OFFLINE SIGNATURE VERIFICATION USING SUPERVISED NEURAL NETWORKS

Meenakshi Sharma[*]

Kavita Khanna[**]

Abstract –

Offline signature verification was the first approach to be applied for solving the signature verification problem for static images. It involves the discrimination of genuine and fake signatures on static images. In offline systems we have only the static image containing the signature as an input, without having any knowledge on the signing process. Some difficulties that may be come up in offline systems are related to the scanning process (noise on the image) and to the signature acquisition process where different pen tips and widths can produce different shapes. This paper presents a method of signature verification using Supervised neural networks and determine the percentage of number of times correct signature have been recognized as correct then we calculate the average performance of the Networks and A comparison among the neural networks was drawn and generalize on which of these techniques provide the better results i.e. which technique is more suitable for identifying the forged signatures.

Index Terms –FF, Recurrent, signature verification, CCR,forgery.

IJMRA

[*] Student, CSE Deptt, PDM College of Engineering for Women

[**] Vice-Principal, CSE Deptt, PDM Collegeof Engineering for Women

I. Introduction

Hand written signature is the most widely form of personal identification, especially for cashing cheques and credit cards transactions. However, for several reasons the task of verifying human signature can't be consider a trivial pattern recognition problem because signature samples from the same person are similar but not identical. A person's signature often changes radically during their life. We cannot see much variability in signature according to country, age, time, and psychological or mental state, physical and practical conditions. Currently all signature verification for daily transaction is based on visual inspection by teller or clerk with the result that large amount. In the business word an automatic signature verification system would be extremely useful for reduction of forgery in monetary transaction. There are two types of handwritten recognition schemes practised today: Online and offline.

On-line handwriting recognition involves the automatic conversion of text as it is written on a special digitizer, where a sensor picks up the pen-tip movements as well as pen-up or On-line handwriting recognition involves the automatic conversion of text as it is written on a special digitizer, where a sensor picks up the pen-tip movements as well as pen-up or pen-down switching. That kind of data is known as digital ink and can be regarded as a dynamic representation of handwriting. The obtained signal is converted into letter codes which are usable within computer and text-processing applications. This method focuses on Dynamic systems produces signal with time (velocity, acceleration, pressure and time). In Offline handwriting recognition involves the automatic conversion of text in an image into letter codes which are usable within computer and text-processing applications. The data obtained by this form is regarded as a static representation of handwriting. The technology is successfully used by businesses which process lots of handwritten documents, like insurance companies. The quality of recognition can be substantially increased by structuring the document (by using forms). In Offline recognition case the signature appears as a 2D (gray level or binary) image.

A. Forgery

Signature forgery refers to the act of falsely replicating the signature of another person. In signature verification, forged signatures can be broken up into three different categories.

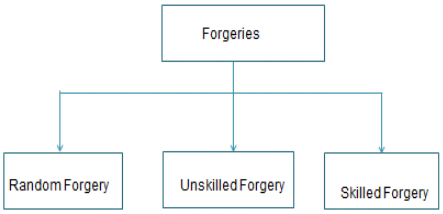


Fig. 1 Types of Forgery

Random forgery—It is produced when the signer knowing the name of the victim and produced signature in his own style. This forgery is easily detected by the visual analysis. In random forgery the forger does not know the signer's name or signature shape.

Unskilled forgery— In simple forgery or unskilled forgery, the forger knows the name of the original signer but not what his signature looks like. It is produced copy the signature in his own style without having any previous experience.

Skilled forgery—It is produced by looking the original signature or by having idea about the signature of the victim. Generally this kind of forgery is generated by the professional persons who have experience in copying the signature. This type of forgery cannot be easily detected by visual analyse.

II. PREPROCESSING

Image processing is a technique to convert an image into digital form and perform some operations on it, so that can get an enhanced image or to extract some characteristics from it. It is a type of signal processing in which input is image, 2-d image, video frame and output may be image or information associated with that image. Usually Image Processing system treating images as two dimensional signals and applying already set signal processing methods to them. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. It basically means manipulation and modification of images.

A.Color Inversion

A gray scale or greyscale digital image is an image in which carries only intensity information. Images of like this, also known as black-and-white, are composed by gray, varying from black at the weakest (0) intensity to white (1) at the strongest. This range is represented in an abstract way as a range from 0 (total absence, black) and 1 (total presence, white), with any fractional values in between. This notation is used in academic papers, but this does not define what "black" or "white" is in terms of colorimetric.

