Analysis for Kidney Stone Detection", International Journal of Rough Sets and Data Analysis, 2(2): 22-39. IGI Global Publication, USA. DOI: 10.4018/ijrsda.2015070102.