SIGNATURE RECOGNITION AND VERIFICATION USING ARTIFICIAL NEURAL NETWORKS: A COMPARATIVE STUDY

Nidhi Arora

ABSTRACT

The paper presents the comparative analysis of signature recognition and verification using Neural Networks. Three well-known and widely used Neural Networks viz. Support Vector Machines, Multilayer Perceptron and Radial Basis Function Network have been used. Each network differs from the other in the manner it approaches the signature given for recognition and verification. A signature database is collected using intrapersonal variations for evaluation. For every 6 training examples, 4 are used to test the signatures based on various features like false rejection rate, false acceptance rate, equal error rate, and average error rate. The merits and demerits of all the approaches are evaluated and hence the results of numerical experiments are given and analyzed in the paper. In this paper an off-line Recognition and Verification is done with the objective of performance comparison. The comparison of the three networks is done with respect to the complexity of the structure as well as the accuracy of expected results so that the forgeries can be minimized.

Keywords: Neural Networks, offline Signature Verification, Multilayer Perception, Support Vector Machine, Radial Basis Function Network.

1. INTRODUCTION

Many applications in today's world check for user identity by asking a password or a pin code for authentication of a valid user. Making emerging applications interactive for public use and maintaining their security at the same time has become a challenge for the organizations. Some complicated and computationally expensive authentication methods like face, eye and fingerprint recognition have become popular. A technique that is cheap, reliable and importantly un-intrusive is most suitable for commercial use. The only technique that meets all three requirements is handwritten signature verification.

The signature recognition is the process of verifying the writer's identity by checking the signature against samples kept in a database. The result of this process is usually a number between 0 and 1 which represents a fit ratio; 1 for match and 0 for mismatch or in percentage terms. The threshold used for confirmation/rejection decision depends on the nature of the application. Although handwritten signatures are by no means the most reliable means of personal identification, signature verification systems are inexpensive and non-

intrusive. Handwritten signatures provide a direct link between the writer's identity and the transaction and are therefore perfect for endorsing transactions. It is well known that no two genuine signatures of a person are precisely the same and some signature experts note that if two signatures written on paper were same, then they could be considered as forgery by tracing [6]. A signature database of around 1000 signatures was prepared from different individuals which are then scanned and stored as a BMP file. Throughout the paper, false rejection rate (FRR), false acceptance rate (FAR), equal error rate (EER), and average error rate (AER) are used as performance comparison measure for offline signatures, discussed in later section.

The paper is organized as follows. Section 3 briefs about the process of signature recognition, in section 4 the neural networks MLP, SVM and RBF are discussed along the reasons for choosing them for comparative study, in section 5 the performance measures criterions are described and at last section 6 shows the study results followed by conclusions.

2. SIGNATURE RECOGNITION AND VERIFICATION

Signatures are composed of special characters and flourishes and therefore most of the time they can be unreadable. Also intrapersonal variations and interpersonal differences make it necessary to analyze them as complete images and not as letters and words put together [4].

Before we compare the networks, a clear distinction should be made between signature verification systems and signature recognition systems. A signature verification system merely decides whether a claim that a particular signature belongs to a specific user is true or false. A signature recognition system, on the other hand, has to decide to which of a certain number of users a particular signature belongs. A signature verification system typically focuses on the detection of one or more category of forged signatures. A killed forgery is produced when the forger has unrestricted access to one or more samples of the writer's actual signature. A casual forgery or a simple forgery is produced when the forger is familiar with the writer's name, but does not have access to a sample of the actual signature stylistic differences are therefore prevalent. A random forgery or zero effort forgery can be any random scribble or a signature of another writer, and may even include the forger's own signature. The genuine signatures and high quality forgeries for other writers are usually considered to be forgeries of this type. The following figure shows the sample signatures used for verification.

Fig. 1: Sample Signatures used for verification

Signature recognition can be done both offline and online. In offline systems, signatures are digitized using a handheld scanner and the completed writing is stored as an image [4]. These images are referred to as static signatures. Offline systems are of interest in scenarios where only hard copies of signatures are available and a large number of documents need to be authenticated. In the online case, a special pen is used on an electronic surface such as a digitizer combined with a liquid crystal display. Apart from the two-dimensional coordinates of successive points of the writing, pen pressure as well as the angle and direction of the pen are captured dynamically and then stored as a function of time. In this paper, we focus on the offline signature recognition and verification.

