# Signature Detection and Verification using Softcomputing

Kuldipsinh A Vala
PG Student
Department of Electronics & Communication
School of Engineering, R K University
Rajkot, India

N. P. Joshi
Assistant Professor
Department of Electronics and Communication
School of Engineering, R K University
Rajkot, India

***Abstract* — The Signature Recognition and Verification system is used to recognize and verify individual's handwritten signature. Now a day's handwritten signature is one of the most widely accepted personal attributes for identity verification. Signature verification provides authorization in financial and business transaction. Signature verification finds its application in the field of net banking, passport verification system, provides authentication to a candidates in public examination from their signatures, credit cards, bank cheques. Therefore it has long been the target of fraudulence. Therefore, with the growing demand for processing of individual identification faster and more accurately, the design of an automatic signature system is needed. This electronic document represents a brief survey on different off-line signature recognition and verification methods.**

***Keywords— Verification, Recognition, Forgeries, Handwritten Signature, Neural networks, Systems, Off-line signature Recognition and Verification.***

***Introduction***

Handwritten signature is one of the most widely accepted personal attributes for identity verification. The major area of research on signature verification is in the field of pattern recognition and image processing. It is also widely used in the fields of finance, access control and security. Handwritten signature has long been the target of frauds. Therefore, with the growing demand for processing of individual identification faster and more accurately, the design of an automatic signature system is needed. Signature verification system is categories in two separate classes that is off-line signature verification system and online signature verification system.

## I. INTRODUCTION

### *A. Off-line verification* [1]:

In off-line verification system verification is performed off-line. Data acquisition been done by scanning individual handwritten signature. That scanned signature will be used for signature verification process.

### *B. On-line Verification [1]:*

In on-line verification system verification is performed on-line. Here data acquisition done by touch screen, digitizer and stylus. This instrument will generate dynamic values such as location, pen pressure, co-ordinate values, speed of signature or time etc.

## II. SIGNATURE VERIFICATION CONCEPT

A handwritten signature is personal attribute ment to be used for identification. The signature verification processes of any person have to be done by analysis of his or her signature. Through which a system can differentiate a genuine signature from a forgery signature [2].
There are two type of error that will define the precision of the signature verification system viz. FAR (False Acceptance Rate) and FRR (False Rejection rate).

*FRR (False Rejection rate)* [3]
The percentage of genuine signatures rejected from genuine signature tested as forgery which is called False Rejection Rate.

$$FRR = \frac{\text{No. of Genuine Signatures Rejected}}{\text{No. of Genuine Signatures Tested}}$$

*FAR (False Acceptance Rate)* [3]
The percentage of forgery signatures accepted from forgery signature tested as genuine which is called false acceptance rate.

$$FAR = \frac{\text{No. of Forgery Signatures accepted}}{\text{No. of Forgery Signatures Tested}}$$

## III. TYPES OF FORGERIES

In handwritten signature verification the forgeries may be categories in 3-type given below [4].

### *A. Random forgery*:

The signature uses the name of a person randomly in his own style to write a forgery known as the simple forgery or random forgery. In majority cases this forgery occurs, although they are very easy to detect even by naked eye.

*B. Unskilled forgery:*

The signers sign the person's signature in his own style without any knowledge of spelling. This type of forgery is known as unskilled forgery.

*C. Skilled forgery:*

The forgeries are created by professional person who have experience in copying the signature called skilled forgery.

Based on the various skilled levels of forgeries, it can also be divided in to six different subsets:

1) Random forgery 2) Causal forgery 3) Simulated forgery 4) Unskilled forgery 4) Targeted forgery 6) skilled forgery

*D. Basic steps of signature verification*

Signature verification system generally consists of four Basic components:

1. *Data acquisition*
2. *Pre-processing*
3. *Feature extraction*
4. *Recognition and verification*

*1) Data acquision :*

The data acquisition phase involves capturing all the physical features from the acquisition device and converting it into numerical data that can be manipulated by the computer. In this work, colored signature images (both genuine and forgery) have been collected from different people using a camera and are stored in JPG (Joint Photographic Experts Group) format. For example, some of the genuine and forgery signatures of a single user are shown in Fig.1 [5]

