International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 12 (2014), pp. 1113-1121

http://www. irphouse.com

A Hybrid Approach for Offline Signature Verification using Artificial Neural Networks

Aditya Kapil[1], Jaspreet Singh[2], Varun Srivastava[3]

[1,2,3]CSE Department, Bharati Vidyapeeth's College of Engineering,
A4, Paschim Vihar, New Delhi

Abstract

The signature of a person is an important biometric attribute of a human being which can be used to authenticate human identity. Various complex methodologies in the past have been proposed for signature verification through feature extraction. This paper presents a new hybrid algorithm for signature verification which incorporates feed forward training of parameters derived through feature extraction. It results in a much efficient algorithm which is yet simpler to operate from user's perspective. The method presented in this paper consists of image prepossessing, geometric feature extraction, neural network training with extracted features and verification. The Off-line Signature Recognition and Verification is implemented using MATLAB.

Abbreviations:
1. NN: Neural Network
2. HSV: Handwriting signature verification

1. INTRODUCTION

Signature is a special case of a person's handwriting. Although the biometrics of a person should not be duplicable but unfortunately it is possible to forge a biometric sample that can be accepted by the biometric system as a true sample. Therefore comes the need for a system to detect forgeries (if any) that are made to the original signature.

The various approaches for signature verification differ in the features that are extracted, the training method and the model used for classification and verification.

The various approaches used are:-

1. Hidden Markov Model
2. Neural Networks Approach

3. Template Matching Approach
4. Statistical Approach
5. Support Vector Machines

The model used for developing the said system is divided into 5 stages:

1. The signatures from various users were collected and a forgery database was created.
2. Pre-processing to prepare the image for feature extraction (like background removal etc.) was applied to all the images.
3. Features were extracted from these samples.
4. These features as input, a neural network was trained by the Levenberg-Marquardt backpropagation algorithm, to differentiate between the original and the forged signature. 5. Finally the trained network was fed with the test data for verification.

2. SIGNATURE RECOGNITION PROCESS

Biometric security is a computerized method of verifying a person's identity based on his/her body and/or physical attributes. Various forms of biometric security exist including fingerprinting, iris recognition [10], speech recognition [17], heart sound recognition [7], and keystroke recognition [12]. However, the longest standing and most natural method for verifying one's identity is through the use of a handwritten signature. Handwritten Signature Verification (HSV) is an automated method of verifying a signature by capturing features about a signature's shape (i.e., static features) and the characteristics of how the person signs his/her name in real-time (i.e., dynamic features). Neural networks extract a feature set representing the signature (details like length, height, duration, etc.), with several samples from different signers. Also Neural Network can 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. Concentrated efforts at applying NNs to HSV have been undertaken for over a decade with varying degrees of success (e.g., see [9], [16]).

2.1 Types of Signature Verification: Based on the definitions of signature, it can lead to two different approaches of signature verification:-

2.1.1 Off-Line or Static Signature Verification Technique:

This approach is based on static characteristics of the signature which are invariant [6]. In this sense signature verification, becomes a typical pattern recognition task knowing that variations in signature pattern are inevitable; the task of signature authentication can be narrowed to drawing the threshold of the range of genuine variation. In the offline signature verification techniques, images of the signatures written on a paper are obtained using a scanner or a camera

2.1.2 On-line or Dynamic Signature Verification Technique:

This is the second type of signature verification technique. This approach is based on dynamic characteristics of the process of signing. This verification uses signatures that are captured by pressure sensitive tablets that extract dynamic properties of a signature in addition to its shape. Dynamic features include the number of order of the strokes, the overall speed of the signature and the pen pressure at each point that make the signature more unique and more difficult to forge. [4].

In this paper we use offline mode of signature verification.

3. METHODOLOGY AND ALGORITHM

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

3.1 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

3.1.1 Converting image to binary:

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

3.1.2 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.

3.1.3 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.

3.1.4 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.

