e-ISSN: 2349-9745
p-ISSN: 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Handwritten Signature Verification using Artificial Neural Network

Shiwani Gupta
Asstt. Prof., CMPN,TCET,Mumbai

ABSTRACT: This paper reviews various Signature Verification approaches; various feature sets, various online databases and types of features. Processing on an online database, post extracting a combination of global and local features onto a signature as an image, using MultiLayer Perceptron Feed Forward Network alongwith Back Propogation Algorithm for training is proposed to classify a genuine and forged (random, simple and skilled) offline signatures.

Keywords: Offline Signature Verification, Artificial Neural Networks, Feature extraction, forgery, preprocessing.

I. INTRODUCTION

Biometrics can be classified into two broad categories — Behavioral (signature verification, keystroke dynamics, handwriting, speech etc.) and Physiological (face, iris, fingerprint, retina etc.)[1].

A. Signature

Human Signature is proven to be the most natural, widely accepted[1,2] biometric attribute of a human being which can be used to authenticate human identity and is even less intrusive and has no negative or undesirable health connotations [3]. The verification of signer from scanned signs of documents has received much more importance in day to day life because still various transactions are done with the faith of signs. But great variability can be observed in signatures according to country, age, time, habits, psychological or mental state, physical and practical conditions [15].

B. Signature Verification

Signatures are composed of special characters 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 [1]. As signature is the primary mechanism both for authentication and authorization in legal transactions, the need for research in efficient auto-mated solutions for signature recognition and verification has increased in recent years.

Recognition is finding the identification of the signature owner whereas Verification is the decision about whether the signature is genuine or forged [1]. Signature verification is widely studied and discussed using two approaches depending on the data acquisition method used[15][19][20].

On-line approach / Dynamic Signature Verification Technique – It uses an electronic pressure sensitive digitizing tablet / stylus operated PDA to extract information about a signature and takes dynamic information like number of order of the strokes, the overall speed of the signature and the pen pressure at each point[4] etc. for verification purpose.

Offline approach / Static Signature Verification Technique – Users write their signature on paper, digitize it through an optical scanner or a camera, and the biometric system recognizes the signature analyzing its shape, length, height, duration, etc [4][14][29]. The features used are [4]. For this only the

pixel image needs to be estimated. In this sense, signature verification becomes a typical pattern recognition task. The task of signature authentication can be narrowed to drawing the threshold of the range of genuine variation [4].

Offline systems are more applicable and easy to use in comparison with on-line systems which are more unique and difficult to forge[4], however it is considered more difficult to design offline than on-line due to the lack of dynamic information such as no. of strokes, velocity etc.

C. 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 [17]. Basically there are three types that have been defined [1][14][15][20]:

1. **Random forgery**: are not based on any knowledge of the original signature i.e. the forger has no information whatsoever about the signature style and the name of the person.
2. **Simple forgery**: are produced knowing the name of the signer or same shape but without having an example of signer's signature.
3. **Skilled forgery**: is signed by a person who has had access to a genuine signature for practice [18].

Every type of forgery requests a different recognition approach. Methods based on Static approach are usually used to identify random and simple forgeries. The reason is that these methods have shown to be more suitable to describe characteristics related to the signature shape [1]. Although a great amount of work has been done on random and simple forgery detection, more hard work is still needed to tackle the problem of skilled forgery detection. No verification algorithms are proposed which might be dealing with skilled forgeries [20][30].

II. DATA ACQUISITION AND PREPROCESSING

The design of a signature verification system requires the solution of four problems: data acquisition, pre-processing, feature extraction and verification [1,33].

A. Data Acquisition

There are different datasets which are available consisting of different signers including some forgeries. Some available datasets are given below [15]:

Real DB1: MCYT-75 Signature DB. This dataset includes 75 signers collected at four different Spanish universities. The corpus includes 15 genuine signatures acquired in two sessions. All the signatures were acquired with the same inking pen and the same paper templates, over the WACOM Intuos A6 pen tablet. The paper templates were scanned at 600 dpi with 256 grey levels. The database is distributed by the Biometric Recognition Group-ATVS from UAM1.