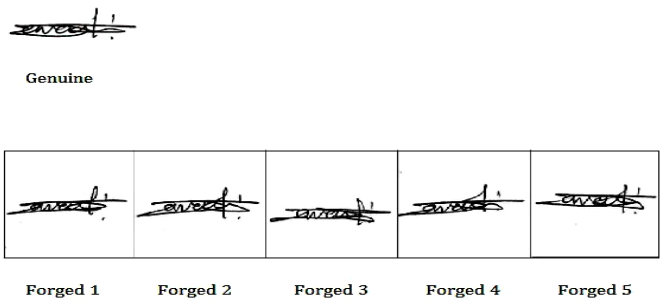


Figure 1: Figure shows colored genuine and forged images of user

A total of 20 signatures were collected from each person to have samples of intra-personal variations. All these sample signatures were scanned and stored as genuine signatures. Forgeries were obtained from volunteers who were asked to imitate genuine signatures. 20 samples for each person was collected, scanned and stored as forgery signatures. Thus the database used for testing the proposed system consists of 20 people's 10 genuine samples and 10 random forgery samples for each person. The size of the database is 400 samples.

*2) Pre-processing:*

There are a few pre-processing steps, aimed to improve the verification performance of a system. The scanned signature is converted to a gray scale image by threshold. The image was resized to a convenient size of 200 pixels in height by 200 pixels in width. Since the signature consists of black pixels on a white background, the image is then complimented to make it a white signature on a black background [6].

Figure 2: Original scanned signature

Figure 3: Segmented and Binaries signature

*3) Feature extraction methodes*

Feature extraction defined by, extracting the information from the raw data which is most relevant for classification stage. This data can be minimized within-class pattern variation and increases the inter-class variations [7].

Different features extraction techniques have been reported for off-line signature verification systems. Discrete Radon Transform (DRT) method, Discrete Wavelet Transform (DWT) technique and Inverse Fourier Transform (IFT) are used to extract global features from a static image of signature in previous systems. Also graphometrics features: Axial slant angle, pixel distribution, pixel density, centre of gravity and stroke curvature are extracted from a static image of signature using grid segmentation method. In, vertical and horizontal centre points are extracted from a static image of signature using vertical and horizontal points splitting technique whereas in, gradient, structural and concavity features are extracted from a binary signature image for verification [8][11][12][13][14].

## IV. PROPOSED METHODES

*1) Self Organizing Map (SOM):*

Self-Organizing Maps (SOM) were introduced by a Finnish Professor, Teuvo Kohonen in 1982, thus SOM's are also sometimes referred to as Kohonen Maps. Self-Organizing Maps are a subtype of Artificial Neural Network. They are trained using unsupervised learning to produce low dimensional representation of the training samples while preserving the topological properties of the input space. Thus, SOM are reasonable for visualizing low-dimensional views

of high-dimensional data, akin to multidimensional scaling [9] [10].

The architecture of self organizing map is shown in figure 4. The key principle for map formation is that training should take place over an extended region of the network centered on the maximally active mode. Hence, the concept of "neighborhood "should be defined for the net. Thus may be fixed by the spatial relation between nodes within the self organizing layer [5].

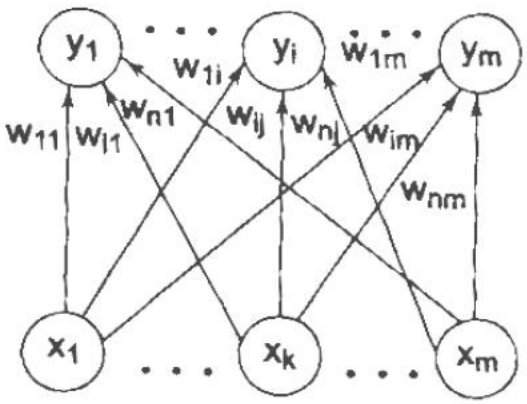


Figure 4: Kohonen Self - Organizing Map

Details of simple competitive learning SOM NN are shown in Figure 7. Each jth output node has connections from all input nodes, with connection strengths given by the n-dimensional vector
wj={wj,1,.....,wj,n}.these weights are initially assigned random values , and their values change during the learning process. The input vectors to be clustered are presented to the network. The neighborhood Nj(t) contains nodes that are within a topological distance of D(t) from node j at time t , where D(t) decrease with time and does not refer to Euclidean distance in input space. Weights change at time t at a rate
(t) which decreases with time. If j is the winner node,
Nj (t) = {j} {neighbors of j at time t},
And i is the input vector presented to the network at time t, then the weight change rule is given by the equation (1).

