IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 28-35
www.iosrjournals.org

Artificial Neural Network Based Signature Verification

Vinayak Jadhav[1], Nikhil kadam[2], Paresh Keluskar[3], Ayyaj Khan[4]
[1, 2, 3, 4]*(Sspmcoe,Kankavali,Mumbai University, Maharashtra, India)*

Abstract: *The human signature is proven to be the most important for access. Signature of the person is proven to be the important biometric attribute of a human being which can be used to authenticate human identity [1]. There are many biometric characteristics by which one can have own identity like face recognition, fingerprint detection, iris inspection and retina scanning [2]. Voice reorganization and signature verification are the upcoming technologies for the human identity.Human signature can be handling as the image and can be recognized by using the computer vision and neural network. With the help of the modern technology there is possibility to develop such algorithm with help of which one can able to recognize and verify the human signature. This paper deals with the off-line signature recognition & verification using neural network in which the human signature is captured and presented in the image format to the system.*

Keywords: *Image Processing, Neural Network, Offline signature Recognition & Verification, Security.*

I. Introduction

Signature is socially accepted & extensively used means for authentication in our daily life. Manual signature is very basic method for person for recognition of the signer of the document with the assumption that signature changes slowly & virtually impossible to forge without detection [1]. A signature may articulate as a behavioral biometric. It is widely used to recognize a person delivering out daily procedures i.e. bank operations, document analysis, electronic funds transfer, and access control, by using his manual signature [1]. This system has two distinct but strongly related tasks as recognition of the signature & verifying it whether it is genuine or forged [1].

1.1 Features:

Features can be generally divided into two types

1.1.1Global Features - which are extracted from the whole signature, including block codes, Wavelet and Fourier series. The global features can be extracted easily and are tough to noise. But they only deliver limited information for signature verification [1].

1.1.2Local Features - which are calculated to describe the geometrical characteristics such as location, tangent track, and curving. Local featuresprovide affluent descriptions of writing shapes and arepowerfulforcultivated writers, but the extraction of consistent local features is still a hard problem [1].

The local features based approaches are more popular in dynamic verification than in the offline one. This is because it is much easier to calculate local shape and to find their corresponding relations in 1D succession than in 2D images [1]. This reality encourages us to consider recovering writing trajectories from offline signature.

II. Types of Signature Verification

A signature verification technique which is used to solve this problem can be divided into two classes Online i.e. Dynamic and Off-line i.e. Static

2.1.1 Online i.e. Dynamic Signature Verification Technique (DSVT*)*

On-line approach uses an electronic pressure sensitive tablets tablet to extract information about a signature and takes dynamic information like pressure, velocity, speed of writing, number of order of the strokes and the pen pressure at each point etc. for verification purpose that make the signature more unique and more difficult to recreate [1][3]. Application areas of Online Signature Verification include protection of PDA, laptop, authorization of computer users for accessing sensitive data or programs and authentication of individuals for access to physical devices or buildings [3].

2.1.2Offline i.e. Static Signature Verification Technique (SSVT)

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 straightforward & are invariant [1]. For this only the pixel image needs to be estimated. The off-line systems are difficult to design because many accepted characteristics such as the no. of strokes, the velocity and other dynamic information are not available in the offline case [3].

The verification process has to rely on the features that are extracted from the copy of the static signature images only. In this logic SSVT, becomes a characteristic pattern recognition task perceptive that deviation in signature pattern are expected. The task of signature authentication can be lessened to drawing the threshold of the range of genuine variation [1][3].

2.2. Types of Counterfeit of Signature

The objective of the signature verification system is to discriminate between two signature classes the genuine and fake signature [3]. A bunch of effort has been taken in the field of off-line signature verification. Forgery is a crime that aims at misleading people. Since actual forgeries are difficult to obtain, the instrument and the results of the verification depend on the type of the forgery [3]. There are basically three types of forgeries as

2.2.1Random forgery - This can normally be represented by a signature sample. Forger has no information about the signature style and the name of the person [3].

2.2.2Simple forgery - This is a signature with the same shape or the legitimate writer's name [3].

2.2.3Skilled forgery - This is signed by a person who has had access to a genuine signature for practice [3].

Although a great amount of work is determined on random and simple forgery detection, more hard work is still needed to tackle the problem of skilled forgery detection. No verification algorithms are proposed which might be deal with skilled forgeries [7].