Real DB2: GPDS-960 Signature DB [16]. This dataset contains 24 genuine signatures from 881 individuals acquired in one site in just one session. For the current work, only the first 350 users of the database were considered in the experiments. Each sheet provided two different box sizes for the signature. The sheets were scanned at 600 dpi with 256 grey levels. The database is distributed by the Grupo Procesado Digital de Se˜nales (GPDS) of the ULPGC2.

Synthetic DB1: SSig-DB 1-Ink. This dataset was produced following the proposed synthetic off-line signature generation method, and comprises 30 samples of 350 synthetic signers. All samples were generated with the _spot = 0:35mm: ballpoint and the viscous ink. The database may be obtained from the Biometric Recognition Group-ATVS website.

Synthetic DB2: SSig-DB Multiple Inks. As the SSig- DB 1-Ink this dataset comprises 30 samples of 350 synthetic signers. However, in this case, samples were generated using the 6 standard ballpoint sizes and three different types of inks. For each signature, both the ballpoint and the ink were randomly selected. The database may also be obtained from the Biometric Recognition Group-ATVS website.

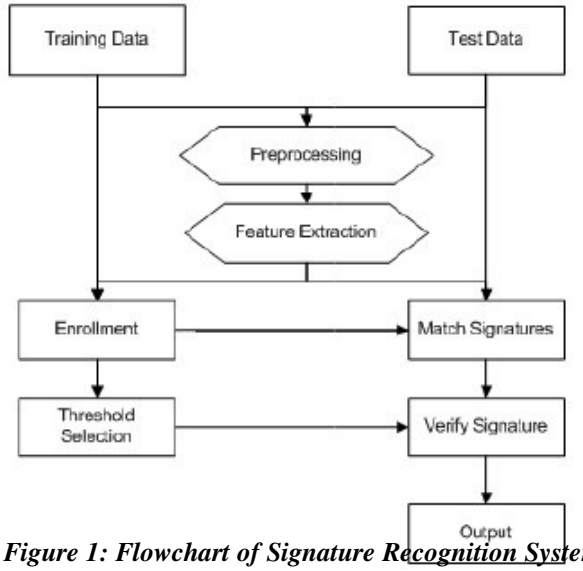

Figure 1: Flowchart of Signature Recognition System

B. Pre Processing

Image pre-processing represents a wide range of techniques that exist for the manipulation and modification of images [15]. The following steps are done [1][19][20]:

1) Thresholding: It is the most trivial and effortlessly appropriate method for segregating objects from the background. Thresholding method can be used for distinguishing the signature from the background. In proposed application, we are concerned in dark objects on light background and hence a threshold value T entitled as the brightness threshold is suitably chosen and applied to image [21]. After the Thresholding, the pixels of the signature would be 1 and the other pixels which belong to the background would be 0 [23]. The brightness threshold [24] can be chosen such that it satisfies the following conditions;

Suppose image pixels f(x, y) then,
If $f(x, y) \geq T$
Then f(x, y) = Background
Else f(x, y) = Object

2) Cropping: The image is cropped, to the bounding rectangle of the signature.

3) Color Normalization: Transformation from color to grayscale, and finally to black and white (binary).

Gray colour = (0.299*Red) + (0.5876*Green) + (0.114*Blue)

4) Signature Normalization[20]: Irregularity in image capturing and scanning process causes dimensions of signature to fluctuate [21]. Height and width of signatures fluctuate from person to person and occasionally even the same person may exercise different sizes of signature [24]. Therefore it is needed to get rid of the size variation and achieve a benchmark signature size for all input signatures. Throughout the normalization process, the characteristic ratio between the width and height of a signature is kept undamaged and following the process, all the signatures will have the similar dimension [24]. Normalization process made use of the following equations:

Xnew = [(Xold-Xmin)/ (Xmax-Xmin)]*M
Ynew = [(Yold-Ymin)/ (Ymax-Ymin)]*M
where,
Xnew, Ynew = Pixel coordinates for the normalized signature,
Xold, Yold = Pixel coordinates for the original signature,
M = Width/height meant for the normalized signature

5) Filtering: Images are contaminated due to stemming from decoding errors or noisy channels. An image also gets degraded because of the detrimental effects due to illumination and other objects in the environment. Median filter is extensively used for smoothing and restoring images corrupted by noise [24]. In a median filter, a window slides over the image, and for each location of the window, the median concentration of the pixels within it decide the intensity of the pixel positioned in the middle of the window. As weigh against to the mean filter, median filter has striking properties for suppressing impulse noise while preserving edges; due to this feature we recommended this filter in our proposed system [24].