$$wl(t+1) = \begin{cases} wl(t) + \eta(t)\,(i - wl(t)) & if\ \ l \in Nj \\ wl(t) & if\ \ l \notin Nj \end{cases} \cdots \quad (1)$$

Initially, the weights and learning rate are set. The input vectors are given, based on the initial weights, the winner unit is calculated either by Euclidean distance method or sum of the product method. An epoch (iteration) is said to be completed once all the input vectors are presented to the network. By updating the learning rate, several epochs of training may be performed.

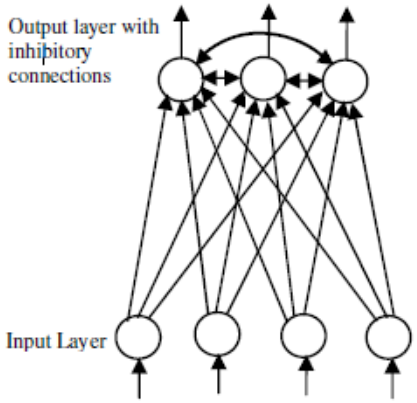


Figure 5: Simple Competitive Learning Network

*2) SVM (Support Vector Machine):*

Support Vector Machines (SVMs) are machine learning algorithms that uses a high dimensional feature space and estimate differences between classes of given data to generalize unseen data [16]. Signature verification begins with features extraction from a signature. SVM are used to classify the features extracted from signature, which will be used in generalizing process of signature verification. Although SVM algorithm has excellent ability in generalizing signature image, but has some drawbacks including the difficulty of determining kernel to be used, classification using SVM requires considerable time and space [15].

To perform signature Verification we can use the technique of Support Vector Machines since it can handle data sets with large number of attributes and has a better generalization performance than other methods [17].
The principle behind SVM relies on a linearly separable feature space .The objective is to find the optimal hyper plane that is uniquely determined by a set of the vectors (or data points) at equal distance from the hyper plane – the support vectors [17] [18].

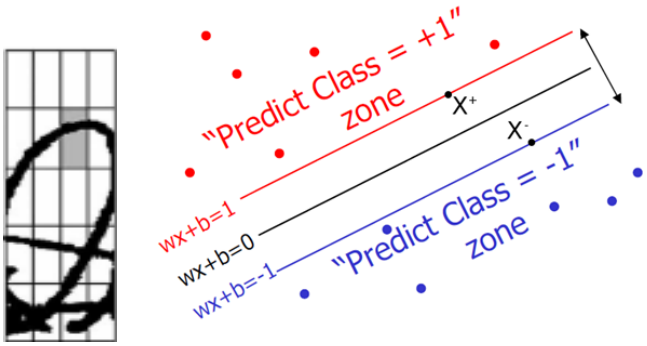


Figure 6: Segmented cell and a sample linear SVM classifier and its margin [19].

*RBF kernel:*

In machine learning, the (Gaussian) radial basis function kernel, or RBF kernel, is a popular kernel function used in support vector machine classification [20].

The RBF kernel on two samples x and x', represented as feature vectors in some input space, is defined as

$$K(x, x') = \exp - \frac{\| x - x' \|^2}{2\sigma^2} \ldots\ldots (2)$$

$\| x - x' \|^2$ , May be recognized as the squared Euclidean distance between the two feature vectors, is a free parameter.

An equivalent, but simpler, definition involves a parameter,

$$\gamma = -\frac{1}{2\sigma^2}$$

Therefore,

$$K(x, x') = \exp (\gamma \| x - x' \|^2).$$

## RESULT ANALYSIS

A total of 20 signatures were collected from each person to have samples of intra-personal variations. All these sample signatures were scanned and stored as genuine signatures. Forgeries were obtained from volunteers who were asked to imitate genuine signatures. 20 samples for each person was collected, scanned and stored as forgery signatures. Thus the database used for testing the proposed system consists of 20 people's 10 genuine samples and 10 random forgery samples for each person. The size of the database is 400 samples.

