# HANDWRITTEN SIGNATURE VERIFICATION USING NEURAL NETWORK & ECLUDEAN APPROACH

**Shalu Saraswat[1], Prof. Sitesh Kumar Sinha[2], Prof. Mukesh Kumar[3]**

[1,2,3] *Department of Computer Science , AISECT University Bhopal(M.P.), (India)*

## ABSTRACT

*This is review paper which is based on signature verification which is recognized and verified off-line. The approach for signature verification which will be using is based on artificial neural network which discriminates between (i) original signature and (ii) forgery signature. This approach uses the technique of signature procurement, signature pre-processing, feature point extraction and neural network training and finally verifies the authenticity of the signature. The main objective of this proposed approach is to reduce two critical parameters i.e False Rejection Rate (FRR) and False Acceptance Rate (FAR) . It means that the output is expressed in terms of FRR and FAR and subsequently comparison has been made with existing techniques. This technique will give more productive result than existing techniques.*

***Keywords***: ***FAR (False Acceptance Rate), FRR (False Rejection Rate), Forgeries, Off-line Signature, Artificial Neural Network .***

## I INTRODUCTION

Signature is a handwritten depiction of someones identity. Signature verification is the method which is used for verifying whether the signature is original or duplicate. Signature verification is an important research area in the field of personal authentication. Today's millions of financial transactions are taking place which are verified through signature[4]. Approaches to signature verification fall into two categories according to the acquisition of the data: On-line and Off-line. Online data records the motion of the stylus while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time[4]. In brief this signature is captured during writing and it makes the dynamic information available, whereas the off-line signature is the kind of two dimensional image and is captured when writing process is over [1]. The recognition of human handwriting is important concern about the improvement of the interface between human beings and computers. Off-line processing is quite complex because of the absence of stable dynamic characteristics. Difficulty also arises in offline verification due to unconventional writing styles and segment signature strokes. There are various reasons of variation in the signatures, because of illness, age, geographic location and due to some reason the emotional state

of the person, creates the problem and the signature get varied. All these coupled together cause large intra-personal variation. A system has to be designed which should consider these factors as well as also detect various types of forgeries. Signature is a special case in this area that provides secure means for authentication, attestation authorization in very high security environment[3]. Signature verification system main objective is to distinguish between two classes: the original and the forgery, which are related to Intra i.e variation among signatures of same person is called Intra Personal Variation and Interpersonal variability i.e the variation between originals and forgeries is called Inter Personal Variation [4]. Problems of signature verification are addressed by taking into account three different types of forgeries: Random forgeries, Simple forgeries and Skilled forgeries. Random forgeries produced without knowing either the name of the signer nor the shape of its signature; whereas Simple forgeries are produced knowing the name of the signer but without having an example of his signature; and Skilled forgeries are produced by people who, after studying an original instance of the signature, attempt to imitate it as closely as possible[5]. Clearly, the problem of signature verification becomes more and more difficult when passing from random to simple and skilled forgeries, the latter is difficult for task as even errors can be produced by human beings in several cases. The threshold is used in the proposed technique which dynamically can be changed according to the task. Threshold is the security level which the user can input as per his requirement. The objective of the work is to reduce two fundamental parameters, i.e False Acceptance Rate (FAR) and False Rejection Rate (FRR). Here the results should be expressed in terms of FAR and FRR and subsequently comparative analysis has been made with standard existing techniques. Results obtained by our proposed algorithm will more efficient than most of the existing techniques [9].


**Fig. 1 : Types Of Forgery**

## II. SIGNATURE DATABASE

This research will be conducted using the "GPDS300signature database" offered for those doing research in the field of signature recognition at the Universidad de Las Palmas de Gran Canaria, Spain[7].

## III. PROPOSED METHOD

It has been observed from existing techniques that an offline signature verification process consist of pre-processing on signature. So, it is necessary to pre-process on signature because it helps to verify a signature correctly. Proposed system consists of following steps:

1. Signature Procurement
2. Signature Pre-processing
3. Feature point Abstraction
4. Preparation of Neural Network
5. Signature Analysis
6. Signature Authentication

### 3.1 Signature Procurement

The proposed scheme is based on off-line signature verification so signature which will be done on paper will be scanned by scanner having 300dpi and will be saved in Portable Network Graphics (PNG) format. Signatures will be scanned in gray. Following fig. 2 shows some sample signature from database.

**Fig. 2 : Sample Signature**

### 3.2 Signature Pre-processing

Pre-processing phase is required for verifying the signature correctly. After signature procurement, image may contain noise (extra pen dots), blurriness. It is important and necessary to remove these extra pixel or blurriness for verifying the image correctly. We can remove the noise by using median filter[6][7]. The pre-processing stage includes five steps: Gray Scale, Threshold and invert, Thinning, Boundary Detection and Auto cropping.