6) Thinning[20]**:** It was introduced to describe the global properties of objects and to reduce the original image into a more compact representation [23]. It uses a Stentiford algorithm for thinning process. Thinning means reducing binary objects or shapes to strokes that are single pixel wide. It makes the extracted features invariant to image characteristics like quality of pen and paper but thinning the black and white image results always in a huge information loss.

C. Feature Extraction

In Feature extraction, the essential features are extracted from the original input signature based on the application, and fluctuate accordingly [23]. The choice of a powerful set of features is crucial in signature verification systems [22]. The features that are extracted from this phase are used to create a feature vector which is then used to uniquely characterize a candidate signature [21].
Features for offline signature verification using scanned images can be divided into three types [1][20][25][31]:

1) **Global features** describe or identify the signature shape like signature area, signature height-to-width ratio, slope & slope direction, skewness of signature etc. They are extracted from every pixel that lies within a rectangle circumscribing the signature. These features do not reflect any local, geometrical, or topological properties of the signature. Although global features are easily extractable and insensitive to noise, they are dependent upon the position alignment and highly sensitive to distortion and style variations and they only deliver limited information for signature verification [21].

2) ***Local Features*** are calculated to describe the geometrical characteristics such as location, tangent track, and curving. They provide affluent descriptions of writing shapes and are powerful for cultivated writers, but the extraction of consistent local features is still a hard problem [21]. The local features based approaches are more popular in online verification than in the offline one. This is because it is much easier to calculate local shape and to find their corresponding relations in 1D succession than in 2D images [21].

3) **Geometrical and topological features** describe the characteristic geometry and topology of a signature and thereby preserve the signatures global and local properties, e.g. local correspondence of stroke segments to trace signature. They have a high tolerance to distortion and style variations, and they can also tolerate a certain degree of translation and rotation variations.

4) **Statistical features** are derived from the distribution of pixels of a signature, e.g. statistics of high gray-level pixels to identify pseudo-dynamic characteristics of signatures. This technique includes the extraction of high pressure factors with respect to vertically segmented zones (for example, upper, middle and lower zones) [7] and the ratio of signature width to short- or long-stroke height [8]. The statistical features take some topological and dynamic information into account and consequently can tolerate minor distortions and style variations.

5) Mask Features provide information about guidelines of the lines of the signature for the reason that the angles of signature have interpersonal variation.

6) Texture Features are the pixel positions with respect to the property of the feature. These can be processed using a matcher which uses co-occurrence matrix of the picture image. It includes[23]:

- End points are points where a signature stroke begins or ends.
- Branch points are points where a signature stroke bifurcates into two strokes.
- Crossing points are points where one signature stroke crosses another stroke.

To extract these features, it is necessary to apply the pre-processing techniques like thresholding and thinning on a gray scale signature image [23].

The features extracted from signatures or handwriting play a vital role in the success of any feature-based HSV system. If a poorly constructed feature set is used with little insight into the writer's natural style, then no amount of modeling or analysis is going to result in a successful system. Further, it is necessary to have multiple, meaningful features in the input vector to guarantee useful learning by the NN [27].
The properties of "useful" features must satisfy the following three requirements [28]:
1) The writer must be able to write in a standard, consistent way (i.e., not unnaturally fast or slow in order to produce a particular feature);
2) The writer must be somewhat separable from other writers based on the feature;
3) The features must be environment invariant (remain consistent irrespective of what is being written).

The third point is more relevant to the process of writer identification than HSV, as a person's signature is most often a fixed text.

What follows now is a description of each of the features that are extracted from a given signature, as well as their significance and method of calculation. Each of these features acts as a single input to the NN. These features are extracted as follows [5,6]:

Center of mass: Split the signature image in two equal parts and finds center of mass for individual parts.

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.

Aspect Ratio: This is the ratio of the writing length to the writing height. It remains invariant to scaling. If the user signs in a different size, the height and length will be altered proportionally to retain the aspect ratio.