3.2 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:

3.2.1 *Center of mass*

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

3.2.2 *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. $Normalized\ area = Signature\ Area\ Area\ enclosed\ in\ a\ bounding\ box.$ (Eq(1))

3.2.3 *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. $Aspect\ Ratio = width\ of\ signature\ in\ a\ bounding\ box\ /\ Heigt\ of\ signature\ in\ a\ bounding\ box$ (Eq. (2))

3.2.4 *Wrinkleless*

It is the total number of black pixels available in the image after all the pre-processing has been done. Since the pixel count parameter is a unique value, we use this property of handwritings to distinguish between genuine and forged signature.

3.3 Training a neural network Extracted feature points are collected in a database. These normalized features are applied as input to the neural network. The detailed explanation of this is in the next part.

3.4 Verification.

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

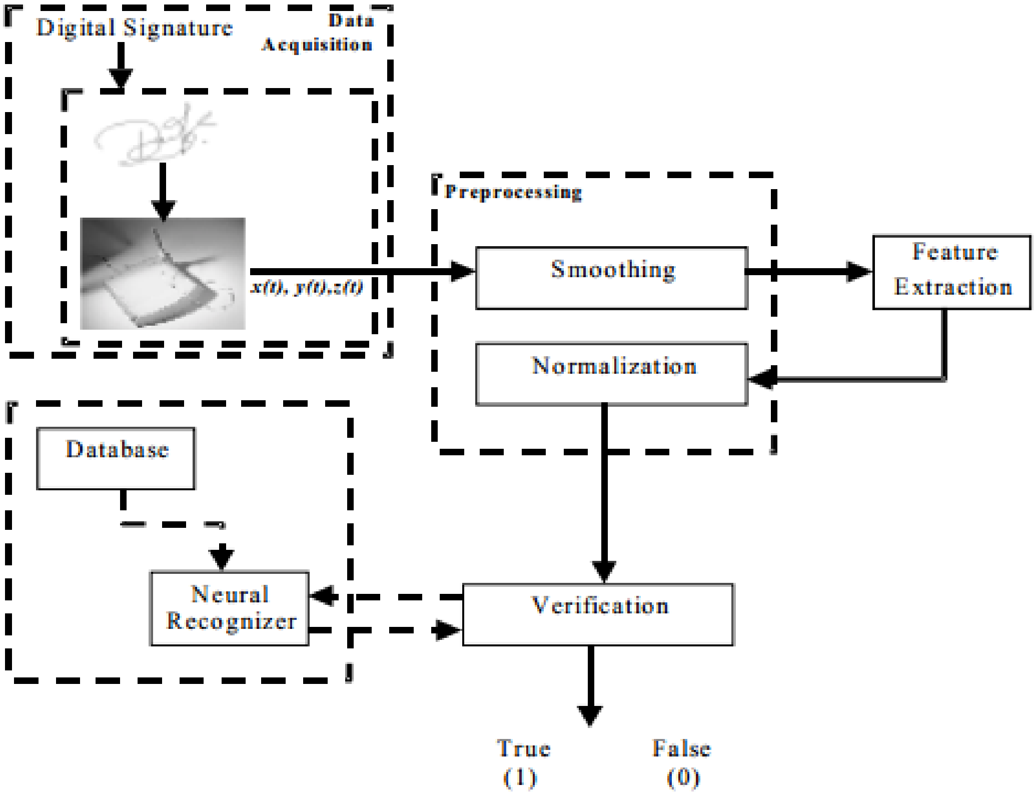


Figure 1: Verification of System

4. RECOGNITION USING NEURAL NETWORK

Plots:

***Performance Plot*:**

Plot perform(TR) plots the training, validation, and test performances given the training record TR returned by the function train.