In MATLAB, neural network training tool is used for simulations using the following specifications.

*For SOM*:
No. of Iteration: 1000
No. of NN layers: 1
No. of inputs n=1
No. of outputs =1
The algorithm takes Training time: 127.5018
Execution time: 132.0113
Processor: 1.9 GHz, RAM: 2 GB
Fig.8 shows the true detected image from the database and fig. 9 shows SOM Layer weights that shows magnitude and layer weight of an input image.

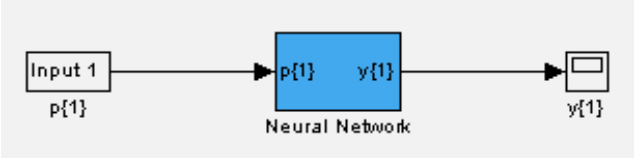


Figure 7 : Simulink block model of the SOM neural network

As shown in Fig. 7 the input is vector p{1}. The processing stage is the Neural Network block and the output result is y{1}, shown in the scope. The neural network block consists of only one layer which connects the input and the output.


Figure 8: Detected signature

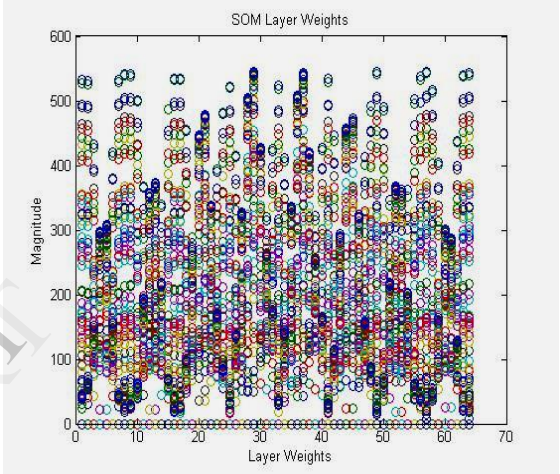


Figure 9: SOM Layer Weights

*For SVM:*

A total of 20 signatures were collected from each person to have samples of intra-personal variations. All these sample signatures were scanned and stored as genuine signatures. Forgeries were obtained from volunteers who were asked to imitate genuine signatures. 20 samples for each person was collected, scanned and stored as forgery signatures. Thus the database used for testing the proposed system consists of 20 people's 10 genuine samples and 10 random forgery samples for each person. The size of the database is 400 samples.

There are 3 step verification processes in SVM:

1. Train
2. Test
3. Exit

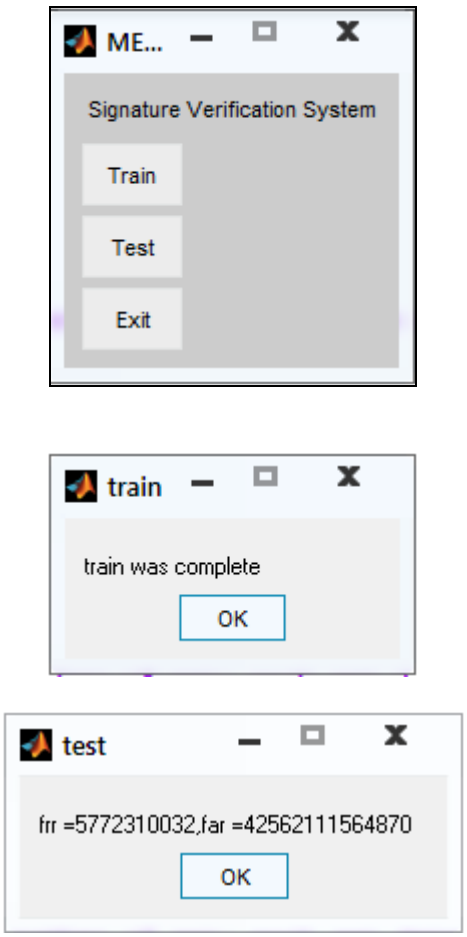


Figure 10: 3 Steps of Verification

Table 1: FAR and FRR for SVM

| NO | Type of Error | | |
|---|---|---|---|
| | ***Proposed System*** | ***FAR*** | ***FRR*** |
| 1. | SVM | 4.2 | 5.7 |

CONCLUSION

In this paper, a machine-learning single-layered Neural Network model (SOM) is discussed for signature Detection for 20 different users. The proposed concept can be extended in a more generalized form for any number of multiple users with a better tuned multi-layered NN model. Also, we were able to extract decent performance from our signature verification system using SVM for 20 different users of 200 genuine and 200 forged signatures. The result can be evaluated using FAR (false acceptance rate) and FRR (false rejection rate).