Wrinkleless: It is the total number of black pixels available in the image after all the pre-processing has been done. Since the pixel count parameter is a unique value, this property of handwritings is used to distinguish between genuine and forged signature.

Slope And Slope Direction - To calculate approximately the slope of the signature the algorithm proposed by Ammar is used [29]. This algorithm formulates the use of the thinned image obtained during the pre-processing. A 3*3 sliding window is used for calculation. The window is stimulated starting from the top left pixel to the bottom right pixel, one pixel at a time in a row major order [29].

Density of Thinned Image - The density of thinned image can be designed after thinning which can be calculated by the following formula [30].

Density of thinned image = No of non zero pixels in the thinned image / Total no of pixels in the thinned image.

Width to Height Ratio- Width to height ratio is the ratio of range of x coordinates to the range of y coordinates [30]. The formula for calculating width to height ratio is given as,

Width to Height Ratio = (Xmax - Xmin) / (Ymax - Ymin)
where, Xmax & Xmin = Maximum & Minimum values of x coordinates of non-zero pixels, Ymax & Ymin = Maximum & Minimum values of y coordinates of non-zero pixels [30].

Skewness- Skewness is a measure of symmetry. It allows us to determine how the curves in each segment of the signature are. The proportion of this torsion is afterwards calculated and extracted. Moreover, this percentage is weighed against those extracted from the other images [30].

Signature Duration**:** The time taken to perform a signature is perhaps the single most discriminatory feature in HSV. A study reported found that 59% of forgeries can be rejected on the basis of the signature duration being more than 20% different from the mean.

Pen-Down Ratio**:** This is the ratio of the pen-down time to the total writing time. This feature does not undergo a large amount of variation when signing, irrespective of the writer's mood or emotions. In addition, it is very difficult to forge as there is no way of determining the pendown ratio from an off-line

writing copy. Calculation is performed by removing leading and trailing zeroes from the captured data, then taking the ratio of the number of non-zero points to the total number of points.

Horizontal Length**:** This is the horizontal distance measured between the two most extreme points in the *x* direction (often simply the distance between the first point captured and the last point captured). Any fragments such as 't' crossings or 'i' dottings are excluded (such fragments far less stable and individual

traits such as extravagant 't' crossings can cause high variability with this feature). The horizontal length tends to remain stable with a practiced word and particularly with a signature, irrespective of the presence of a bounding box, horizontal line or even with no line present.

***Number of "pen-ups"*:** This indicates the number of times the pen is lifted while signing after the first contact with the tablet and excluding the final pen-lift. This is highly stable and almost never changes in an established signature. This can be a difficult feature for a forger to discern from an off-line copy of the signature.

***Cursivity*:** This is a number normalized to between zero and one that represents the degree to which a writer produces isolated handprint characters or fully-connected cursive script. The higher the cursivity value, the more connected the word is. A value of one means that there were no pen-ups over the entire word and value closer to zero means that the writing was mostly printed rather than cursive. However, the drawback with this approach is that it is necessary to have a priori knowledge of how many letters are there in the word being written.

***Top Heaviness*:** This is a measure of the proportion of the signature that lies above the vertical midpoint. The only real issue in the calculation of top heaviness is to decide which measure of central tendency is most indicative of the true vertical midpoint. It would be pointless to use the median in this situation as, by definition, half of the points would lie above the median and half below. It is therefore a question as to which of the other two standard central measures (mean or mode) is more appropriate.

***Horizontal Dispersion*:** This is the same as top heaviness but with respect to the horizontal spread of the handwriting rather than the vertical spread. Calculation is done in a similar fashion.

***Curvature*:** This is a measure of how "flat" or how "curved" the handwriting is. A high curvature value means that the writing is more dramatically curved, which is associated with more thorough or exaggerated completion of handwritten characters. Curvature is slightly susceptible to change depending on the writer's mood or demeanor. Curvature is calculated as the ratio of the signature path length to the word length. The path length is the sum of distances between each consecutive point in the sample so is generally quite large, of the order of 10,000 pixels. The word length is the physical, or Euclidean, distance between the captured writing's first and last point.