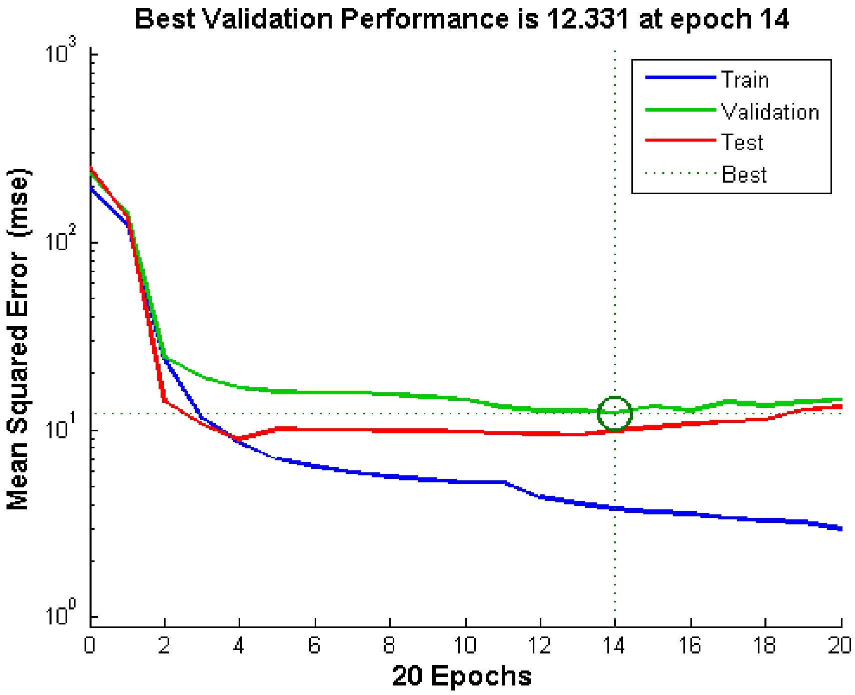


Figure 2: Performance Plot

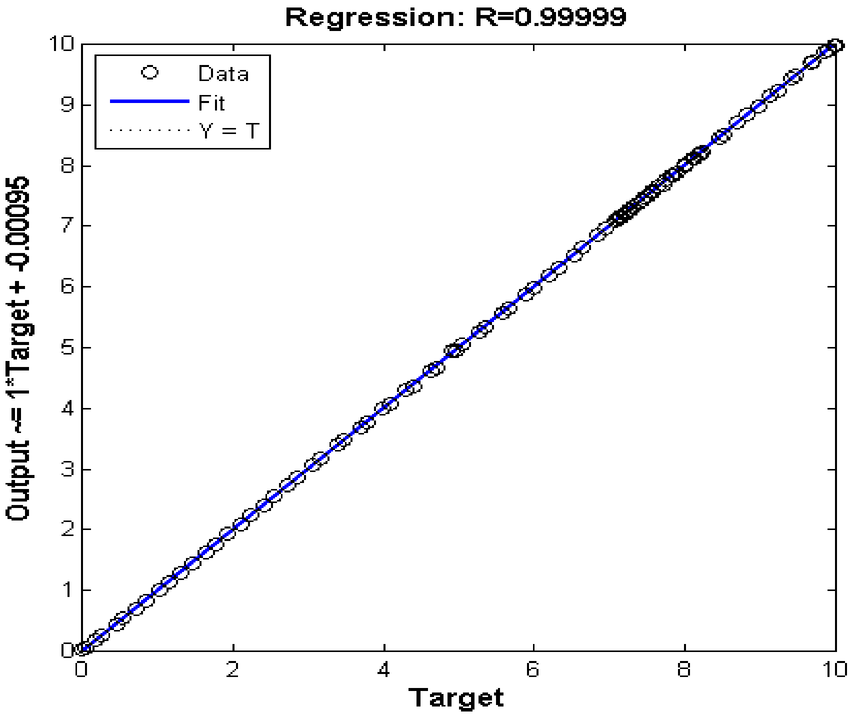


Figure 3 : Regression Plot

5. RESULT AND DISCUSSION

For training and testing of the system many signatures are used. The results given in this paper are obtained by creating a database of many genuine signatures of different people and then one forged specimen for each. The results provided in this research used a total of 200 signatures. Those 200 signatures are comprised of 20 sets (i.e. from 20 different people).. To train the system, a subset of this database was taken comprising of 10 genuine samples taken from each of the 20 different individuals and 20 forgeries made by different person for one signature. The features extracted from 20 genuine signatures and 20 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 6, 6 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, depending upon the error generated throughout the process.