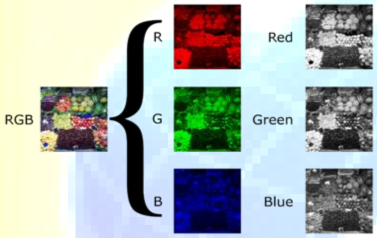


Fig. 2 Gray scale image

B. Filtering

When an image is captured by a digital camera or other imaging system, often the system for which it is intended is unable to use it directly. The image may be distorted by random variations in intensity, noisy variations in illumination, or poor contrast that must be removed with in the early stages of vision processing. Image filtering is useful for many applications, including smoothing, sharpening, dropping noise, and edge enhancement. A filter is defined by a kernel or convolution mask, which is a small array placed to each pixel and its neighbors within an image. In most applications, the center of the kernel is aligned with the current pixel, and is a square with an odd number (3, 5, 7, etc.) of elements in each dimension. The process used to apply filters to an image is known as convolution, and may be applied in either the spatial or frequency domain. Fig. 3 shows the image before the filtering and after the filtering.

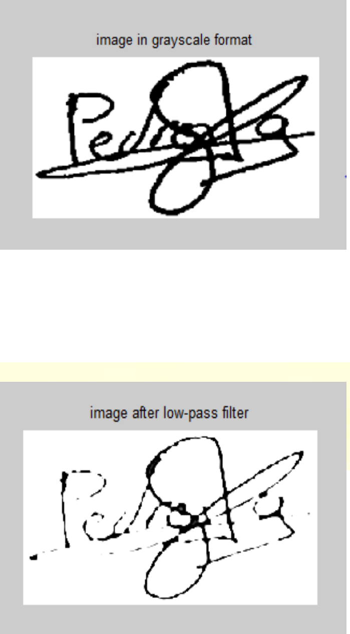


Fig 3. Before and After Low-Pass Filter

C. Binarization

.A binary image is a digital image that has only two possible values for each pixel such as 0 or 1 only the two colors are used for a binary image i.e. black and white though any two colors can be used. The color used for the object(s) in the image is the foreground color while the rest of the image is the background color. In the document-scanning this is often referred to as "bi-tonal".

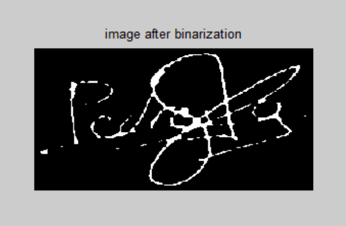


Fig.4 Binarized image

III. FEATURES EXTRACTION

Feature extraction is necessary to the success of a signature verification system. In an offline environment, the signatures are acquired from a medium, usually paper, and pre-processed before the feature extraction begins. Offline feature extraction is a fundamental problem because of handwritten signatures variability and the lack of dynamic information about the signing process. An ideal feature extraction technique extracts a minimal feature set that maximizes interpersonal distance between signature examples of different persons, while minimizing intrapersonal distance for those belonging to the same person. Some of these features are as follows:

Area: Actual number of pixels in the region.

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

Eccentricity: It is the central point of the signature. If deviation in the central point of an image but this is not enough evidence by itself. The central point is acquired by applying the ratio of the major to the minor axes of an image. The ratio of the distance between the foci of the ellipse and its major axis length.

Skewness: It is a measure of symmetry, or more precisely, the lack of symmetry. A distribution or data set, is symmetric if it looks the same to the left and right of the centre point allows us to determine how bowed are the lines in each segment of the signature. The percentage of this torsion is then calculated and extracted. Most signatures are complicated, with no edges but twists, and the width and height of these twists is a very important

Kurtosis: It is a measure of flatness of distribution. Basically measure of whether the data are peaked or flattened, relative to a normal distribution. Data sets with high kurtosis tend to have a distinct peak near the mean, decline rather rapidly, and have heavy tails. Data sets with low kurtosis tend to have a flat top near the mean rather than a sharp peak. It also measures the existence, or the absence of tails, that are unconnected lines with no peaks.

Orientation: defines the direction of the signature lines. This feature is important because it allows us to know how the signer wrote down the signature, which letters came first emphasizing the direction of angles and peaks

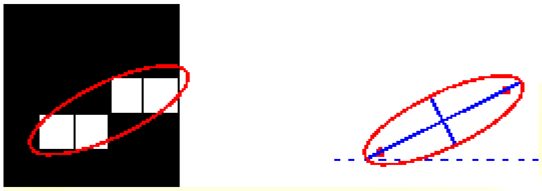
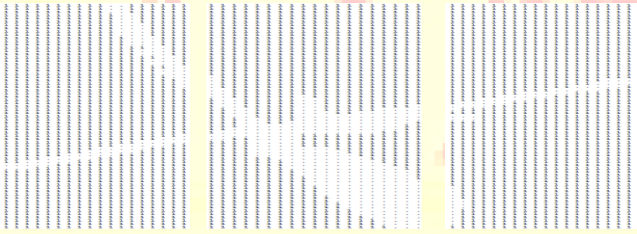


Fig.6 Orientation

Trisurface: The surface area of two visually different signatures could be the same. For the purpose of increasing the accuracy of feature describing the surface area of a signature, the 'Trisurface' feature was investigated, as an extension, in which the signature was separated into three equal parts, vertically. The surface area feature is the surface covered by the signature, including the holes contained in it. The total number of pixels in the surface was counted, and the proportion of the signature's surface over the total surface of the image was calculated.

