Volume 3, Issue 3, March 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Hand Written Signature Recognition & Verification using Neural Network

Pradeep Kumar[*]
Assistant Professor
PIET, Samalkha

Shekhar Singh
Assistant Professor
PIET, Samalkha

Ashwani Garg
Assistant Professor
PIET, Samalkha

Nishant Prabhat
Assistant Professor
PIET, Samalkha

Abstract*— the signature of a person is an important biometric attribute of a human being which can be used to authenticate human identity. A number of biometric techniques have been proposed for personal identification in the past. Among the vision-based ones are voice recognition, face recognition, fingerprint recognition, iris scanning and retina scanning. Voice recognition or signature verification are the most widely known among the non-vision based ones. As signatures continue to play a very important role in financial, commercial and legal transactions, truly secured authentication becomes more and more crucial. Handwritten signatures are considered as the most natural method of authenticating a person's identity. A signature by an authorized person is considered to be the "seal of approval" and remains the most preferred means of authentication. However human signatures can be handled as an image and recognized using computer vision and neural network techniques. With modern computers, there is need to develop fast algorithms for signature recognition. There are various approaches to signature recognition with a lot of scope of research. The method presented in this paper consists of image prepossessing, geometric feature extraction, neural network training with extracted features and verification. A verification stage includes applying the extracted features of test signature to a trained neural network which will classify it as a genuine or forged. In this paper, off-line signature recognition & verification using neural network is proposed, where the signature is captured and presented to the user in an image format. Signatures are verified based on parameters extracted from the signature using various image processing techniques. The Off-line Signature Recognition and Verification is implemented using MATLAB. This work has been tested and found suitable for its purpose.

***Keywords*- Biometrics, error back propagation algorithm, center of mass, neural network, normalized area of signature, Signature, Biometric, Neural Networks, Off-line Signature Recognition and Verification**

I. INTRODUCTION

In our society, traditional and accepted means for a person to identify and authenticate himself either to another human being or to a computer system is based on one or more of these three (3) general principles:

- What the person knows
- What he possesses or
- What he is

The hand written signature is regarded as the primary means of identifying the signer of a written document based on the implicit assumption that a person's normal signature changes slowly and is very difficult to erase, alter or forge without detection. The handwritten signature is one of the ways to authorize transactions and authenticate the human identity compared with other electronic identification methods such as fingerprints scanning, face recognition and retinal vascular pattern screening. It is easier for people to migrate from using the popular pen-and-paper signature to one where the handwritten signature is captured and verified electronically. The signature of a person is an important biometric attribute of a human being and is used for authorization purpose. Various approaches are possible for signature recognition with a lot of scope of research. Here, we deal with an off-line signature recognition technique. 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 [6]. Signature recognition is the process of verifying the writer's identity by checking the signature against samples kept in the database. The result of this process is usually between 0 and 1 which represents a fit ratio (1 for match and 0 for mismatch). Signature recognition is used most often to describe the ability of a computer to translate human writing into text. This may take place in one of two ways either by scanning of written text (off-line method) or by writing directly on to a peripheral input device. The first of these recognition techniques, known as Optical Character Recognition (OCR) is the most successful in the main stream. Most scanning suites offer some form of OCR, allowing user to scan handwritten documents and have them translated into basic text documents. OCR is also used by some archivist as a method of converting massive quantities of handwritten historical documents into searchable, easily-accessible digital forms.

As signature is the primary mechanism both for authentication and authorization in legal transactions, the need for efficient auto-mated solutions for signature verification has increased [1].Unlike a password, PIN, PKI or key cards – identification data that can be forgotten, lost, stolen or shared – the captured values of the handwritten signature are unique to an individual and virtually impossible to duplicate. Signature verification is natural and intuitive. The technology is easy to explain and trust. The primary advantage that signature verification systems have over other type's technologies is that signatures are already accepted as the common method of identity verification [2].