5.1Training State Plot:

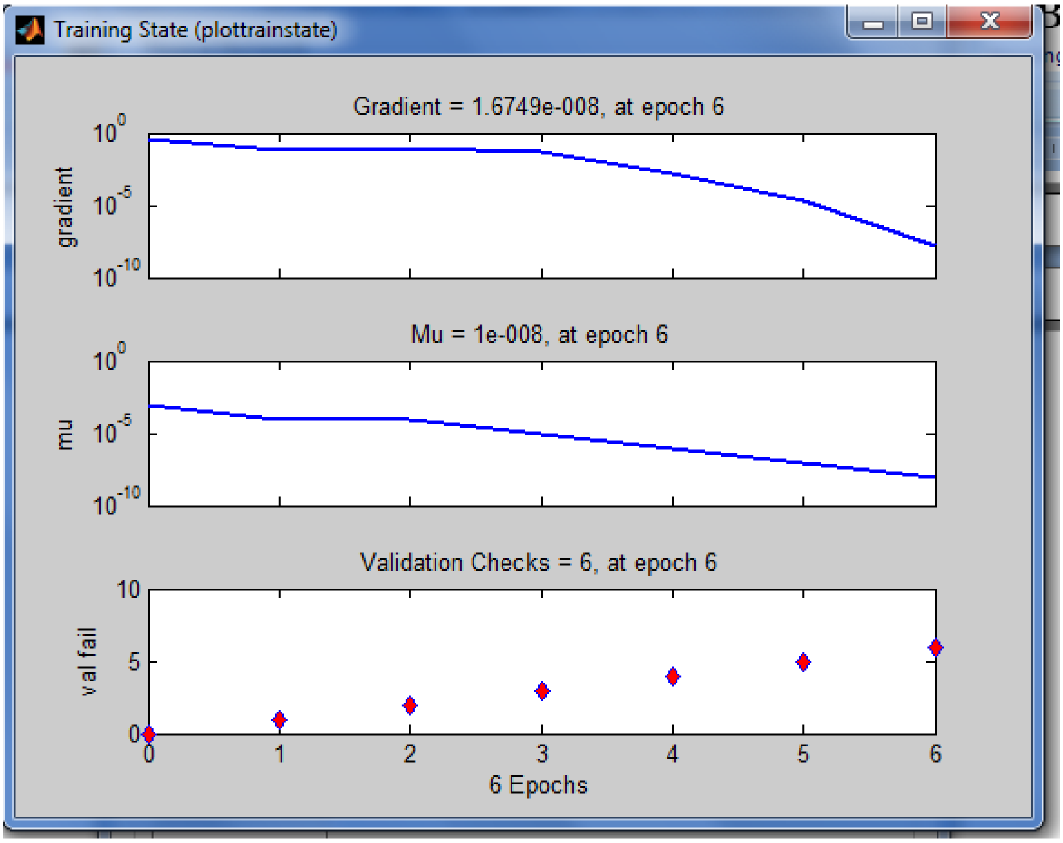
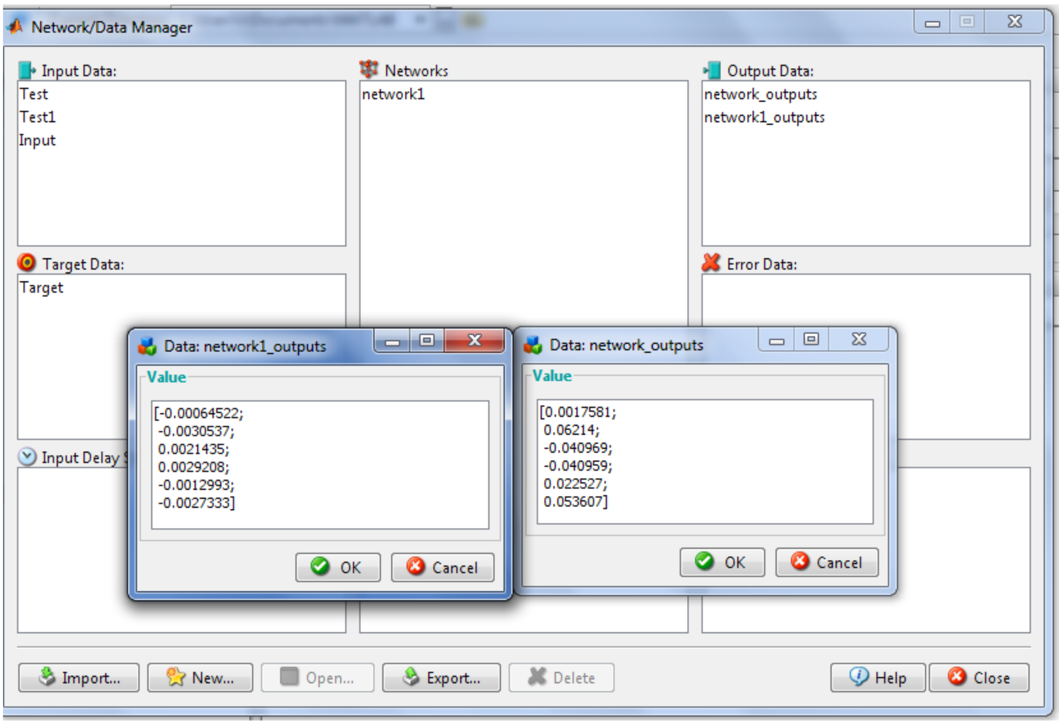