***Average Curvature per Stroke*:** This is a feature based on the curvature value described above, except that the curvature value is calculated for each individual stroke in the handwriting sample, then averaged. The difference between this feature and the global curvature value is that by examining the curvature of the individual strokes, it is possible to obtain a more insightful measure of the depth of the local curves in the handwriting.

***Number of Strokes*:** This feature is indicative of how many segments or states the handwriting goes through during the signature's production. This feature remains quite stable over a user's various samples as even with the natural variations in a user's signature, the segmentation remains quite similar. Furthermore, this feature is nontrivial for a forger to reproduce as the segmentation is based purely on the pen-tip velocity, which is not visible with just a written version of the word.

***Mean Ascender Height*:** This is the mean height of "ascenders" in the handwriting. Ascenders are letters such as'd', 'f' and't' in which a part of the letter extends above the main body of the sample [1]. Formal detection of ascenders in the body of a signature involves computing the mean of the data, as well as points at one quarter and three quarters of the maximum height. The ascender's peaks are the local maxima in the *y* direction that are above the three quarter mark. The distance between a local maximum and the *y* mean is found and this distance is taken as the height of that ascender.

***Mean Descender Depth*:** Descenders are the opposite of ascenders. They are letters such as 'g', 'y' and 'j' that typically contain parts extending below the main body of the sample (it is possible for an individual letter to be an ascender and a descender – the letter 'f' is sometimes written in this way). Finding the descender extremities is done in a similar fashion to ascenders and uses the same frequency histogram. The descender extremities are the local minima in the *y* direction that fall below the lower quarter of the sample. The depth value for each extremity is measured as the distance between the local minimum and the *y* mean expressed as a positive integer. ***Maximum Height*:** This is the distance between the lowest point in a word (the lowest descender's depth) and the highest point in a word (the highest ascender's height). This calculation ignores 'i' dottings and't' crossings or other such artifacts occurring in the handwriting. Also removed from consideration is the final trailing stroke in a signature. This feature remains reasonably stable across several written samples.

***Average Velocity*:** This measure how fast the pen-tip is travelling across the tablet's surface. This is calculated as the mean of all individual velocity values (there is one velocity value for each pair of consecutive points).

***Average Absolute Acceleration*:** This is the absolute value of the acceleration and deceleration measurements. The average absolute acceleration captures the mean rate of velocity change in both positive and negative directions.

***Maximum Acceleration*:** While this feature is less stable than some others, the purely dynamic nature and difficulty in forging still make it a useful characteristic.

***Maximum Deceleration*:** This is the rate which the pentip's velocity decreases as it approaches a stroke's end.

***Handwriting Slant Using All Points*:** Slant calculation bears much importance in handwriting analysis. It is not trivial and several different approaches were considered. The first approach involved using all captured writing points. The points are spatially resampled and the angle (expressed as a gradient) between each pair of consecutive points in the signature is calculated, giving several gradient values. The slant is given by the mean of these gradient values. 'i' dottings, 't' crossings and other such artifacts are removed from consideration.

***Horizontal Velocity*:** This is the average velocity over the *x* direction. It measures how fast the signature moves horizontally and is related to pen-tip velocity, cursivity, horizontal length and acceleration. It is impossible for a potential forger to discern the horizontal velocity from an off-line copy of the writing. This feature is calculated as the ratio of horizontal distance to the duration in which the sample's body was produced.

***Degree of Parallelism*:** This refers to the extent to which slant remains consistent throughout the entire sample. This is a feature intrinsic to a writer's natural handwriting and is a characteristic naturally produced without conscious thought. This feature's main problem is that users tend to write with higher parallelism if they are forcing themselves to write slower and more deliberately. Calculation is based on the handwriting slant. Long strokes are extracted and the standard deviation of the slant of the long strokes is obtained (a higher value indicates a lower slant consistency).

***Baseline Consistency*:** The baseline of a single handwritten word is the line-of-best-fit drawn through the bottom of all non-descender characters. The baseline is analogous to the position of the line when a user is signing on a ruled or dotted line. This is another very personal feature and is particularly representative of a signer's natural tendency when no ruled line is present as a guide. Some writers are naturally more irregular or "sloppy" when forming their baseline than others. Calculation is done by extracting the set of

minima from all non-descender characters (i.e., *y*-minima that fall *below* the mean of the *y* data and *above* the lower quarter).