A signature verification system and the techniques used to solve this problem can be divided into two classes Online and Off-line [3].On-line approach uses an electronic tablet and a stylus connected to a computer to extract information about a signature and takes dynamic information like pressure, velocity, speed of writing etc. for verification purpose. 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 much simpler. In this only the pixel image needs to be evaluated. But, the off-line systems are difficult to design as many desirable characteristics such as the order of strokes, the velocity and other dynamic information are not available in the off-line case [4, 5]. The verification process has to wholly rely on the features that can be extracted from the trace of the static signature images only. Vigorous research has been pursued in handwriting analysis and pattern matching for a number of years. In the area of Handwritten Signature Verification (HSV), especially offline HSV, different technologies have been used and still the area is being explored. In this section we review some of the recent papers on offline HSV. The approaches used by different researchers differ in the type of features extracted, the training method, and the classification and verification model used.

1.1 Hidden Markov Models Approach

Hidden Markov Model (HMM) is one of the most widely used models for sequence analysis in signature verification. Handwritten signature is a sequence of vectors of values related to each point of signature in its trajectory. Therefore, a well chosen set of feature vectors for HMM could lead to the design of an efficient signature verification system. These Models are stochastic models which have the capacity to absorb the variability between patterns and their similarities. In HMM stochastic matching (model and the signature) is involved. This matching is done by steps of probability distribution of features involved in the signatures or the probability of how the original signature is calculated. If the results show a higher probability than the test signatures probability, then the signatures is by the original person, otherwise the signatures are rejected. In paper [6], a system is introduced that uses only global features. A discrete random transform which is a sinograph is calculated for each binary signature image at range of $0 - 360$, which is a function of total pixel in the image and the intensity per given pixel calculated using non overlapping beams per angle for X number of angles. Due to this periodicity, it is shift, rotation and scale invariant. A HMM is used to model each writer signature. The method achieves an AER of 18.4% for a set of 440 genuine signatures from 32 writers with 132 skilled forgeries.

1.2 Neural Networks Approach

The main reasons for the widespread usage of neural networks (NNs) in pattern recognition are their power and ease of use. A simple approach is to firstly extract a feature set representing the signature (details like length, height, duration, etc.), with several samples from different signers. The second step is for the NN to learn the relationship between a signature and its class (either "genuine" or "forgery"). Once this relationship has been learned, the network can be presented with test signatures that can be classified as belonging to a particular signer. NNs therefore are highly suited to modeling global aspects of handwritten signatures. The proposed system in [7] uses structure features from the signatures contour, modified direction feature and additional features like surface area, length skew and centroid feature in which a signature is divided into two halves and for each half a position of the centre of gravity is calculated in reference to the horizontal axis. For classification and verification two approaches are compared the Resilient Back propagation (RBP) neural network and Radial Basic Function(RBF) using a database of 2106 signatures containing 936 genuine and 1170 forgeries. These two classifiers register 91.21% and 88 % true verification respectively.

1.3 Template matching approach

Fang et al. [8] proposed two methods for the detection of skilled forgeries using template matching. One method is based on the optimal matching of the one-dimensional projection profiles of the signature patterns and the other is based on the elastic matching of the strokes in the two-dimensional signature patterns. Given a test signature to be verified, the positional variations are compared with the statistics of the training set and a decision based on a distance measure is made. Both binary and grey-level signature images are tested. The average verification error rate of 18.1% was achieved when the local peaks of the vertical projection profiles of grey-level signature images were used for matching and with the full estimated covariance matrix incorporated.

