ISSN (Online): 2230-7893
www.IJCEM.org

# Offline Signature Verification Using Neural Network

**Upasana Dewan[1], Javed Ashraf[2]**

**[1]Department of Electronics & Communication, AFSET, Faridabad, India.**
***dewanupasana@yahoo.com***

**[2]Assistant Professor, Department of Electronics & Communication, AFSET, Faridabad, India.**
***jashraf.jmi@gmail.com***

**Abstract**

Even today an increasing number of transactions, especially financial, are being authorized via signatures, hence methods of automatic signature verification must be developed if authenticity is to be verified on a regular basis.

Verification can be performed either Offline or Online based on the application. Online systems use dynamic information of a signature like velocity, acceleration and pressure 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 geometric features. The features that are used are Token length, Average values, Trend Coefficients and Standard Deviations of observation components. Before extracting the features, pre-processing of a scanned image is necessary to isolate the signature part and to remove any spurious noise present. The system is based on backpropagation neural network and is initially trained using a database of signatures obtained from the individual whose signatures have to be authenticated by the system. Then another set of test signatures of the same person are input to the system to check whether they are genuine or forgery. We either accept or reject the test signatures by using a suitable threshold. If the magnitude of the output of the neural network is less than a pre-defined threshold (corresponding to minimum acceptable degree of similarity), the test signature is verified to be genuine else detected as a forgery.

***Keywords:*** False rejection rate (FRR), False acceptance rate (FAR)

## 1. Introduction

### 1.1 Biometrics

*Biometrics* is an emerging field of technology. It makes use of unique but measurable physical, biological, or behavioural characteristics to perform identity verification of a person [1]. A number of biometric techniques have been proposed for personal identification in the past. Well known biometric methods include iris, retina, face, fingerprint, and signature-based identification .Face recognition, fingerprint recognition, iris scanning and retina scanning fall under the non-vision based techniques. Among the vision-based ones, we can mention voice recognition and signature verification.

Though choice of a proper biometric depends to a large extent on a given application, it should be unique, hard to copy, acceptable by the public, and have lower implementation cost. Signature has been a distinguishing feature for person identification through ages. An important advantage of signature verification compared to other biometric characteristics is its traditional use in many common commercial fields such as E-business, which includes online banking transactions, electronic payments, access control, and so on. Signature is a behavioural biometric; it is not based on physiological properties of the individual, such as fingerprint or face, but on behavioral ones. The attributes like iris, fingerprint and face do not change over time on the average and thus have low intra-class variation, but they require special and relatively expensive hardware to capture the image. Whereas signatures may change over time and it is not nearly as unique or difficult to forge as iris patterns or fingerprints, signature's widespread acceptance by the public, however, makes it more suitable for certain lower-security authentication needs.

### 1.2 Types of Signature verification systems

Signature Verification Systems are often categorized in two major classes: on-line systems and off-line systems.

*Off-line systems* deal with a static image of the signature, i.e. the result of the action of signing. Off-line data is a 2-D image of the signature. In off-line systems, signature samples are scanned into image representation where signature images are acquired with scanners or cameras after the complete signatures have been written. The image acquisition devices like cameras are much smaller and simple to handle, and are becoming ubiquitous in the current computer environment. They capture static features of the image like the X-coordinates and Y-coordinates. Image processing techniques are applied to implement the system. Processing in Off-line systems is complex due to the absence of stable dynamic features. The non-repetitive

nature of variation of the signatures, because of age, illness, geographic location and perhaps to some extent the emotional state of the person, accentuates the problem. All these coupled together cause large intra-personal variation. Nevertheless, offline systems have a significant advantage in that they do not require access to special processing devices when the signature is produced. *On-line systems* work on the dynamic process of generating the signature, i.e. the action of signing itself. On-line data records the dynamic features like motion of the stylus while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time [2]. Online systems use this information captured during acquisition. These dynamic features are specific to each individual and sufficiently stable as well as repetitive.
Online Signature verification requires the use of electronic tablets or digitizers for capturing data. These interfaces have the drawback that they are bulky and complicated to use, increasing the complexity of the whole identification system. Signal processing techniques are applied to implement the system.