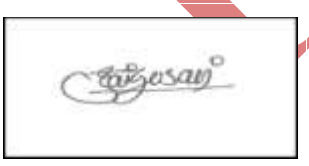

**Fig. 3 Gray Scale**

**Fig.4 Threshold**

**Fig. 5 Thinning**

**Fig. 6 Boundary Detect**

**Fig. 7 Cropping**

### 3.2.1 Gray Scale

In signature verification, scanned image is converted in gray scale. Gray scale is an image in which value of each pixel is a sample and it carries intensity information. Images of this type are composed of mainly gray shades, varied from black at weakest intensity and white at strongest intensity. It also called as monochromatic.

### 3.2.2 Threshold And Invert

Thresholding is the method of converting gray scale image to binary image. i.e. image with only black or white colours. In the simplest implementation, the output is a binary image representing the segmentation. Black pixels correspond to background and white pixels correspond to foreground (or *vice versa*). In simple implementations, the segmentation is determined by a single parameter known as the intensity threshold. In a single pass, each pixel in the image is compared with this threshold. If the pixel's intensity is higher than the threshold, the pixel is set to, say, white in the output. If it is less than the threshold, it is set to black. Threshold image is used for feature extraction.

### 3.2.3 Thinning

Thinning is the transformation of a digital image into a simplified, but topologically equivalent image. It is a type of topological skeleton, but computed using mathematical morphology operators. Thinning eliminate the thickness differences of pen due to the nature of variation of the signatures, because of age, illness, geographic location etc. by making the image one pixel thick.

### 3.2.4 Boundary Detection

It helps to get scanned image with necessary part of signature.

### 3.2.5 Cropping

Cropping refers to the removal of the outer parts of an image to improve framing, accentuate subject matter or change aspect ratio. Depending on the application, this may be performed on a physical photograph, artwork or film footage, or achieved digitally using image editing software. The term is common to

the film, broadcasting, photographic, graphic design and printing industries. This image is ready for feature extraction.

### 3.3 Feature Point Abstraction

Feature point Abstraction is the important phase in signature verification as it is the key to identifying and differentiating a user's signature from one another. This system will be consisting of 60 features. Features extracted in proposed system are based on geometric centre of signature image[1]. Geometric features are based on dimensions of the signature image, shape and depth of signature image. Here geometric features are based on two set of points in 2 dimensional planes. The vertical splitting of the image results thirty features points (v1,v2,v3,……,v30) and the horizontal splitting results thirty features points (h1,h2,h3,……,h30) [2]. Geometric centre of image split image in two halve left and right portion of image. Then again find out geometric centre of left and right part of image and calculate the total number of black pixel. Then divide the two parts in four parts with respect to the black pixel. This process gives 30 features in vertical splitting and 30 features in horizontal splitting[4]. Horizontal splitting of signature image: Horizontal feature points give thirty feature points by splitting image horizontally w. r. t. geometric centre point (h0). Here the geometric centre plays important role. After finding geometric centre of signature image, split the image with horizontal line passing through the geometric centre (h0). Splitting gives two part top and bottom[4]. Find geometric centre point of top and bottom portion say h1 and h2 correspondingly. Split the top and bottom portion with vertical lines through h1 and h2 to divide the two parts into four parts: Left-top, Right-top and Left-bottom, Right bottom parts from which we obtain h3, h4 and h5, h6. We again split each part of the image through their geometric centers to obtain feature points h7, h8, h9,…, h13, h14. Then we split each of the parts once again to obtain all the thirty vertical feature points (as shown in Fig. 8).

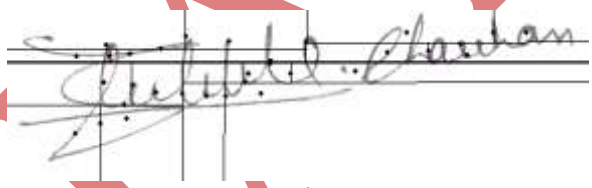

**Fig. 8 : Horizontal Splitting Of Signature Image**

Vertical splitting of signature image: Vertical feature points give thirty feature points by splitting image vertically w. r. t. geometric centre point (v0). After finding geometric centre of signature image, split the image with vertical line passing through the geometric centre (v0). Splitting gives two part left and right. Find geometric centers v1 and v2 for left and right parts correspondingly[4]. Split the left and right part with horizontal lines through v1 and v2 to divide the two parts into four parts: Top-left, Bottom-left and Top-right, Bottom right parts from which we obtain v3, v4 and v5, v6. Again split each part of the image through their geometric centers to obtain feature points v7, v8, v9,….v13, v14. Then split each of the parts once again to obtain all the thirty vertical feature points (as shown in Fig. 9).

**Fig. 9 : Vertical Splitting Of Signature Image**

### 3.4 Preparation of Neural Network

Original signature's extracted 60 features points are then fed to neural network using back propagation algorithm[7]. Back Propogation used in conjunction with an optimization method such as gradient descent. The method calculates the gradient of a loss function with respects to all the weights in the network. The gradient is fed to the optimization method which in turn uses it to update the weights, in an attempt to minimize the loss function. Backpropagation requires a known, desired output for each input value in order to calculate the loss function gradient. It is therefore usually considered to be a supervised learning method.