1.4 Statistical approach

Using statistical knowledge, the relation, deviation, etc between two or more data items can easily be found out. To find out the relation between some set of data items we generally follow the concept of Correlation Coefficients. In general statistical usage refers to the departure of two variables from independence. To verify an entered signature with the help of an average signature, which is obtained from the set of, previously collected signatures, this approach follows the concept of correlation to find out the amount of divergence in between them. A unique method is introduced in [9]. In this approach various features are extracted which include global features like image gradient, statistical features derived from distribution of pixels of a signature and geometric and topographical descriptors like local correspondence to trace of the signature. The classification involves obtaining variations between the signatures of the same writer and obtaining a distribution in distance space. For any questioned signature the method obtains a distribution which is compared with the available known and a probability of similarity is obtained using a statistical Kolmorogorv-Smirnov test. Using only 4 genuine samples for learning, the method achieves 84% accuracy which can be improved to 89% when the genuine signature sample size is increased. This method does not use the set of forgery signatures in the training/learning.

1.5 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. The system in [10] uses global, directional and grid features of the signature and SVM for classification and verification. The database of 1320 signatures is used from 70 writers. 40 writers are used for training with each signing 8 signatures thus a total of 320 signatures for training. For initial testing, the approach uses 8 original signatures and 8 forgeries and achieves FRR 2% and FAR 11%.

Contribution:

In this paper we present a model in which neural network classifier is used for verification. Signatures from database are pre-processed prior to feature extraction. Features are extracted from pre-processed signature image. These extracted features are then used to train a neural network. In verification stage, on test signatures pre-processing and feature extraction is performed. These extracted features are then applied as input to a trained neural network which will classify it as a genuine or forged signature.

II. Signature Recognition Process

A problem of personal verification and identification is an actively growing area of research. The methods are numerous and are based on different personal characteristics; voice, lip movement, hand geometry, face, odor, gait, iris, retina and fingerprint are the most commonly used authentication methods. All these psychological and behavioral characteristics are called biometrics. The driving force of the progress in this field is above all, the growing role of the internet and electronic transfers in modern society. Therefore considerable number of applications is concentrated in the area of electronic commerce and electronic banking systems [9]. The biometrics have a significant advantage over traditional authentication techniques due to the fact that biometric characteristics of the individual are not easily transferable are unique of every person and cannot be lost, stolen or broken. The choice of one of the biometric solutions depends on several factors which include [3]:

- User acceptance
- Level of security required
- Accuracy
- Cost and implementation time

The method of signature verification reviewed in this paper benefits the advantage of being highly accepted by potential customers. The use of the signature has a long history which goes back to the appearance of writing itself [9]. Utilization of the signature as an authentication method has already become a tradition in the western civilization and is respected among the others. The signature is an accepted proof of identity of the person in a transaction taken on his or her behalf. Thus the users are more likely to approve this kind of computerized authentication method [10]. Signature verification systems differ in both their feature selection and their decision methodologies. More than 40 different feature types have been used for signature verification [8]. Features can be classified into two major types: local and global [4]. Global features are features related to the signature as a whole, for instance the average signing speed, the signature bounding box and Fourier descriptors of the signatures trajectory. Local features correspond to a specific sample point along the trajectory of the signature. Examples of local features include distance and curvature change between successive points on the signature trajectory [4]. Most commonly used online signatures acquisition devices are pressure sensitive tablets capable of measuring forces exerted at the pen-tip, in addition to the coordinate of the pen. The pressure information at each point along the signature trajectory is another example of commonly used local feature. Some of these features are compared in order to find the more robust ones for signature verification purposes. Other systems have used genetic algorithms to find the most useful features. Due to the high sampling rate of the tablet, some consecutive sample points may mark the same trajectory point especially when the pen movement is slow. Most verification systems resample the input so as to obtain a trajectory consisting of equidistant points. This is often done in order to remove redundant points to speed up the comparisons and to obtain a shape-based representation, removing the time dependencies, separately keep track of the local velocity values and use them in aligning two signatures. Signature recognition and verification involves two separate but strongly related tasks: one of them is identification of the signature owner, and the other is the decision about whether the signature is genuine or forged. Also, depending on the need, signature recognition and verification problem is put into two major classes: (i) On-line signature recognition and verification systems (SRVS) and (ii) Off-line SRVS. On-line SRVS requires some special peripheral units for measuring hand speed and pressure on the human hand when it creates the signature. On the other hand, almost all Off-line SRVS systems rely on image processing and feature extraction techniques [1].

