Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 3 (2011) 155–161

Procedia Computer Science

www.elsevier.com/locate/procedia

WCIT 2010

Offline signature recognition using neural networks approach

Ali Karouni[a] *, Bassam Daya[b], Samia Bahlak[b]

[a] *Lebanese University, Ecole Doctorale des Sciences et de Technologie (EDST), LEBANON*
[b] *Lebanese University, Institute of Technology of Saida, LEBANON, P.O.B. 813*

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, Center of gravity, Eccentricity, Kurtosis and Skewness. 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. The details of preprocessing as well as the features depicted above are described throughout the discussion. Then artificial neural network (ANN) was used to verify and classify the signatures: exact or forged, and a classification ratio of about 93% was obtained under a threshold of 90%.The implementation details and simulation results are discussed in the thesis.

Selection and/or peer-review under responsibility of the Guest Editor.

Keywords: Offline Signature Recognition; Image Processing; Personal Verification; Neural Networks

1. 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

*Ali Karouni
E-mail address: ali_karoni@hotmail.com

doi:10.1016/j.procs.2010.12.027

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].

We approach the problem in two steps. Initially the scanned signature image is preprocessed to be suitable for extracting features. Then the preprocessed image is used to extract relevant geometric parameters that can distinguish forged signatures from exact ones using the ANN approach. Part2 deals with the preprocessing steps and explains the features that are extracted followed by ANN construction and training procedures in Part 3. Implementation details and simulation results are listed in Part 4. Finally the conclusions are drawn in Part 5.

2. Image Preprocessing and Features Extraction

We approach the problem in two steps. Initially, the scanned signature image is preprocessed to be suitable for extracting features. Then, the preprocessed image is used to extract relevant geometric parameters that can distinguish forged signatures from exact ones using the ANN approach.

2.1. Preprocessing[8]

The signature is first captured and transformed into a format that can be processed by a computer. Now it's ready for preprocessing. In preprocessing stage, the RGB image of the signature is converted into grayscale and then to binary image. The purpose of this phase is to make signatures ready for feature extraction. The preprocessing stage includes two steps: Color inversion, Filtering and Binarization.

2.1.1. Color Inversion[9]:

The true color image RGB is converted to the grayscale intensity image by eliminating the hue and saturation information while retaining the luminance.

Fig. 1. (a) A sample signature to be processed; (b) A Grayscale Intensity Image

A grayscale image is a data matrix whose values represent intensities within some range where each element of the matrix corresponds to one image pixel.

2.1.2. Image Filtering and Binarization[10],[11]:

Any image when resample is filtered by a low pass FIR filter. This is done to avoid aliasing. This aliasing occurs because of sampling the data at **a rate lower than twice the largest frequency component of the data. So a low pass filter will remove the image high** frequency components. And for this purpose the filter used.

Now the grayscale image is segmented to get a binary image of objects. In a binary image, each pixel assumes one of only two discrete values: 1 or 0. A binary image is stored as a logical array.

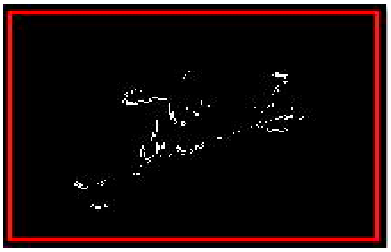
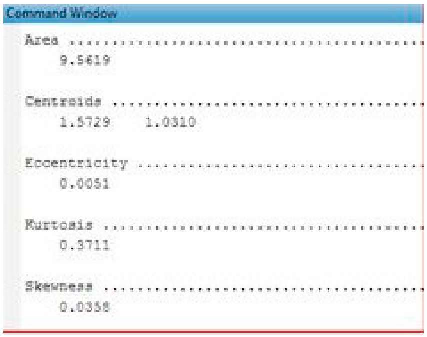


Fig. 2. Binary Image interpreting the bit value of 0 as black and 1 as white

2.2. Features Extraction

Features Extraction is the key to develop an offline signature recognition system. We use a set of five 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, Centroid Coordinates, Eccentricity, Kurtosis and Skewness [12],[13].

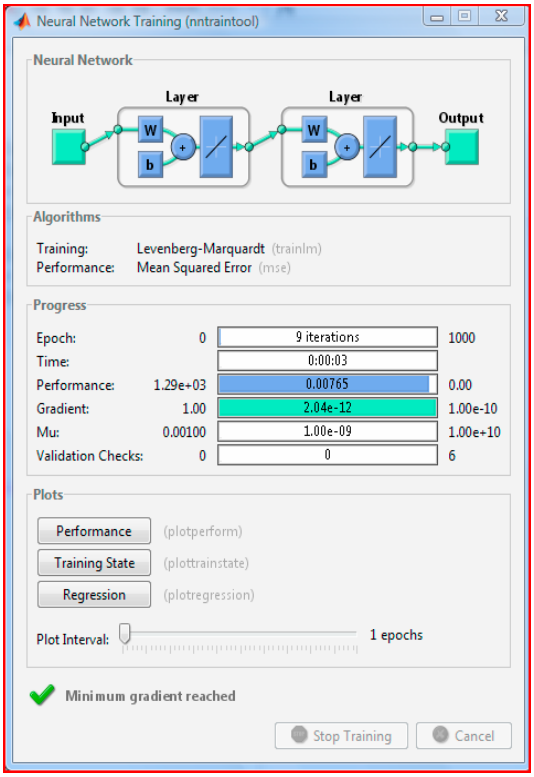


```
  Area .......................................
      9.5619

  Centroids ..................................
      1.5729    1.0310

  Eccentricity ...............................
      0.0051

  Kurtosis ...................................
      0.3711

  Skewness ...................................
      0.0358
```