### 3.5 Signature Analysis

Here signature to be tested is firstly scanned in gray then pre-processed takes place. After pre-processing feature extraction is performed to obtain 60 feature points. These 60 features are then fed to trained neural network using multiple layer feed forward algorithm[5][9].

### 3.6 Signature Authentication

In proposed system, we are obtaining total 60 features based on vertical splitting and horizontal splitting. These features helps us to categorize whether particular signature is genuine or duplicate.Here geometric centre plays an important role to obtain features. So here we use Euclidean distance model for classification. The Euclidean distance is the "ordinary" distance between two points that one would measure with a ruler, and is given by the Pythagorean formula. By using this formula as distance, Euclidean space becomes a metric space. In simple terms we will be using this model for finding distance between feature points[8]. Following Eq. 1 is used to find out distance between pair of feature points. Let V (v1, v2, v3,…., v30) and H (h1,h2,h3,…..,h30) are two set of features points based on vertical and horizontal features point respectively. Here x and y is horizontal and vertical coordinator of pixel.

$$\text{Distance (d)} = \sqrt{(y_2 - y_1)^2 + (x_2 - x_1)^2} \quad (1)$$

After getting Euclidean distance, we calculate weighted average by multiplying with depth of feature point. Here in proposed system depth is set to maximum 5 i.e. geometric centers calculate upto depth 5 in horizontal and vertical splitting. This calculated average will help to classify the signature. Let d1, d2, d3, d4 and d5 are distances calculated by Euclidean distance model based on depth. Individual weighted average (wa) is calculated for horizontal splitting and vertical splitting. Weighted distance average is given by following Eq. 2.

Weighted Average (wa) = d1*5+d2*4+d3*3+d4*2+d5*1 (2)

## IV. PERFORMANCE EVALUATION

False Acceptance Rate (FAR) and False Rejection Rate (FRR) are the two parameters used for measuring performance of any signature verification method. FAR and FRR are calculated by the equations given below:

**False Acceptance Rate (FAR):** False acceptance ratio is the total number of fake signature accepted by the system with respect to the total number of comparison made[1].

$$FAR = \frac{\textit{Number of forgeries accepted}}{\textit{Number of forgeries tested}} \times 100$$

**False Rejection Rate (FRR):** False rejection ratio is the total number of original signature rejected by the system with respect to the total number of comparison made[4].

$$FRR = \frac{\textit{Number of originals rejected}}{\textit{Number of originals tested}} \times 100$$

## V. RESULT AND DISCUSSION

The proposed system will give better result in terms of FAR and FRR than existing techniques. In training section, we will train ANN by original signature's and it will use 60 features which will be based on horizontal and vertical splitting. As mentioned earlier Euclidean distance model will help to calculate the distance between pair of feature point of original signature and testing signature. In testing section, weighted average calculated in vertical and horizontal features and that will be compared with the threshold value. If weighted average of horizontal splitting is less than or equal to threshold, then new signature is acceptable by horizontal splitting. Same process will follow by vertical splitting. New signature i.e. test signature have to satisfy both horizontal splitting and vertical splitting thresholds.

## REFERENCES

[1] Banshidhar Majhi, Y. Santhosh Reddy and D. Prasanna Babu, 2006. Novel features for offline signature verification. Int. J. Comput. Commun Control, 1: 17-24.

[2] Debasish Jena, Centre for IT Education, Bhubaneswar, Orissa, India, 'Improved Offline Signature Verification Scheme Using Feature Point Extraction Method', Journal of Computer Science 4 (2): 111-116, 2008.

[3] K. Bowyer, V. Govindaraju, N. Ratha, 'Introduction to the special issue on recent advances in biometric systems', IEEE Transactions on Systems, Man and Cybernetics— B 37(5)(2007)1091–1095.

[4] Manoj Kumar / International Journal on Computer Science and Engineering (IJCSE), 'Signature Verification using Neural Network', Vol. 4 No. 09 Sep 2012.

[5] Meenakshi K. Kalera, Sargur Srihari and Aihua 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.

[6] Qi.Y, Hunt B.R., 'Signature Verification using Global and Grid Features', Pattern Recognition, Vol. 27, No. 12, 1994, pp. 1621-1629.

[7] Suhail M. Odeh, Manal Khalil, 'Off-line Signature Verification and recognition: Neural Network Approch',2011.

[8] Swati Srivastava, Suneeta Agarwal, 'Offline Signature Verification using Grid based Feature Extraction', 2011.

[9] Vahid Kiani, Reza Pourreza, Hamid Reza Pourezza, "Offline Signature Verification Using Local Radon Transform and Support Vector Machines", International Journal of Image Processing (IJIP), Vol.3, No.5, pp.184-194, 2010.