Biometric security is a computerised method of verifying a person's identity based on his/her body and/or physical attributes. Various forms of biometric security exist including fingerprinting, iris recognition [10], speech recognition [17], heart sound recognition [7], and keystroke recognition [12]. However, dispite the novelty and perceived security of the aforemention techniques, the longest standing and most natural method for verifying one's identity is through the use of a handwritten signature. Handwritten Signature Verification (HSV) is an automated method of verifying a signature by capturing features about a signature's shape (i.e., static features) and the charactertics of how the person signs his/her name in real-time (i.e., dynamic features). HSV is more generally accepted by the public and is less intrusive than other biometric authentication techniques. Neural networks (NNs) have been a fundamental part of computerized pattern recognition tasks for more than half a century, and continue to be used in a very broad range of problem domains. The two main reasons for their widespread usage are: 1) power (the sophisticated techniques used in NNs allow a capability of modeling quite complex functions); and 2) ease of use (as NNs learn by example it is only necessary for a user to gather a highly representative data set and then invoke training algorithms to learn the underlying structure of the data). The HSV process parallels this learning mechanism.

There are many ways to structure the NN training, but a very simple approach is to firstly extract a feature set representing the signature (details like length, height, duration, etc.), with several samples from different signers. The second step is for the NN to learn the relationship between a signature and its class (either "genuine" or "forgery"). Once this relationship has been learned, the network can be presented with test signatures that can be classified as belonging to a particular signer. NNs therefore are highly suited to modeling *global* aspects of handwritten signatures. Concentrated efforts at applying NNs to HSV have been undertaken for over a decade with varying degrees of success (e.g., see [9], [16]). The main attractions include:

1) *Expressiveness*: NNs are an attribute-based representation and are well-suited for continuous inputs and outputs. The class of multi-layer networks as a whole can represent any desired function of a set of attributes, and signatures can be readily modeled as a function of a set of attributes.

2) *Ability to generalize*: NNs are an excellent generalization tool (under normal conditions) and are a useful means of coping with the diversity and variations inherent in handwritten signatures.

3) *Sensitivity to noise*: NNs are designed to simply find the best fit through the input points within the constraints of the network topology (using nonlinear regression). As a result, NNs are very tolerant of noise in the input data.

4) *Graceful degradation*: NNs tend to display graceful degradation rather than a sharp drop-off in performance as conditions worsen.

5) *Execution speed*: The NN training phase can take a large amount of time. In HSV this training is a oneoff cost undertaken off-line (i.e., rarely performed while a user waits for verification results).

This paper presents a method for HSV by using NN architecture. Various static (e.g., height, slant, etc.) and dynamic (e.g., velocity, pen tip pressure, etc.) signature features are extracted and used to train the NN. Several Network topologies are tested and their accuracy is compared. The resulting system performs reasonably well with an overall error rate of 2.3% being reported for the best case.

2.1 Types of Signature Verification

Based on the definitions of signature, it can lead to two different approaches of signature verification.

2.1.1 Off-Line or Static Signature Verification Technique

This approach is based on static characteristics of the signature which are invariant [6]. In this sense signature verification, becomes a typical pattern recognition task knowing that variations in signature pattern are inevitable; the task of signature authentication can be narrowed to drawing the threshold of the range of genuine variation. In the offline signature verification techniques, images of the signatures written on a paper are obtained using a scanner or a camera.