3. SIGNATURE RECOGNITION PROCESS

The process of signature recognition and verification is divided into two major parts: Training signatures, Verification or recognition of given signature. The block diagram of the system is shown in Figure 2.

The preprocessing step includes four steps: Background elimination, noise reduction, width normalization and skeletonization. It is applied both in training and testing phases. The purpose in this phase is to make signatures standard and ready for feature extraction.

In background elimination, data area is cropped to capture and distinguish the signature from the background. Noise reduction is one of the most important processes. Signatures are often corrupted due to positive and negative impulses stemming from decoding errors or noisy channels. It may also be degraded because of the undesirable effects due to illumination and other objects in the environment. The signature width is adjusted to a default value and the height will change without any change on height-to-width ratio in width normalization. At last, thinning is applied to the signature to eliminate the thickness differences of pen by making the image one pixel thick.

4. ARTIFICIAL NEURAL NETWORKS UNDER CONSIDERATION

Artificial Neural nets are the future of computing. A neural network is composed of biological neuron like units and weighted unidirectional connections between them. In some neural nets, the number of units may be in thousands. The output

of one unit typically becomes an input for another. There may also be units with external inputs and/or outputs. Although many neural networks are available which have been used in past for signature recognition and verification, only MLP, SVM and RBF are considered here.

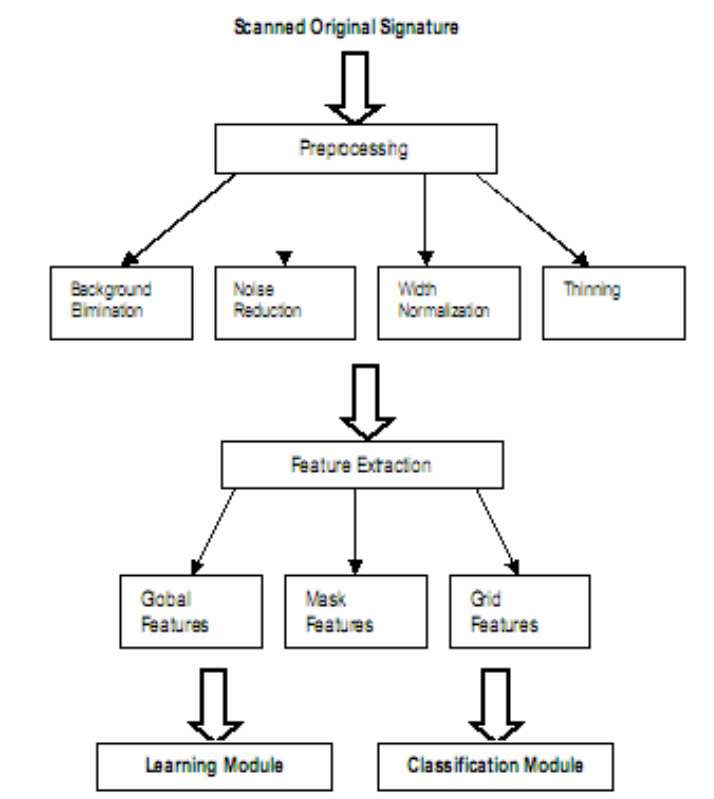

Fig.2: Signature Recognition and Verification Process

MLP takes longer time to give results but it discriminates the inputs in a better way as compared to other Networks. SVM is used for signature recognition and verification if input data is separable with a wide margin using functions from the hypothesis space [8]. With RBF there is a trade-off between performance and memory requirement. It is widely accepted network for signature recognition and verification because of its good performance but it requires more memory.

A. Multilayer Perceptron Network

A Multilayer Perceptron consists of networks of large number of processing units called neurons with connections between them. Multilayer Perceptrons include two phases of computation Forward pass and Backward Pass. In forward pass, the input pattern presented to the network generates a forward flow of activation from the input to the output layer i.e. run the NN and compute the error for each neuron of the output layer.