Fig. 3. Features extracted from a sample signature

Area: Actual number of pixels in the region.

Centroid: Horizontal and vertical centers of gravity of the signature.



Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)

Epoch:	0	9 iterations	1000
Time:		0:00:03	
Performance:	1.29e+03	0.00765	0.00
Gradient:	1.00	2.04e-12	1.00e-10
Mu:	0.00100	1.00e-09	1.00e+10
Validation Checks:	0	0	6

Performance (plotperform)
Training State (plottrainstate)
Regression (plotregression)
Plot Interval: 1 epochs

✓ Minimum gradient reached

Eccentricity: The ratio of the distance between the foci of the ellipse and its major axis length

Kurtosis: It is a measure of flatness of distribution. It gives an idea of whether the data are peaked or flat relative to a normal distribution.

Skewness: It is a measure of asymmetry of distribution. A distribution, or data set, is symmetric if it looks the same to the left and right of the center point.

3. Artificial Neural Network

3.1. ANN Training [14]

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 [15], the neural network output is compared with the target 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.4.

Five exact signatures and three forged signatures train the network and they were enough to give very good results in verification.

Fig. 4. Neural Network Training

Table1 contains all the information related to the design of the neural network. Both original and forgery signatures are used for training the network. Testing signatures are also available.

Learning rate (Constant)	Default
Transfer Function First Layer	Tangent Hyperbolic
Transfer Function Second Layer	Tanget Hyperbolic
Training Algorithm	Trainlm
Initial weights	Randomized

Initial biases	Randomized
Max number of epochs	1000
Momentum Constant	Default
Error goal	0.0001
Number of patterns for original signature	5
Number of patterns for fake signature	3
Number of tested signatures	100
Number of tested original signatures	50
Number of tested fake signatures	50

Table.1. Neural Network Specifications

3.2. ANN Testing

The system has been tested for its accuracy and effectiveness on a database of about 100 signatures from 3 users which contains both their genuine and skilled forged signature sample counterparts. Our database consists of signatures done with different pens with different colors.

All the samples of our database were pre-processed and the global features were extracted out.

After features extraction, testing is done and the result is displayed, and the **threshold** was taken **90%** in the study that is below the percentage of 90% the signature is considered forged.

4. Results

The data base of about 100 signatures was tested. The precision of signature verification systems can be expressed by two types of error [16]:

False Acceptance Ratio (FAR): The false acceptance ratio is given by the number of fake signatures accepted by the system with respect to the total number of comparisons made.

False Rejection Ratio (FRR): The false rejection ratio is the total number of genuine signatures rejected by the system with respect to the total number of comparisons made.

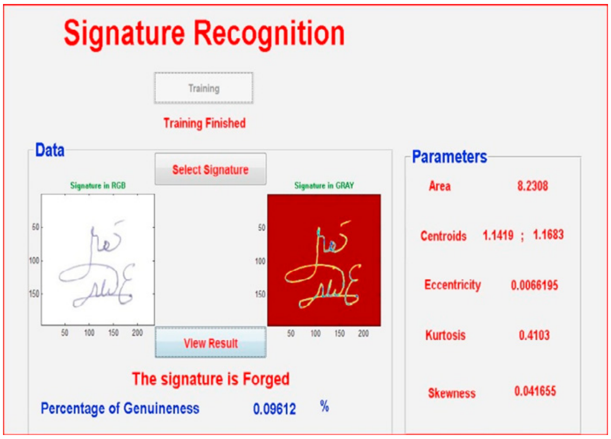
Both FAR and FRR depend on the threshold variance parameter taken to decide the genuineness of an image. If we choose a high threshold variance then the FRR is reduced, but at the same time the FAR also increases. If we choose a low threshold variance then the FAR is reduced, but at the same time the FRR also increases.

We obtain taking a threshold of 90% a FAR of 1.6% and a FRR of 3%.

The network was tested and it was capable of classifying the signatures of the taken database: exact or forged and a classification ratio of about 93% was obtained. And the minimized error percentages constitute an additional factor for the success of the verification system.

5. Graphical User Interface

Through the following interface, the user can select signature database of interest. Then train the network with the content of this database and simulate it. Current extracted features from each signature are displayed. The interface shows also a percentage level of ‘originality’ which indicates if the signature is exact or forged.