2.1.2 On-line or Dynamic Signature Verification Technique

This is the second type of signature verification technique. This approach is based on dynamic characteristics of the process of signing. This verification uses signatures that are captured by pressure sensitive tablets that extract dynamic properties of a signature in addition to its shape. Dynamic features include the number of order of the strokes, the overall speed of the signature and the pen pressure at each point that make the signature more unique and more difficult to forge. Application areas of Online Signature Verification include protection of small personal devices (e.g. PDA, laptop), authorization of computer users for accessing sensitive data or programs and authentication of individuals for access to physical devices or buildings [4].

2.2 Nature of Human Signature

It is supposed that the features of the process of signing originate from the intrinsic properties of human neuromuscular system which produces the aforementioned rapid movements. Knowing that this system is constituted by a very large number of neurons and muscle, fibers is possible to declare based on the central limit theorem that a rapid and habitual movement velocity profile tends toward a delta-log normal equation [10]. This statement explains stability of the characteristics of the signature. Thus, the signature can be treated as an output of a system obscured in a certain time interval necessary to make the signature. This system models the person making the signature [7].

2.3 Types of Forgeries

The main task of any signature verification system is to detect whether the signature is genuine or counterfeit. Forgery is a crime that aims at deceiving people. Since actual forgeries are difficult to obtain, the instrument and the results of the verification depend on the type of the forgery [9]. Basically there are three types that have been defined:

Random forgery: this can normally be represented by a signature sample that belongs to a different writer i.e. the forger has no information whatsoever about the signature style and the name of the person.

Simple forgery: this is a signature with the same shape or the genuine writer's name.

Skilled forgery: this is signed by a person who has had access to a genuine signature for practice [4].

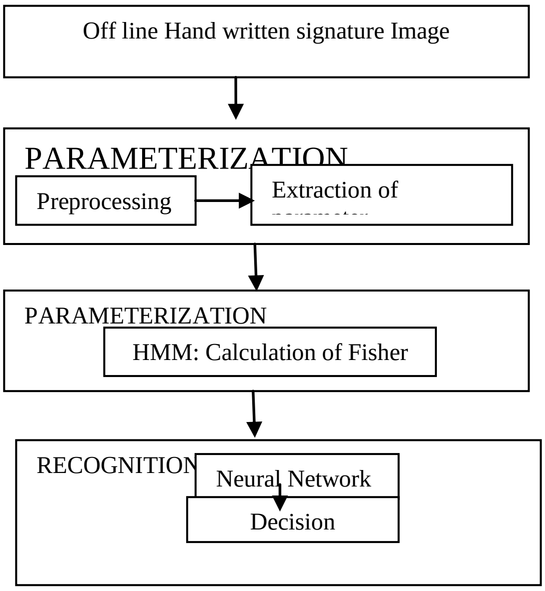

Figure 1: hand written signature recognition

2. METHODOLOGY

In this section, block diagram of system is discussed. Fig. 1 gives the block diagram of proposed signature verification system which verifies the authenticity of given signature of a person. The design of a system is divided into two stages:

1. Training stage
2. Testing stage

A training stage consist of four major steps

1) Retrieval of a signature image from a database
2) Image pre-processing
3) Feature extraction
4) Neural network training

A testing stage consists of five major steps

1) Retrieval of a signature to be tested from a database
2) Image pre-processing
3) Feature extraction
4) Application of extracted features to a trained neural network
5) Checking output generated from a neural network.

Fig. 2 shows one of the original signature image taken from a database and all the subsequent figures show the resultant signature image obtained after performing the steps mentioned in an algorithm.

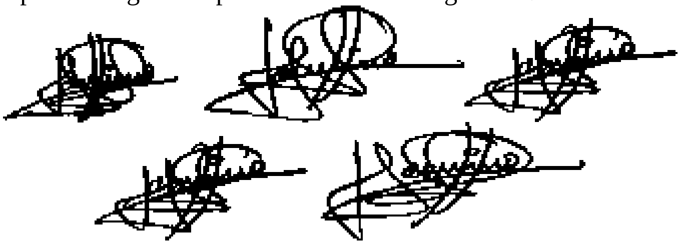

Figure 2: Signature Image

2.1 Pre-processing

The pre processing step is applied both in training and testing phases. Signatures are scanned in gray. The purpose in this phase is to make signature standard and ready for feature extraction. The pre-processing stage improves quality of the image and makes it suitable for feature extraction [11]. The prepossessing stage includes

2.1.1 Converting image to binary

A gray scale signature image is converted to binary to make feature extraction simpler.