***Circularity*:** This feature tries to capture how "round" or "distended" the handwritten characters are. It is measured as the ratio of the *area* to the horizontal length. This feature is one that is quite difficult for a forger to judge so proves useful in preventing false acceptances. The area of signatures with multiple components is found by summing each of the independently calculated component areas. Circularity is a computationally expensive feature as it requires several iterations through the *x* and *y* profiles.

***Middle-Heaviness*:** This is the percentage of the handwritten samples bounding box that is interior to the signature itself. It measures the concentration of the handwriting around the midpoint. Calculation is undertaken by finding the signature's area (as performed previously) and dividing this value by the area of the bounding box. The bounding box is a rectangle drawn around the sample using the two extremities in each of the *x* and *y* data streams (with artifacts removed).

***Component Physical Spacing*:** The average spacing between the components is again indicative of a writer's natural style and is very stable across multiple instances of the signature. Calculation involves taking the Euclidean distance between the last point sampled in a component and the first point sampled in the following component (if any). This value is calculated for each pen-up instance and averaged to obtain the final feature value.

***Component Time Spacing*:** This is the average duration of a pen-up instance in a signature (often referred to as pen-up time). It is slightly less stable than physical component spacing, but it is impossible for a forger to copy this feature from an off-line signature image.

D. Signature Verification Approaches [19]

1. **Hidden Markov Model**[1]: Hidden Markov Model (HMM) is one of the most widely used models for sequence analysis in signature verification. A well chosen set of feature vectors for HMM could lead to the design of an efficient signature verification system. 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. There are various topologies for the HMM models, each of which adapt to one particular characteristic. Yacoubi et al. proposed a basic and robust system for the verification of static or offline signatures. AERs of 0.46% and 0.91% are reported in his experiment.

Justino et al. [6] in his work presented a robust system for off-line signature verification using simple features, different cell resolutions and multiple codebooks in an HMM framework. An FRR of 2.83%and an FAR of 1.44%, 2.50%, and 22.67% are reported for random, casual, and skilled forgeries, respectively.

2. **Neural Networks Approach**[1]: The main reasons for the widespread usage of neural networks (NNs) in pattern recognition are their power and ease of use. 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.

Alan McCabe et al. [10] proposed a method for verifying handwritten signatures 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 3.3% being reported for the best case.
Rasha Abbas in his earlier research investigated the suitability of using backpropagation neural networks for the purpose of offline signature verification however later on in [4] the suitability of using multilayered feed forward neural network was investigated.

3. **Template Matching Approach** [1][9]: Fang et al. 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 gray-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 gray-level signature images were used for matching and with the full estimated covariance matrix incorporated.

4. **Statistical Approach**[1]: Using statistical knowledge, the relation, deviation, etc between two or more data items can easily be found out. 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 Bayesian model for off-line signature verification involving the representation of a signature through its curvature is developed by McKeague[11]. The prior model makes use of a spatial point process for specifying the knots in an approximation restricted to a buffer region close to a template curvature, along with an independent time warping mechanism. In this way, prior shape information about the signature can be built into the analysis. The observation model is based on additive white noise superimposed on the underlying curvature. The approach is implemented using Markov chain Monte Carlo (MCMC) algorithm and applied to a collection of documented instances of Shakespeare's signature.
The algorithm proposed in [5] has the flexibility of choosing the number of signature for testing purpose to generate a signature containing the specialized mean features set from the test signatures set. After collecting the signatures for testing, the algorithm converts them into a set of 2D arrays of binary data values-0 and 1.

5. **Support Vector Machines(Structural/Syntactic Approach)** [1]: The key idea in structural and syntactic pattern recognition is the representation of patterns by means of symbolic data structures such as strings, trees, and graphs. In order to recognize an unknown pattern, its symbolic representation is compared with a number of prototypes stored in a database. Structural features use modified direction and transition distance feature (MDF) which extracts the transition locations and are based on the relational organization of low-level features into higher-level structures. The Modified Direction Feature (MDF) [12] utilizes the location of transitions from background to foreground pixels in the vertical and horizontal directions of the boundary representation of an object.