Training State (plottrainstate)
Gradient = 1.6749e-008, at epoch 6
gradient
10^0
10^-5
10^-10
Mu = 1e-008, at epoch 6
mu
10^0
10^-5
10^-10
Validation Checks = 6, at epoch 6
val fail
10
5
0
0
1
2
3
4
5
6
6 Epochs

Figure 4: Training State Plot Display Output Comparison for Forged/authentic sign. :



Input Data:
Test
Test1
Input

Networks
network1

Output Data:
network_outputs
network1_outputs

Target Data:
Target

Data: network1_outputs

```
[-0.00064522;
 -0.0030537;
 0.0021435;
 0.0029208;
 -0.0012993;
 -0.0027333]
```

Data: network_outputs

```
[0.0017581;
 0.06214;
 -0.040969;
 -0.040959;
 0.022527;
 0.053607]
```

Figure 5: Final Output Display

6. CONCLUSION AND FUTURE SCOPE

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.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 200 such signatures (150 genuine and 50 forged) it could recognize 148 signatures correctly. Hence, the correct classification rate of the system is 82.66% in generalization. Our recognition system exhibited 100% success rate by identifying correctly all the signatures that it was trained for. However, it exhibited poor performance when it was presented with signatures that it was not trained for earlier. We did not consider this a "high risk" case because recognition step is always followed by verification step and these kinds of false positives can be easily caught by the verification system. Generally the failure to recognize/verify a signature was due to poor image quality and high similarity between 2 signatures. Recognition and verification ability of the system can be increased by using additional features in the input data set. This study aims to reduce to a minimum the cases of forgery in business transaction.

7. REFERENCES

[1] 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.

[2] 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.

[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] 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.

[5] 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.

[6] 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.

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

[8] 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.

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

[10] 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

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