This process was used for the three equal parts of the signature, giving three values between 0 and 1.

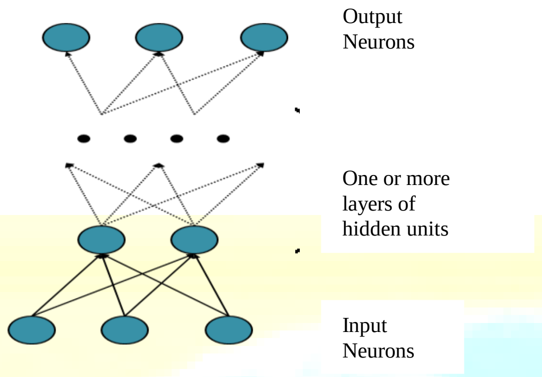


(a) (b) (c)

Fig.7 The Trisurface feature

IV. ARTIFICIAL NEURAL NETWORK TRAINING

A. Feed Forward Network



- Allow signals to travel one way only: from input to output.
- There is no feedback (loops); *i.e.*, the output of any layer does not affect that same layer.
- bottom-up or top-down
- The ANN is created and trained through a given input/target data training pattern. During the learning process 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.

We used the ‘newff’ MatLab command to generate the network.

Net=newff(P,T,S,TF,BTF,BLF,PF,IPF,OPF,DDF)takes optional inputs,

TFi - Transfer function of ith layer. Default is 'tansig' for hidden layers, and 'purelin' for output layer.

TF - Backprop network training function, default = 'trainlm'.

BLF - Backprop weight/bias learning function, default = 'learngdm'.

PF - Performance function, default = 'mse'.

IPF - Row cell array of input processing functions.Default is {'fixunknowns','remconstantrows','mapminmax'}

OPF - Row cell array of output processing functions. Default is {'remconstantrows','mapminmax'}

DDF - Data division function, default = 'dividand returns an N layer feed-forward backprop network.

Six genuine signatures and Four forged signatures of 50 different persons are used to train the network and they were enough to give very good results in verification.

Table 1 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.

Number of hidden Layers	4
Number of neurons in Hidden Layer	6,12,6,1
Number of neurons Output layer	1
Number of inputs	10
Transfer Function Second Layer	Tangent Hyperbolic
Transfer Function Second Layer	Tangent Hyperbolic
Transfer Function Third Layer	Tangent Hyperbolic
Transfer Function fourth Layer	Tangent Hyperbolic
Transfer Function output Layer	Purelin
Learning rate (Constant)	Default
Training Algorithm	Trainlm
Initial Weights	Randomized
Initial Biases	Randomized

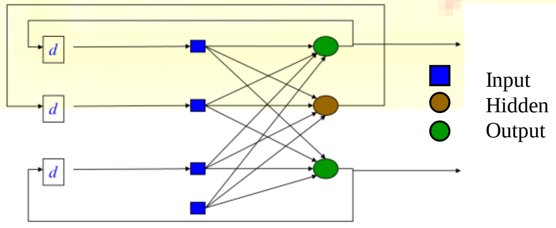
IJMRA

Max number of epochs	1000
Error goal	0.001
Momentum constant	0.001
Number of original signature for training	300
Number of fake signature for training	200
Number of tested signatures	300
Number of tested original signatures	200
Number of tested fake signatures	100

Table.1. Neural Network Specifications for feed forward network

B. Recurrent Neural Network

A recurrent neural network (RNN) is a class of neural network where connections between units form a directed cycle. This creates an internal state of the network which allows it to exhibit dynamic temporal behavior. Unlike feedforward neural networks, RNNs can use their internal memory to process arbitrary sequences of inputs.



- signals travels in both directions
- Dynamic
- There are feedbacks (loops).

We used the ‘layrecnet’ MatLab command to generate the network

layrecnet(layerDelays,hiddenSizes,trainFcn) takes a row vectors of layers delays, a row vector of hidden layer sizes, and a backpropagation training function, and returns a layer recurrent neural network with N+1 layers.