2.1.2 Image resizing

The signatures obtained from signatory are in different sizes so, to bring them in standard size, resizing is performed, which will bring the signatures to standard size 256*256 as shown in Fig. 2.

2.1.3 Thinning

Thinning makes the extracted features invariant to image characteristics like quality of pen and paper. Thinning means reducing binary objects or shapes to strokes that are single pixel wide.

2.1.4 Bounding box of the signature:

In the signature image, construct a rectangle encompassing the signature. This reduces the area of the signature to be used for further processing and saves time.

2.2 Feature Extraction

The choice of a powerful set of features is crucial in signature verification systems. The features that are extracted in this phase are used to create a feature vector. A feature vector of dimension 24 has been used to uniquely characterize a candidate signature. These features are extracted as follows:

1. Maximum horizontal and vertical histogram

Horizontal histogram is calculated by going through each row of the signature image and counting number of black pixels. A row with maximum number of black pixels is recorded as maximum horizontal histogram. Similarly, a vertical histogram is calculated by going through each column of the signature image and finding a column with maximum number of black pixels.

2. Center of mass

Split the signature image in two equal parts and find center of mass for individual parts.

3. Normalized area of signature

It is the ratio of area of signature image to the area of signature enclosed in a bounding box. Area of a signature is the number of pixels comprising it. *Normalized area = Signature Area Area enclosed in a bounding box* Eq. (1)

4. Aspect Ratio

It is the ratio of width of signature image to the height of the image. This is done because width or height of person's signature may vary but its ratio remains approximately equal. *Aspect Ratio = widt of signature in a bou nding box Heig t of signature in a bounding box* Eq. (2)

5. Tri surface feature

Two different signatures may have same area .so; to increase the accuracy of the features three surface feature has been used. In this, a signature is divided into three equal parts and area for each part is calculated. Eq. (1) is then used to calculate normalized area of each part. Figure (6) shows tri surface feature

6. The six fold surface feature

Divide a signature in three equal parts and find bounding box for each part. Then calculate centre of mass for each part. Draw a horizontal line passing through centre of mass of each part and calculate area of signature above and below centre of mass within a bounding box. This provides six features.

7. Transition feature

Traverse a signature image in left to right direction and each time there is a transition from 1 to 0 or 0 to 1, calculate a ratio between the position of transition and the width of image traversed and record it as a feature. Repeat a same process in right to left, top to bottom and bottom to top direction. Also calculate total number of 0 to 1 and 1 to 0 transitions. This provides ten features.

2.3 Creation of feature vector

A feature vector of size 24 is formed by combining all the extracted features as discussed in section 2.2.

2.4 Training a neural network

Extracted 24 feature points are normalized to bring them in the range of 0 to 1.These normalized features are applied as input to the neural network.

2.5 Verification.

In the verification stage, a signature to be tested is pre-processed and feature extraction is performed on pre processed test signature image as explained in section 2.2 to obtain feature vector of size 24. After normalizing a feature vector it is fed to the trained neural network which will classify a signature as a genuine or forged.

III. RECOGNIZATION USING NEURAL NETWORK

In this work there is a challenge of creating a system with the ability to recognize hand written signature and verify its authenticity. This poses a problem because we are trying to get the computer to solve a problem with a method of solution that goes outside the convention of writing an algorithmic process.

The challenge involves making the computer solve the problem using a series of new steps. After a lengthy research, the only feasible solution required is using the concept of the Neurons in human brain, which is familiar with medical practitioners.