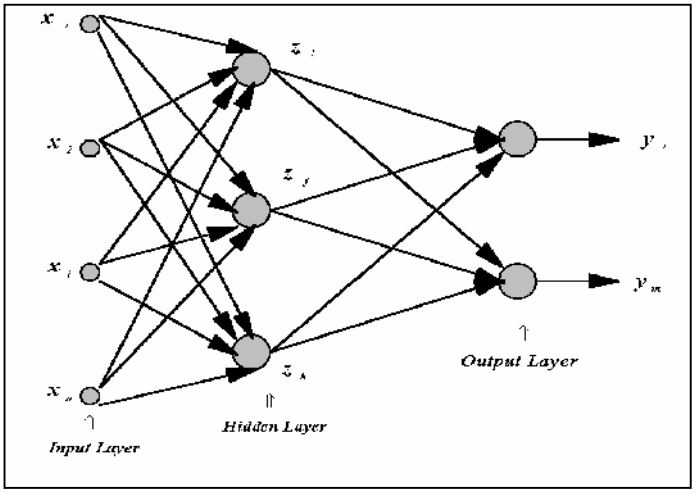

Fig.3: A Feed-Forward Multilayer Perceptron

The second pass is Backward pass in which the errors in the network's output generate a flow of information from the output layer backward to the input layer i.e. start at the output layer, and pass the errors backwards through the network, layer by layer, by recursively computing the local gradient of each neuron.

B. Support Vector Machines

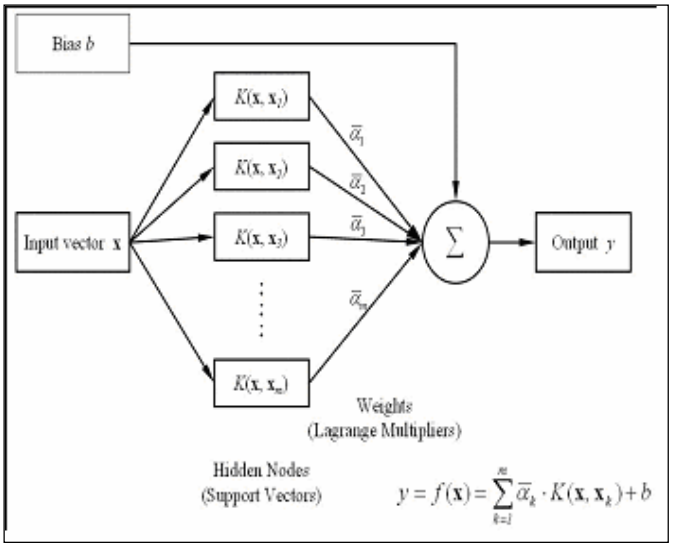

Fig.4: Support Vector Machine

Support Vector Machine (SVM) is a linear machine working in the highly dimensional feature space formed by the nonlinear mapping of N-dimensional input vector x into a K-dimensional feature space (K>N) through the use of a mapping Ø(x).

The way in which SVM network is created differs for the classification and regression tasks, although both transform the learning task to the quadratic problem. SVMs are said to be universal learners [1].

C. Radial Basis Function Network

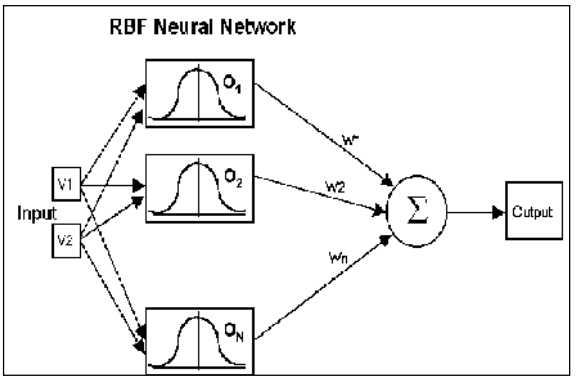

Fig.5: Radial Basis Function Network

The RBF neural network has three layers, the input layer, the hidden layer and the output layer. The hidden layer consists of an array of computing units called hidden nodes. Each hidden node contains a centre c that is a parameter vector of the same dimension as the input data vector x, and calculates the Euclidean distance between the centre and the network input vector x defined by $\|x(t) - c_j(t)\|$.