III. Overview of Artificial Neural Network

The simplest definition of a neural network is provided by the inventor of one of the first neuron computer, Dr. Robert Hecht-Nielsen. He defines a neural network as: "Acomputing system made up of a number of simple, extremely interrelated processing elements, which practice information by their dynamic state response to peripheral inputs."[9]

Artificial neural networks are models motivated by the brain that is competent of machine learning and pattern recognition. They are usually presented as organization of interconnected "neurons" that can calculate values from inputs by providing information through the network [9]. Neural networks are characteristically structured in layers. Layers are consisting of a number of interrelated 'nodes' which hold an 'activation function'. Patterns are available to the network by means of the 'input layer', which communicate to one or more 'hidden layers' where the concrete processing is done using a system of subjective 'connections'. The hidden layers then unite to an 'output layer' where the answer is final output of the system as shown in the figure below [9].

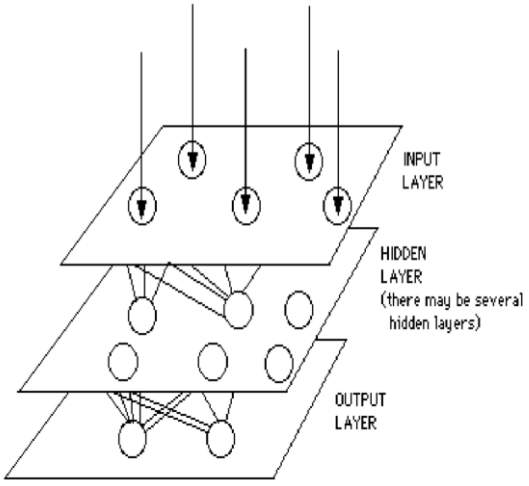

Fig. 1 simple neural network diagram.

To better understand artificial neural computing it is vital to be know how a conventional computer processes information. A serial computer has a fundamental processor that can address an array of memory locations where data and instructions are stored. Computations are made by the processor by interpretation of instruction as well as data that instruction requires. Then instruction is executed and results are saved in a memory location as necessary. In a conventional system the computational steps are deterministic,sequential and rational, and the status of a given variable can be track from one operation to another [10].

In contrast, Artificial neural network i.e. ANNs are not chronological or essentially deterministic. There are no intricate central processors, to a certain extent there are numerous uncomplicated ones which generally do nothing more than take the weighted summation of their inputs from other processors [10]. ANNs

do not execute programmed instructions; they react in parallel to the pattern of inputs offered to it. There are no separate memory addresses to accumulate data. Instead, information is controlled in the general activation 'state' of the network [9]. 'Knowledge' is represented by the network itself, which is fairly more than the summation of its individual components. Although there are many different types of knowledge rules used by neural networks, this expression is concerned with the delta rule. The delta rule is frequently use by the most ordinary class of ANNs called 'back propagation neural networks'. [10] With the delta rule, 'learning' is a organize process that take place with each cycle during a forward activation stream of outputs, and the backwards error propagation of weight regulation [9].

IV. Proposed System

This projected offline signature verification system offers computerized method of verification and recognition by extracting features that characterizes each input signature [7]. The approach starts by scanning images into the computer using peripheral devices, then modifying their quality through image enhancement, followed by feature extraction and neural network training, and finally verifies whether a signature is genuine or counterfeit.

4.1. Pre-processing

Generally in any image processing application preprocessing is required to remove alteration, from the original input image [7] [8]. Any normal scanner with sufficient resolution can be used as an image attainment device for offline operation [1]. Signatures are scanned in gray, using following equation as [8]:

(1) Gray colour = (0.299*Red) + (0.5876*Green) + (0.114*Blue)

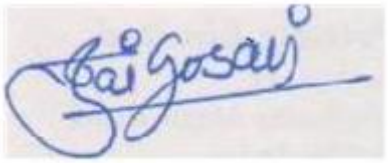

Fig.2 Original image

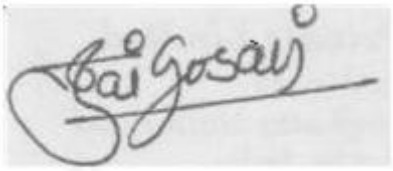

Fig.3 Image after gray scale

The purpose in this stage is to build signature standard and prepared for feature extraction. The pre-possessing stage includes following processing,

4.1.1Scaling

Let H be the height of the inputted image & W be the width of the inputted image [7]. We can fit the image uniform at 100*100 pixels by using the following equation as:

(2) Xnew = (Xold * 100)/H;

Where X_{new}&X_{old} are calculated & original X coordinate

(3) Y_{new}= (Y_{new} * 100)/W;

Where Y_{new}&Y_{old} are calculated & original Y coordinate.

With these equations input image is transformed to uniformed 100*100 pixels image [7].