REFERENCES

[1] A.Sanmorino,S.Yazid,"A Survey for Handwritten Signature Verification", IEEE 2012.

[2] J.Singh,Dr. M.Sharma,"A Survey on Offline Signature Recognition and Verification Schemes", IOSR Journal of Electronics and Communication Engineering (IOSRJECE) ISSN : 2278-2834 Volume 2, Issue 3 , pp. 34-38,2011.

[3] 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.

[4] M. Hanmandlua, Mohd. H. Mohd.Y. , V. K. Madasuc," Off-line signature verification and forgery detection using fuzzy modeling", Pattern Recognition Society. Pattern Recognition 38, pp. 341 – 356, Published by Elsevier Ltd (2005).

[5] K.V.Lakshmi, S.Nayak," Off-line Signature Verification Using Neural Networks", IEEE 2012.

[6] S. Paigwar & S. Shukla" Neural Network Based Offline Signature Recognition and Verification System",Research Journal of Engineering Sciences Vol. 2(2), pp. 11-15, February (2013) .

[7] [5] N. Y. Choudhary, Mrs. R. Patil, Dr. U. Bhadade, Prof. B. M Chaudhari, "Signature Recognition & Verification System Using Back Propagation Neural Network", International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) , ISSN: 2319-4413 Volume 2, No. 1, January 2013

[8] Dr. D. Samuel,prof. I.samuel,"novel feature extraction technique for off-line signature verification system",International Journal of Engineering Science and Technology Vol. 2(7), 2010, pp. 3137-3143.

[9] A.Pacut and A.Czajka," Recognition of human signatures", Proceedings of the International Joint Conference on Neural Networks Washington, DC, USA (2001).

[10] K .Phua, J.Chen, T. Huy Dat and L.Shue," Heart, Sound as a biometric", Pattern Recognition, 41(3), 906919 (2008)

[11] F. V. Jose, S. Angle and A. B Moreno, (2003): Robust off-line Signature Verification using compression networks and positional cuttings", Universidad Rey Juan Carlos.

[12] E.J.R. Justino, F. Bortolozzi and R. F Sabourin, (2002): "The interpersonal and intrapersonal variability influences on Off-line signature verification using HMM", Proc. XV Brazillian Symposium on Computer Graphics and Image Processing. Vol.1, pp. 197-202.

[13] E. Justino, F. Bortolozzi and R. Sabourin, (2005): Comparison of SVM and HMM classifiers in the off-line signature verification", Pattern Recognition Letters, pp. 1377-1385.

[14] M. Banshider, R .Y Santhosh and B .D Prasanna (2006): Novel features for off-line signature verification" International Journal of Computers, Communications & Control ,Vol. 1 , No. 1, pp. 17-24.

[15] A.Sanmorino, S.Yazid, "A Survey for Handwritten Signature Verification", IEEE 2013.

[16] A. Pansare, and S. Bhatia, "Handwritten Signature Verification using Neural Network," IJAIS – ISSN: 2249-0868, Vol. 1 – No. 2, pp. 44-49,Januari 2012.

[17] Audet, S., Bansal, P., Baskaran, S.,"Offline Signature Verification Using Virtual Support Vector Machines", ECSE 526 - Artificial intelligence, final project, april 7, 2006 (revised may 7, 2006).

[18] R. Fisher, S. Perkins, A. Walker, and E. Wolfart, "Hypermedia Image ProcessingReference(HIPR2)",http://homepages.inf.ed.ac.uk/rbf/HIPR2/, 2004.

[19] A. W. Moore, "Support Vector Machines, Tutorial Slides," 2001, http: //www.autonlab.org/tutorials/svm.html

[20] http://en.wikipedia.org/wiki/Radial_basis_function_kernel.