### 1.3 Types of Forgeries

Forgery means copying, altering or falsifying written matter for the purpose of defrauding others.
There are three kinds of forgeries –Random, Unskilled and Skilled [3] as shown in Fig. 1

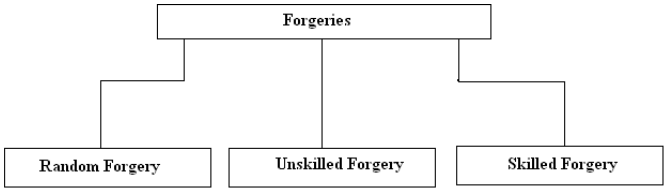


Fig. 1 Types of Forgeries

1. Random forgery—It is produced when the signer knows the name of the victim and produces the signature in his own style. This forgery is easily detected by visual analysis.
Random forgeries are formed without any knowledge of the signature's shape.
2. Unskilled forgery—It is produced when the signer copies the signature in his own style without having any previous experience. They are produced by knowing the name of the signer but without having an example of signer's signature.
3. Skilled forgery—It is produced by looking at the original signature or by having idea about the signature of the victim. Generally this kind of forgery is generated by professional persons who have experience in copying the signature.

The Random and Unskilled forgeries are easy to catch but skilled forgery is hard to detect.

## 2. Proposed System

A robust system has to be designed which should be able to judge whether the signature is genuine or a forgery. The system should neither be too sensitive nor too coarse [4].
The FRR and the FAR are used as quality performance measures. The FRR is the ratio of the number of genuine test signatures rejected to the total number of genuine test signatures submitted. The FAR is the ratio of the number of forgeries accepted to the total number of forgeries submitted.
It should have an acceptable trade-off between a low FAR and a low FRR.
The design of the proposed system requires four steps:

1. Data acquisition
2. Pre-processing
3. Feature extraction
4. Matching process/Decision-making

Initially, the signature image is acquired using a digital camera. Then it is pre-processed to remove any spurious noise present to be suitable for extracting features. Then the pre-processed image is used to extract relevant features that can distinguish genuine and forgery signatures of a person. Then these features are fed at the input of the neural network for training and testing purposes. Section 3 deals with the pre-processing steps and Section 4 explains the features that are extracted followed by the implementation details in Section 5. The conclusion follows in Section 6.

## 3. Pre-processing

Pre-processing is generally done to eliminate any noise if they get induced in the data acquisition phase. For this, operations of image processing are applied. It is done in the following steps:
1) Loading the image: The colour image file (jpg/tiff/bmp format) is loaded and intensity levels of Red-Green-Blue (RGB) pixels are stored as a 3-D array in an m-file in Matlab.

2) Resizing the image: The image is resized to 128 rows and 128 columns.

3) Converting to gray scale: The coloured RGB (3-D with intensities from 0 to 255) image is converted to gray scale (2-D with intensities between 0 and 1).

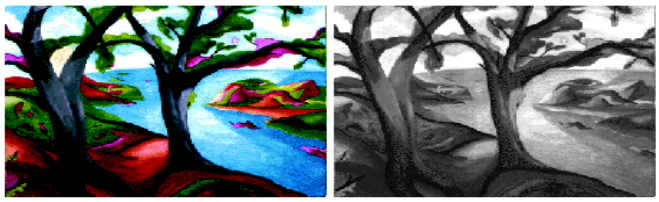

Fig. 2 An example to show conversion from RGB to Gray

4) Noise Removal/ Binearization/ Converting to Black and White (0-1): Gray scale image pixels contain values between 0-1. The noise is eliminated by using a user defined threshold (0.5 in this case) which distinguishes different gray colour intensities between 0 and 1 to take crisp values, which can be either 0 or 1.

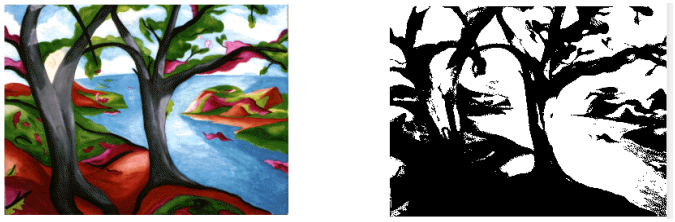

Fig. 3 An example of how light colours are converted to white and other dark colours are converted to black.

5) Thinning of signature: The signatures are thinned in order to make the recognition invariant to the thickness of the pen.

6) Extracting the black pixels from the grid and defining the centre of mass: It is done by calculating the standard deviation and mean along with the x and y coordinates separately in the standard user defined grid.

7) Rotation of signature: It may happen that the same authenticator may use different elevation angles at every other incidence w.r.t origin in the x-y grid. Therefore, the angle of rotation must be standardized.