Back Propagation Artificial Neural Network:

There are several algorithms that can be used to create an artificial neural network, but the Back propagation was chosen because it is probably the easiest to implement, while preserving efficiency of the network. Backward Propagation Artificial Neural Network (ANN) use more than one input layers (usually 3). Each of these layers must be either of the following:

- Input Layer – This layer holds the input for the network
- Output Layer – This layer holds the output data, usually an identifier for the input.
- Hidden Layer – This layer comes between the input layer and the output layer. They serve as a propagation point for sending data from the previous layer to the next layer.

A typical Back Propagation ANN is as depicted below. The black nodes (on the extreme left) are the initial inputs. Training such a network involves two phases. In the first phase, the inputs are propagated forward to compute the outputs for each output node. Then, each of these outputs are subtracted from its desired output, causing an error [an error for each output node]. In the second phase, each of these output errors is passed backward and the weights are fixed. These two phases are continued until the sum of square of output errors reaches an acceptable value. Each neuron is composed of two units. The First unit adds products of weights coefficients and input signals while the second unit realizes nonlinear function, called neuron activation function.

Signal e is adder output signal and $y=f\ e$ is output signal of nonlinear element. Signal y is also output signal of neuron. To teach the neural network, we need data set. The training data set consists of input signals $x1\ and\ x2$ assigned with corresponding target (desired output)y. The network training is an iterative process. In each iteration weights coefficients of nodes are modified using new data from training data set. Each teaching step starts with forcing both input signals from training set. After this stage we can determine output signals values for each neuron in each network layer.

IV. Result And Discussion

For training and testing of the system many signatures are used. The results given in this paper are obtained using the "Grupo de Procesado Digital de Senales" (GPDS) signature database [12]. The results provided in this research used a total of 2000 signatures. Those 2000 signatures are comprised of 50 sets (i.e. from 50 different people) and, for each person there are 24 samples of genuine signatures and 24 samples of forgeries. Figure 6 shows some of the signatures in the GPDS database. 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. The features extracted from 19 genuine signatures and 19 forged signatures for each person were used to train a neural network. The architecture of neural network used has input layer, hidden layer and output layer [13]. Number of neurons in the input layer are 24, 24 neurons in the hidden layer and one neuron in the output layer. After applying 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.Fig.8 shows performance graph of the training a two layer feed forward neural network using Error Back Propagation Algorithm (EBPTA). When verification begins, the application updates the user of the current state of events. For instance, at the first stage, settings are initialized, indicated by "Initializing settings..." and "initializing settings...Done", when completed. At the second stage, the training set for the inputs is generated, indicated by the output "Generating training set..." and "Generating training set...Done", when completed. At third stage, when training on the images begins, the program notifies with "Began training process..." and when done, the final notification states "Completed training process successfully." After the entire process of training, a file is generated and stored in the files system. This file contains the network details of the training process in binary.

V. Conclusion

This paper presents a method of handwritten signature verification using neural network approach. The method uses features extracted from preprocessed signature images. The extracted features are used to train a neural network using error back propagation training algorithm. As shown in Table 2 CCR in recall is 100%. The network could classify all genuine and forged signatures correctly. When the network was presented with signature samples from database different than the ones used in training phase, out of 300 such signatures (150 genuine and 150 forged) it could recognize 248 signatures correctly. Hence, the correct classification rate of the system is 82.66% in generalization as shown in Table 3. Our recognition system exhibited 100% success rate by identifying correctly all the signatures that it was trained for. 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. Generally the failure to recognize/verify a signature was due to poor image quality and high similarity between 2 signatures. Recognition and verification ability of the system can be increased by using additional features in the input data set. This study aims to reduce to a minimum the cases of forgery in business transaction.

References

[1] Prashanth CR,KB Raja,KR Venugopal, LM Patnaik,"Standard Scores Correlation based Offline signature verification system", International Conference on advances in computing, control and telecommunication Technologies 2009 .