4.1.2 Noise Reduction

Images are contaminated due to stemming from decoding errors or noisy channels. An image also gets degraded because of the detrimental effects due to illumination and other objects in the environment. Median filter is extensively used for smoothing and restoring images corrupted by noise [8]. This is a nonlinear process useful principally in reducing impulsive noise [7]. In a median filter, a window slides over the image, and for each location of the window, the median concentration of the pixels within it decide the intensity of the pixel positioned in the middle of the window. As weigh against to the mean filter, median filter has striking properties for suppressing impulse noise while preserving edges; due to this feature we are recommended this filter in our proposed system [8].

4.1.3 Background Elimination

Numerous image processing applications necessitate segregation of objects from the background. Thresholding is the most trivial and effortlessly appropriate method for this [8]. We used Thresholding method for distinguish the signature from the background. In proposed application, we are concerned in dark objects on light background and hence a threshold value T entitled as the brightness threshold is suitably chosen and applied to image [1]. After the Thresholding, the pixels of the signature would be 1 and the other pixels which belong to the background would be 0 [7].

The brightness threshold [8] can be chosen such that it satisfies the following conditions;

Suppose image pixels f(x, y) then,

If $f(x, y) \geq T$

Then f(x, y) = Background

Else f(x,y) = Object

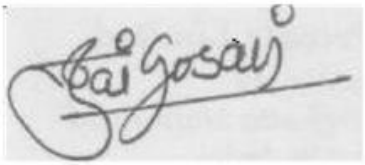

Fig. 4.image with background

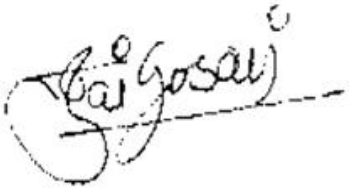

Fig. 5.image after thresholding

4.1.4Signature Normalization

Irregularity in image capturing and scanning process causes dimensions of signature to fluctuate [1]. Height and width of signatures fluctuate from person to person and occasionally even the same person may exercise different sizes of signature [8]. Therefore it is needed to get rid of the size variation and achieve a benchmark signature size for all input signatures. Throughout the normalization process, the characteristic ratio between the width and height of a signature is kept undamaged and following the process, all the signatures will have the similar dimension [8]. Normalization process made use of the following equations:

(4) Xnew = [(Xold-Xmin)/ (Xmax-Xmin)]*M

(5) Ynew = [(Yold-Ymin)/ (Ymax-Ymin)]*M

Where,

X_{new}, Y_{new} = Pixel coordinates for the normalized signature,

X_{old}, Y_{old} = Pixel coordinates for the original signature,

M = Width/height meant for the normalized signature

The normalization procedure is verified in the subsequent figure [8].

Fig. 6.original image

Fig. 7.image after normalization

4.1.5 Thinning

The goal of thinning is to eliminate the thickness differences of pen by making the image one pixel thick [2]. Thinning was introduced to describe the global properties of objects and to reduce the original image into a more compact representation [7]. It uses a Stentiford algorithm for thinning process.

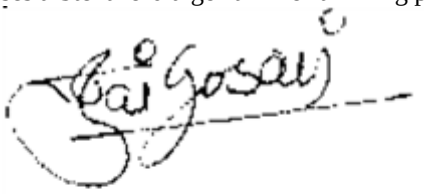

Fig. 8.image before thinning

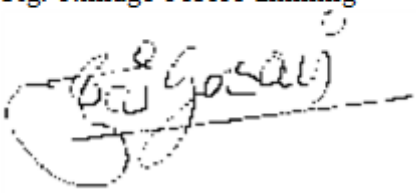

Fig. 9.image after thinning

4.2. Feature Extraction

In Feature extraction, the essential features are extorted from the original input signature. The features to be extorted are based on the application and fluctuate accordingly [7]. Characteristic constraints are computed from the sort out data and are used to characterize signature. The choice of a powerful set of features is crucial in signature verification systems [2]. The features that are extracted from this phase are used to create a feature vector. We use a feature vector to uniquely characterize a candidate signature [1]. These features are extracted as follows,

4.2.1 Global Features

Global feature offers information regarding shape like signature area, signature height-to-width ratio, slope & slope direction skewness of signature etc. *Slope And Slope Direction* - To calculate approximately the slope of the signature the algorithm proposed by Ammar is used [7]. This algorithm formulates the use of the thinned image obtained during the pre-processing. A 3*3 sliding window is used for calculation. The window is stimulated starting from the top left pixel to the bottom right pixel, one pixel at a time in a row major order [7].

Density of Thinned Image - The density of thinned image can be designed after thinning which can be calculated by the following formula [7].