5. PERFORMANCE CRITERIA UNDER CONSIDERATION

The criterions that are used as quality performance measure for above neural networks are false rejection rate (FRR), false acceptance rate (FAR), equal error rate (EER), and average error rate (AER). 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. When a certain threshold is selected, the FRR is equal to the FAR. This error rate is called the EER and the corresponding threshold may be called the equal error threshold. The average of the FRR and FAR is called the AER. When a threshold is used,

6. STUDY RESULTS

The Signature Recognition System is evaluated with the following three scenarios viz. training and testing only samples without a frame (TNTN), training and testing samples with both with and without frame (TATA), training signatures without frame and testing all signatures (TNTA). The evaluation parameters for recognition are True Classification Ratio and False Classification Ratio. Other parameters that are use for performance evaluation are MER (Mean Error Ratio) and TER (Total Error Ratio).

	TA	FR	TR	FA	MER	TER
MLP	78%	22%	84%	16%	1.38%	-
SVM	98%	2%	89%	11%	1.40%	-
RBF	-	3.4%	-	2.91%	3.15%	6.31%

Table-I: Signature Recognition System Evaluation Results

The true classification and false classification ratios show the ability of the given networks to classify the signatures correctly. The following table depicts the performance of all the networks for the same.

	True Classification Ratio	False Classification Ratio
MLP	75%	25%
SVM	95%	5%
RBF	67%	12%

Table-II: Comparison Results of MLP, SVM and RBF Networks

A comparative study between various methodologies for implementing signature recognition shows that SVM outperforms MLP in both signature verification and recognition. SVM makes the system more powerful compared to the other systems in terms of success ratio, ease of implementation and optimized run time. Although MLPs are very good at performing discriminative classification between patterns of well-defined classes, they are not adequate for applications requiring a reliable rejection. Study reveals that RBF Neural Networks are more reliable for such problems.

7. CONCLUSIONS

Signatures are composed of special characters and therefore most of the time they can be unreadable. Many intrapersonal and interpersonal variations make it necessary to analyze them as complete images. As signatures are the primary mechanism both for authentication and authorization in legal transactions, the need for knowing the best and efficient solutions for signature recognition and verification has arose in recent years.

The results of an offline system show that SVM outperforms ANN in both verification and recognition processes. The use of SVM can make signature verification and recognition system more powerful as compared to other existing systems both in terms of success ratio and ease of implementation and optimized run time.

REFERENCES:

1. C.Cortes and V.Vapnik, "Support-vector networks. Machine Learning", vol. 20, Nov. 1995.
2. E.J.R. Justino, F. Bortolozzi, and R. Sabourin. "A comparison of SVM and HMM classifiers in the off-line signature verification", Pattern Recognition Letters 26, 2005.
3. G.K.Gupta, R.C.Joyce, "Using position extrema points to capture shape in on-line hand written signature verification", Pattern Recognition, vol 40, pp. 2811 – 2817, 2007.
4. J. F. Vélez, Á. Sánchez , and A. B. Moreno, "Robust Off-Line Signature Verification Using Compression Networks And Positional Cuttings", Proc. 2003 IEEE Workshop on Neural Networks for Signal Processing, vol. 1, pp. 627-636, 2003.
5. Joachims, T, "Text categorization with support vector machines: Learning with many relevant features". Proceedings of the Tenth European Conference on Machine Learning.
6. K. Han, and I.K. Sethi, "Handwritten Signature Retrieval and Identification", Pattern Recognition.
7. K. R Radhika, M K Venkatesha andG N Sekhar, "Pattern Recognition Techniques in Off-line hand written signature verification - A Survey", proceedings of world academy of science, engineering and technology volume 36 December 2008.
8. L.E. Martinez, C.M. Travieso, J.B. Alonso, and M. Ferrer, "Parametrization of a forgery Handwritten Signature Verification using SVM", IEEE 38th Annual 2004 International Carnahan Conference on Security Technology, 2004, pp. 193-196.
9. Stephane Armand, Michael Blumenstein and Vallipuram Muthukkumarasamy, "Off-line Signature Verification based on the Modified Direction Feature".