[2] R. Plamondon and S.N. Srihari, "Online and Offline Handwriting Recognition: A Comprehensive Survey", IEEE Tran. on Pattern Analysis and Machine Intelligence, vol.22 no.1, pp.63-84, Jan.2000.

[3] J Edson, R. Justino, F. Bortolozzi and R. Sabourin, "An off-line signature verification using HMM for Random,Simple and Skilled Forgeries", Sixth International Conference on Document Analysis and Recognition, pp.1031-1034, Sept.2001. 211-222, Dec.2000.

[4] B. Herbst. J. Coetzer. and J. Preez, "Online Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model," *EURASIP.Journal on Applied Signal Processing*, vol. 4, pp. 559–571, 2004.

[5] M. Blumenstein. S. Armand. and Muthukkumarasamy, "Off-line Signature Verification using the Enhanced Modified Direction Feature and Neural based Classification," *International Joint Conference on Neural Networks*, 2006.

[6] S.Srihari. K. M. Kalera. and A. 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.

[7] H. S. Srihari and M. Beall, "Signature Verifcation Using Kolmogrov Smirnov Statistic,"*Proceedings of International Graphonomics Society,Salemo Italy* , pp. 152–156, june,2005.

[8] T.S. enturk. E. O¨ zgunduz. and E. Karshgil, " Handwritten Signature Verification Using Image Invariants and Dynamic Features," *Proceedings of the 13*th *European Signal Processing Conference EUSIPCO 2005,Antalya Turkey*, 4th-8th September, 2005.

[9] Ramachandra A. C ,Jyoti shrinivas Rao"Robust Offline signature verification based on global features" IEEE International Advance Computing Conference ,2009.

[10] Martinez, L.E., Travieso, C.M, Alonso, J.B., and Ferrer, M. *Parameterization of a forgery Handwritten Signature Verification using SVM.* IEEE 38thAnnual 2004 International Carnahan Conference on Security Technology ,2004 PP.193-196

[11] "An Introduction to Artificial Neural Systems" by Jacek M. Zurada, West Publishing Company 1992.

[12] OZ, C. Ercal, F. and Demir, Z. Signature Recognition and Verification with ANN.

[13] Golda, A. 2005. Principles of Training multi-layer neural network using back propagation.

[14] Jain, A., Bolle, R., and Pankarti. 1999. Biometrics: Personal Identification in Networked Society. The Springer International series in Engineering & Computer Science. vol. 479.

[15] Aykanat C. et. al ,(Eds). 2004. Proceedings of the 19th International Symposium on Computer and Information Sciences, ISCIS 2004. Springer-Verlag Berlin Heidelberg New York. pp. 373-380.

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

[17] Ozgunduz, E., Karsligil, E., and Senturk, T. 2005.Off-line Signature Verification and Recognition by Support Vector Machine. Paper presented at the European Signal processing Conference.

[18] Pacut, A. and Czaja, A. 2001. Recognition of Human Signatures. Neural Network, in proceedings of the International Conference on Neural Network, IJCNN'01, vol.2, pp 1560-1564.

[19] Jain, A., Griess, F., and Connel1, S. "Online Signature Recognition", Pattern Recognition, vol.35,2002, pp 2963-2972.

[20] Kalenova, D. 2005. Personal Authentication using Signature Recognition.

[21] Plamondon, R.1995. The Handwritten Signature as a Biometric Identifier: Psychophysical Model & System Design. IEE Conference Publications, Issue CP408, 23-27

[22] Sonsone and Vento. "Signature Verification: Increasing Performance by Multi-Stage System", Pattern Analysis & Application, vol.3, no. 2, 2000, pp.169-181

[23] Velez, J.F., Sanchez, A. and Moreno, A.B. 2003. Robust Off-Line Signature Verification using Compression Networks and Position Cuttings.