Density of thinned image = No of non zero pixels in the thinned image / Total no of pixels in the thinned image.

Width to Height Ratio

Width to height ratio is the ratio of range of x coordinates to the range of y coordinates [7]. The formula for calculating width to height ratio is given as:

(6) Width to Height Ratio = $(X_{max} - X_{min}) / (Y_{max} - Y_{min})$

Where, X_{max}&X_{min} = Maximum & Minimum values of x coordinates of non-zero pixels,

Y_{max}&Y_{min} = Maximum & Minimum values of y coordinates of non-zero pixels [7].

Skewness

Skewness is a measure of symmetry. It allows us to determine how curved are in each segment of the signature. The proportion of this torsion is afterwards calculated and extracted. Moreover, this percentage is weigh against to that extracted from the other images [7].

4.2.2Mask Feature

This provides information about guidelines of the lines of the signature for the reason that the angles of signature have interpersonal variation [1].

4.2.3Texture Feature

The texture features are the pixel positions with respect to the property of the feature. These can be processed using a matcher which uses co-occurrence matrix of the picture image. It includes End points, Branch points, crossing points. To extract these features, it is necessary to apply the pre-processing techniques like Thresholding and thinning on a gray scale signature image [7]. End points are points where a signature stroke begins or ends. Branch points are points where on signature stroke bifurcates into two strokes. Crossing points are points where one signature stroke crosses another stroke [7].

V. Algorithm & Flowchart

This section offers algorithm for the offline signature verification system in which artificial neural network is used to confirm the genuineness of signature [2].

Input = Signature Image

Output = Conformation from system whether signature is genuine or counterfeit.

5.1Algorithm

1. Acquire signature image from the database
2. Enhanced the inputted signature image by preprocessing
2.1 Convert original image to gray scale image
2.2 Scaling
2.3 Noise Reduction
2.4 Background Elimination
2.5 Signature Normalization
2.6 Thinning
3. Extract the various features
3.1 Global features
3.1.1 Slope & slope direction
3.1.2 Density of thinned image
3.1.3 Width to height ratio
3.1.4 Skeweness
3.2 Mask features
3.3 Texture features
4. Create a feature vector by combining extracted features from the pre-processed signature image.
5. Normalized the feature vector for further processing.
6. Apply this normalized feature vector to the neural network for training purpose.
7. Repeat step 1-6 to train neural network to test signature.
8. Perform pattern matching with the test data set present in the hidden layer of neural network
9. Do the classification
10. Using outcome produced by the output layer of the neural network announce signature as genuine or forged.

5.2 ***Flow Diagram For The System***

This diagram shows how the whole system works from image acquisition till result whether signature is genuine or counterfeit.

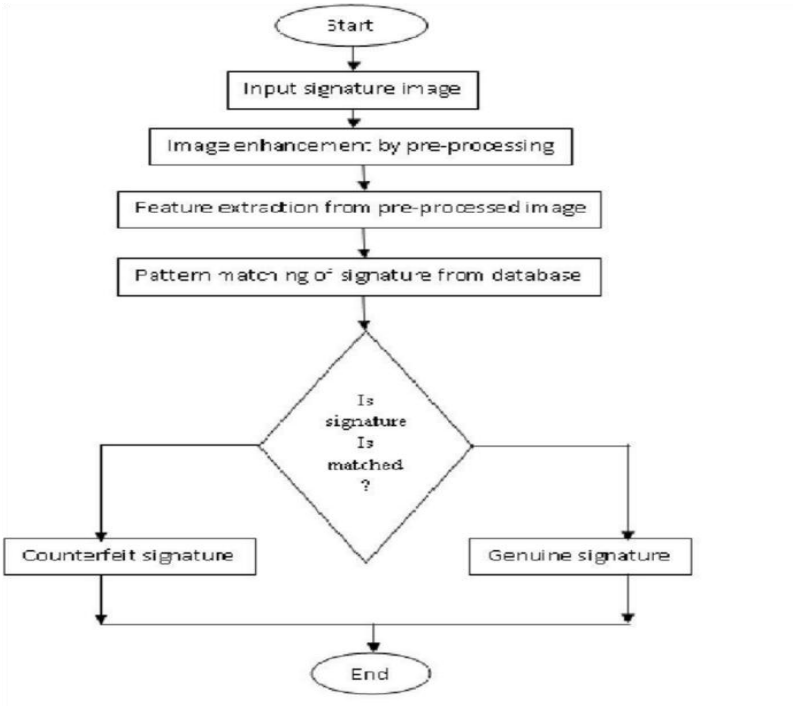

Fig. 10.flow chart of system

VI. Result & Performance Analysis

The result provided in this research for training and testing of the system many signatures are used. The results specified in this paper are acquired using the "Grupo de Procesado Digital de Senales" (GPDS) signature database [2]. 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 [2]. The architecture of neural network used has input layer, hidden layer and output layer.