## 4. Feature Extraction

The features used for signature recognition are: token length, mean, Standard Deviation and Trend Coefficient values of observation components. They are explained below:

1) **Token length:** The number of token points **N** in the signature sample.

2) **Average values** of observation components
$\overline{s_j} = 1/N \sum_{k=1}^{N} s_j(k)$ ; j=1,2,3...

3) **Standard deviations** of observation components
$\sigma_j = \sqrt{\overline{s_j^2} - \overline{s_j}^2}$ ; j=1, 2, 3…

4) **Trend coefficients:** They are the slopes $\alpha_j$ of trend lines of each observation component. The trend lines are given by $s_j^0(k) = \overline{s_j} - \alpha_j k$ ; j=1, 2, 3… where

$\alpha_j = \rho_j \sigma_j / \sigma_k$

$\rho_j = (\overline{ks_j} - \overline{k}\,\overline{s_j})/\sigma_j \sigma_k$

$\overline{ks_j} = 1/N \sum_{k=1}^{N} k s_j(k)$ $\sigma_k^2 = \overline{k^2} - \overline{k}^2$

$\overline{k} = \frac{1}{2} N(N+1)$

$\overline{k^2} = \frac{1}{6} N(N+1)(2N+1)$

The feature vector has 12 components. The first three of them are the token sizes of angle, x and y i.e., N. It is the same for all the three, i.e, angle, x and y coordinates for a signature. The second three of them are the means of angle, x and y coordinates. The next three of them are the variances of angle, x and y coordinates. The last three of them are the trend coefficients of angle, x and y coordinates.

`

## 5. Matching Process

A total of 20 genuine and 20 forgery signatures of a person whose signature needs to be authenticated are taken as the signature database. Out of these, 15 genuine signatures are used to train the neural network about the genuine signature of a person and 5 genuine signatures are used to test the performance of the network for testing the genuine signatures. Similarly, 15 forgery signatures are used to train the neural network about the forgery signature of a person and 5 forgery signatures are used to test the performance of the network for testing the forgery signatures.

The feature vectors are obtained for each of these signatures in the feature extraction process. The neural network learns about the signature in the training phase in which the feature vectors of the signatures act as inputs to the network. In the testing phase, the network's performance is evaluated. Based on the closeness of the test input to the learned input, it produces an output between 0 and 1. We either accept or reject the signatures by using a suitable threshold. In the experiments we will use a threshold of 0.5. If the magnitude of the output is greater than 0.5, the test input is accepted and if it is less than 0.5, the input is rejected.

## 5.1 Expected Ideal output performances

### 5.1.1 For ideal Genuine case:

The FRR is the ratio of the number of genuine test signatures rejected to the total number of genuine test signatures submitted. The FRR should be 0%, i.e, no genuine signatures should be rejected. Figure 4 illustrates this fact.

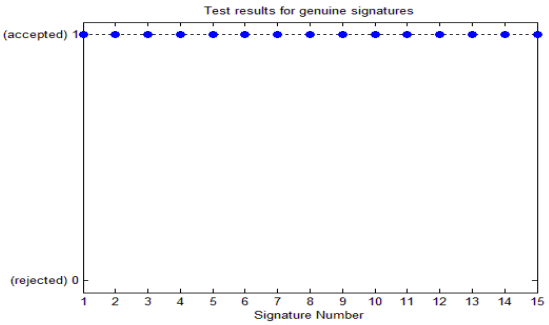


Fig. 4 FRR of 0%

### 5.1.2 For ideal Forgery case:

The FAR is the ratio of the number of forgeries accepted to the total number of forgeries submitted. The FAR should be 0%, i.e, no forgery signatures should be accepted. Figure 5 illustrates this fact.

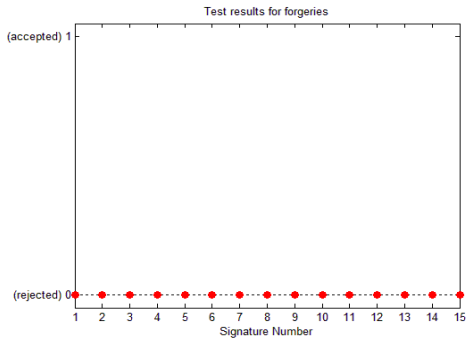


Fig. 5 FAR of 0%

**5.2 Non-Ideal Cases:** In practical cases, FAR and FRR may not be 0%.

**5.2.1 For non-ideal Genuine case:** Figure shows 3 genuine signatures rejected out of 15 giving an FRR of 3/15*100 = 20%.