Table 2 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

Number of hidden Layers	4
Number of neurons in Hidden Layer	6,12,6,1
Number of neurons Output layer	1
Number of inputs	10
Layer delay	1:2
Learning rate (Constant)	Default
Training Algorithm	Trainlm
Initial Weights	Randomized
Initial Biases	Randomized
Max number of epochs	1000
Error goal	0.001
Momentum constant	0.001
Number of original signature for training	300
Number of fake signature for training	200
Number of tested signatures	300
Number of tested original signatures	200
Number of tested fake signatures	100

IJMRA

Table.2. Neural Network Specifications for Recurrent network

V. ARTIFICIAL NEURAL NETWORK TESTING

- The trained neural network – which has learned how to work on signatures and their features through training – compares the features of the given signature with those of the signatures in the database.
- If the output of tested image is greater than 0.5 then it is considered true or genuine signature and number of correct outputs is incremented.
- Based on the total number of correct outputs out of 300 we calculate the percentage.
- We test these 300 signatures over 30 different networks.

The system has been tested for its accuracy and effectiveness on a database of about 300 signatures from 50 users which contains both their genuine and skilled forged signature sample counterparts.All the samples of our database were pre-processed and the features were extracted out. After features extraction, testing is done and the result is displayed, and the threshold was taken 50% in the study that is below the percentage of 50% the signature is considered forged

VI. RESULTS

The data base of about 300 signatures was tested under the feed-forward and Recurrent neural network. The threshold of 50% was given to the networks and the Correct Classification Rate (CCR)was determined on the both networks.

Both networks was trained using 30 neural networks and average of correct classification was determined for feed- forward network was 96.8222%.and 97.9777% for recurrent network.

S.No	Methods	CCR (%)
1.	Feed Forward network	96.82
2.	Recurrent neural network	97.97

Table 3. Results for methods

VII. CONCLUSION

This paper presents a research on the offline signature verification and recogintion using supervised neural networks.

We were used feed-forward and Recurrent Neural Network.we were taken 500 signature from 50 users for training which contain both genuine and forged signatures and 300 signatures were used for testing which includes 200 original signature and 100 forged signatures.A feature vector of 10*500 was given as an input to the networks and we were used athreshold of 50% and obtained the CCR above 95%.The recurrent network as compare to feed forward was given better results for signature verification and Recognition.

REFERENCES

[1] Ali Karouni,Bassam Daya,Samia Bahlak, “Offline signature recognition using neural networks approach” Procedia Computer Science Vol 3, pp 155–161,2011

[2] H. Baltzakis, N. Papamarkos, “A new signature verification technique based on a two-stage neural network classifier”, Engineering Applications of Artificial Intelligence ,2001.

[3] Odeh, S.M and Khalil,M., " Apply Multi-Layer Perceptrons Neural Network for Off-line signature verification and recognition ", IEEE transactions on pattern analysis and machine intelligence, Vol 27, pp 235-247, June 2011.

[4] P. Deng, H. Yuan Mark Liao & H. Tyan, “Wavelet Based Off-line Signature Recognition System”, Proceedings 5th Conference on Optical Character Recognition and Document Analysis, Beijing,China,1996

[5] A. Piyush Shanker and A. N. Rajagopalan, “Off-line signature verification using DTW, Pattern Recognition Letters”, Vol.28 n.12, pp 1407-1414,2007

[6] Indrajit Bhattacharya bir Ghosh,Swarup Biswas,“Offline Signature Verification Using Pixel Matching Technique” Procedia Computer Science Vol 2,pp 134-142 ,2013.

[7] Prashanth C. R. and K. B. Raja,” Off-line Signature Verification Based on Angular Features”, *International Journal of Modeling and Optimization, Vol. 2, No. 4, August 2012.*

[8] S. Rashidi, A. Fallah, F. Towhidkhah,"Feature extraction based DCT on dynamic signature verification" Procedia Computer Science Vol 3, pp 1810–1819 December 2012.

[9] S. Audet, P. Bansal, and S. Baskaran ,"Off-line signature verification using virtual support vector machines", ECSE 526 – Artificial Intelligence, April 7, 2006.

[10] Ibrahim S. I. Abuhaiba ,"Offline 10.Signature Verification Using Graph Matching" Turk J Elec Engin, VOL.15, NO.1 2007.

[11] H. Lv, W. Wang, C. Wang, and Q. Zhou,"Off-line Chinese signature verification based on support vector machines", PRL , vol. 26, no. 15, pp. 2390–2399 ,2005

[12] J.Edson, R.Justino, F.Bortolozzi and R. Sabourin, "Off-line signature verification using HMM for Random, Simple and Skilled Forgeries", 2001

[13] B. Majhi, Y. Reddy, D. Babu, "Novel Features for Off-line Signature Verification", International Journal of Computers,.Communications & Control Vol.I (2006), No. 1, pp. 17-24,2012

[14] 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

[15] V.E. Ramesh, M. Narasimha Murty ," Off-line signature verification using genetically optimized weighted features", Pattern Recognition Vol.32, Issue 2,, pp.217–233,February 1999

[16] Tulsi Gupta ,"Off-line Signature Verification", INTERNATIONAL JOURNAL OF COMPUTER APPLICATION Vol. 3 ISSUE 2, JUNE 2012.