Training Finished

The signature is Forged

Percentage of Genuineness 0.09612 %

Area 8.2308

Centroids 1.1419 ; 1.1683

Eccentricity 0.0066195

Kurtosis 0.4103

Skewness 0.041655

Fig. 5. Graphical Interface when selecting a forged signature

Conclusions

Neural networks have demonstrated their success in many applications due to their ability to solve some problems with relative ease of use and the model-free property they enjoy. One of the main features, which can be attributed to ANN, is its ability to learn nonlinear problem offline with selective training, which can lead to sufficiently accurate response.

Application of Artificial Neural Network (ANN) to the above mentioned problem has attained increasing importance mainly due to the efficiency of present day computers. In addition, the times of simulation and testing in the ANN application are minimal. And the verification system based on ANN is able to learn different kinds of signature datasets, by using only geometrical offline features.

Moreover, the use of large databases is not required to show the capability of learning for this sort of problem, we have chosen only five genuine signatures and three forged ones for training, and we get very good results. However for real practice use, larger training data can increase the robustness of the system.

After training, the best classification accuracies were achieved. The classification ratio exceeds 93%, although the threshold, the parameter deciding the *genuineness of an image,* is 90%. The algorithm we supported uses simple geometric features to characterize signatures that effectively serve to classify signature as exact or forged. The system is robust and can detect random, simple and semi-skilled forgeries. We have no clear idea about its performance in case of very skilled forgeries because we are not skillful imitating signatures to the extent being considered as skilled forgeries.

References

1. K.R. Radhika, M.K. Venkatesha and G.N. Sekhar, “Off-Line Signature Authentication Based on Moment Invariants Using Support Vector Machine”, Journal of Computer Science 6 (3): 305-311, 2010.
2. Reza Ebrahimpour, Ali Amiri, Masoom Nazari and Alireza Hajiany, “Robust Model for Signature Recognition Based on Biological Inspired Features”, International Journal of Computer and Electrical Engineering, Vol. 2, No. 4, August, 2010.
3. A. Piyush Shanker, A.N. Rajagopalan, “Off-line signature verification using DTW”, Pattern Recognition Letters

28 (2007) 1407–1414.
4. Alessandro Zimmer and Lee Luan Ling, "Offline Signature Verification SystemBased on the Online Data", EURASIP Journal on Advances in Signal Processing Volume 2008, Article ID 492910, 16 pages.
5. D. Bertolinia, L.S.Oliveirab, E.Justinoa, R.Sabourinc, "Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers", Pattern Recognition (2009), doi:10.1016/j.patcog.2009.05.009.
6. Ramachandra A C, Ravi J, K B Raja, Venugopal K R and L M Patnaik, "Signature Verification using Graph Matching and Cross-Validation Principle", International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.
7. L.Basavaraj and R.D Sudhaker Samuel, "Offline-line Signature Verification and Recognition: An Approach Based on Four Speed Stroke Angle", International Journal of Recent Trends in Engineering, Vol 2, No. 3, November 2009.
8. Abhay Bansal, Bharat Gupta, Gaurav Khandelwal, and Shampa Chakraverty, "Offline Signature Verification Using Critical Region Matching", International Journal of Signal Processing, Image Processing and Pattern Vol. 2, No.1, March, 2009.
9. Bassam Al-Mahadeen, Mokhled S. AlTarawneh and Islam H. AlTarawneh, "Signature Region of Interest using Auto cropping", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 2, No 4, March 2010.
10. Mohammed A. Abdala & Noor Ayad Yousif, "Offline Signature Recognition and Verification Based on Artifical Neural Network", Eng and Tech. Journal, Vol.27, No.7,2009.
11. Dr. Daramola Samuel, Prof. Ibiyemi Samuel, "Novel Feature Extraction Technique For Off-Line Signature Verification System", Daramola Samuel et. al. / International Journal of Engineering Science and Technology Vol. 2(7), 2010, 3137-3143.
12. Vu Nguyen, Michael Blumenstein, Graham Leedham, "Global Features for the Off-Line Signature Verification Problem", 2009 10th International Conference on Document Analysis and Recognition.
13. A. Alizadeh, T. Alizadeh, Z. Daei, "Optimal Threshold Selection for Online Verification of Signature", Proceedings of the International MultiConference of Engineers and Computer Scientists 2010 Vol I, IMECS 2010, March 17-19, 2010, Hong Kong.
14. B. Daya, S. Khawandi and M. Akoum, "Applying Neural Network Architecture for Inverse Kinematics Problem in Robotics", Information Systems Architecture and Technology, Wroclaw 2009, part 2, pages.85-94, 2009.
15. Daya Bassam And Ismail Anis, "A Neural Control System of a Two Joints Robot for Visual Conferencing", Neural Processing Letters (2006) 23:289–303- DOI 10.1007/s11063-006-9003-z.
16. Zhong-Hua Quan, Kun-Hong Liu, " Online Signature Verification Based on the Hybrid HMM/ANN Model", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007.