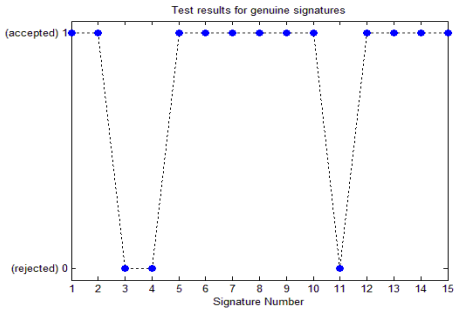


Fig. 6 FRR of 20%

**5.2.2 For non-ideal Forgery case:** Figure shows 1 forgery signature accepted out of 15 giving an FAR of 1/15*100 = 66.7%.

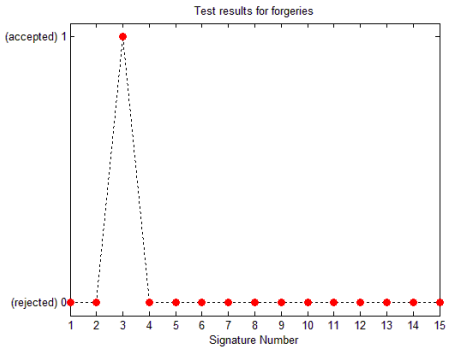


Fig. 7 FAR of 66.7%

## 6. Implementation Details

A **Backpropagation Neural Network** with the following parameters is trained with 5 genuine and 5 forged signatures of a user:

1. Mode of Processing: Batch Processing
2. Number of Neural Network layers = 3
3. Activation function of hidden layer = Log-sigmoidal
4. Activation function of output layer = Linear
5. Number of inputs, n = 6
6. Number of neurons in hidden layer, m = 20
7. Number of outputs = 1(b/w 1 and 0)
8. Learning rate, lr = 0.08
9. No. of epochs = 25

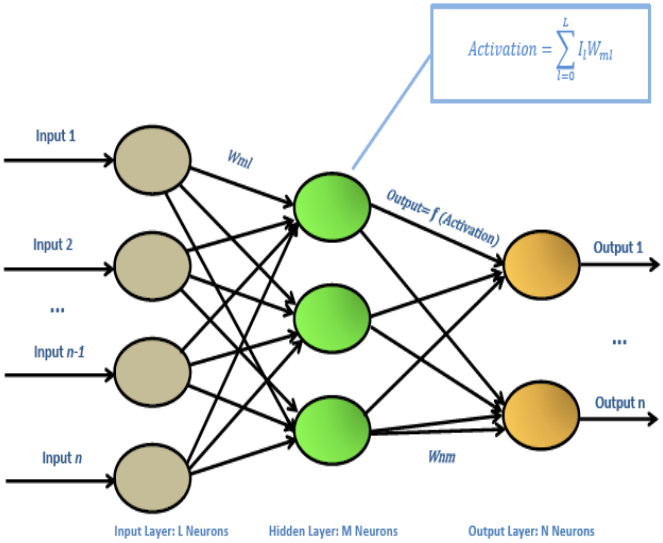


Fig. 8 Backpropagation Neural Network

## 7. Conclusion

The algorithm uses simple static features like mean, standard deviation etc. that effectively serve to authenticate signatures. The system is expected to provide zero percent FAR and FRR for casual forgeries. A larger database for training can reduce false acceptances as well as false rejections to build systems with high accuracy. The parameters like learning rate, number of epochs and mode of training of the backpropagation neural network can be varied to improve the results. Furthermore, other feature vectors obtained during feature extraction process can be used to train the network to improve it's accuracy.

## References

[1] Biometrics the Ultimate Reference by John D. Woodward-Jr., Nicholas M. Orlans, Peter T. Higgins (Dreamtech Press).
[2] Sansone and Vento, "Signature Verification: Increasing Performance by a Multi-Stage System", Pattern Analysis & Applications, vol. 3, pp. 169–181, 2000.
[3] Qi.Y, Hunt B.R., "Signature Verification using Global and Grid Features", Pattern Recognition, Vol. 27, No. 12, 1994, pp. 1621-1629.
[4] Plamondon.R., Brault J.J., "A Complexity Measure of Handwritten curves: Modeling of Dynamic Signature Forgery", IEEE Trans. on Systems, Man and Cybernetics, Vol. 23, No.2, 1993, pp. 400-413.