After relating 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 [2].

False Acceptance Rate (FAR), False Rejection Rate (FRR) and Correct Classification Rate (CCR) are the three constraint used for measuring performance of system. All these constraints are calculated [2] by following equations as:

(7) FAR = (Number of forgeries accepted/Number of forgeries tested) * 100

(8) FRR = (Number of originals rejected/Number of original tested) * 100

(9)CCR=(Number of samples correctly Recognized/Number of samples tested) * 100

These errors for signature verification using artificial neural network [4] are calculated during training using different iterations.

Table 1

Sr. No	No. of iterations	FAR %	FRR %	TER %
1	100	15	12	27.0
2	102	12.5	15	27.5
3	103	12.5	10	22.5
4	104	14.5	12	26.5
5	105	17.5	15	22.5

VII. Conclusion

This paper presents a method of offline signature verification using artificial neural network approach. Signatures are verified based on parameters extracted from the signature using various image processing techniques [8]. For verification of signatures some novel features needs to be extracted. The extracted features are used to train a neural network using error back propagation training algorithm. Our recognition system exhibited 100% success rate by identifying correctly all the signatures that it was trained for [2]. 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. Recognition and verification ability of the systemcan be increased by using additional features in the input data set. This study intends to reduce to a minimum the cases of forgery in business transactions [7].For implementation of above this paper uses Feed Forward Neural Network (FFNN) using Error Back propagation algorithm for recognition and verification of signatures of individuals [7].

References

[1] O.C Abikoye M.A Mabayoje R. Ajibade "Offline SignatureRecognition& Verification using Neural Network", Department of Computer Science University of Ilorin P.M.B 1515, Ilorin, Nigeria, *International Journal of Computer Applications* (0975 – 8887) Volume 35– No.2, December 2011

[2] AshwiniPansare, Shalini Bhatia "Off-line Signature Verification Using Neural Network", *International Journal of Scientific &Engineering Research*, Volume 3, Issue 2, February-2012 1 ISSN 2229-5518

[3] Ms. VibhaPandey, Ms. SanjivaniShantaiya, "Signature Verification Using Morphological Features Based on ArtificialNeural Network", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[4] PaigwarShikha, ShuklaShailja, "Neural Network Based OfflineSignature Recognition and Verification System", Department of Electrical Engineering, Jabalpur Engineering College Jabalpur, MP, INDIA, *Research Journal of Engineering Sciences* ISSN 2278 – 9472, Vol. 2(2), 11-15, February (2013)

[5] Guangyu Zhu, YefengZheng, David Doermann, Stefan Jaeger, "Signature Detection and Matching for Document ImageRetrieval", *IEEETRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE*, VOL. 31, NO. 11, NOVEMBER 2009

[6] Yu Qiao, Jianzhuang Liu, Department of Information Engineering The Chinese University of Hong Kong, Xiaoou Tang, MicrosoftResearch Asia Beijing, China, "Offline Signature Verification Using Online Handwriting Registration"

[7] S.T. Kolhe, S. E. Pawar, Dept. of Computer Engg, AVCOE,Sangamner, India, " Offline Signature Verification Using Neural Network", *International Journal of Modern Engineering Research (IJMER),* Vol.2, Issue.3, May-June 2012 pp-1171-1175

[8] Cemil OZ, Sakarya University Computer Eng.Department, Sakarya, Turkey, FikretErcal,UMR Computer Science Department, Rolla, MO 65401, ZaferDemir, Sakaraya University electric electronic eng. Department sakarya , Turkey, "SignatureRecognition and Verification with ANN"

[9] "What is ArtificialNeuralNetworks" http://www.psych.utoronto.ca/users/reingold/courses/ai/cache/neu ral2.html

[10] Stergiou, C. and Siganos, D. 2003. Neural Networks RetrieveApril 1, 2011 from www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/cs#/report.html

[11] Bradley Schafer, SerestinaViriry "An Offline Signature Verification system" *IEEE International conference on signals and image processing application*, 2009.

[12] Qi, Y., Hunt, B.R., "signature verification using global and grid features." *Pattern recognition* 27, pp.1621-1629, 1994.

[13] Baltzakis H., Papamorkos N., "A new signature verification technique based on a two-stage neurol network classifier.", *PergomanEngineering Application of Intelligence* 14, pp.95-103, 2001.