Nguyen et al [2] presents a new method in which structural features are extracted from the signature's contour using MDF and its extended version: the Enhanced MDF (EMDF) and further two neural network-based techniques and Support Vector Machines (SVMs) are investigated and compared for the process of signature verification. The classifiers were trained using genuine specimens and other randomly selected signatures taken from a publicly available database. A distinguishing error rate (DER) of 17.78% was obtained with the SVM whilst keeping the false acceptance rate for random forgeries (FARR) below 0.16%.

6. **Wavelet Based Approach** [1]: A novel approach to off-line signature verification is proposed by Wei Tian et al. [13]. Both static and pseudodynamic features are extracted as original signal, which are processed by Discrete Wavelet Transform (DWT) and converted into stable features in each sub-band which can enhance the difference between a genuine signature and its forgery. During the training phase, the proposed fuzzy net is trained with genuine signatures only. The signatures with the maximal ratio of the mean value of the similarity to the standard deviation are selected as the training samples from a set of genuine signatures. The verification scheme is achieved by combining the proposed fuzzy net output in each sub-band level. The entire system was tested by using two databases of English and Chinese signatures, and the average error rates of 12.57% and 13.96% were obtained, respectively.
Each type of forgery requires a different verification approach. Hence it becomes mandatory to compare these approaches with respect to various levels of forgeries [1].

- **Template matching** is suitable for rigid matching to detect genuine signatures however these methods are not very efficient in detecting skilled forgeries.
- **Neural networks** are among the most commonly used classifiers for pattern recognition problems. This approach offers a significant advantage that each time we want to add a set of signatures (a new person) to the systems database; we only have to train three new small neural networks (one for each set of features) and not the entire neural network. This approach gives very promising results with extremely low FAR and FRR.
- Methods based on the **statistical approach** are generally used to identify random and simple forgeries. The reason for this is that these methods have proven to be more suitable for describing characteristics related to the signature shape. For this purpose, the graphometry-based approach has many features that can be used, such as calibration, proportion, guideline and base behaviors. In addition, other features have been applied in this approach, like pixel density, pixel distributions. However, static features do not describe adequately the handwriting motion. Therefore, it is not enough to detect skilled forgery.

- When using **HMM**s for signature verification, we can find that the simple and random forgery error rates have shown to be low and close to each other, but the type II error rate in skilled forgery signatures are high.
- **Structural** techniques are suitable for detecting genuine signatures and targeted forged signatures however, this approach is exhaustive due to demand for large training sets and computational efforts.

III. ARTIFICIAL NEURAL NETWORKS

Neural networks (NNs) have been a fundamental part of computerised pattern recognition tasks for more than half a century, and continue to be used in a very broad range of problem domains [26]. Concentrated efforts at applying NNs to HSV have been undertaken for over a decade with varying degrees of success. 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 generalise*:** 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).

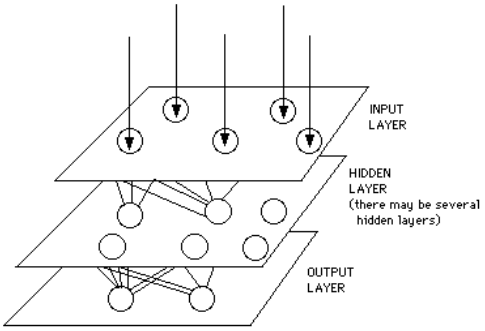

Figure 2: Simple Neural Network

Dr. Robert Hecht-Nielsen defines a neural network as: "A computing system made up of a number of simple, extremely interrelated processing elements, which practice information by their dynamic state response to peripheral inputs" [20]. They are usually presented as organization of interconnected "neurons" that can calculate values from inputs by providing information through the network. Neural networks are characteristically structured in layers. Layers are consisting of a number of interrelated 'nodes' which hold an 'activation function'. Patterns are available to the network by means of the 'input layer', which communicate to one or more 'hidden layers' where the concrete processing is done using a system of subjective 'connections'. The hidden layers then unite to an 'output layer' where the answer is final output of the system.

Artificial neural network i.e. ANNs are not chronological or essentially deterministic. There are no intricate central processors, to a certain extent there are numerous uncomplicated ones which generally do nothing more than take the weighted summation of their inputs from other processors. ANNs do not execute programmed instructions; they react in parallel to the pattern of inputs offered to it. There are no separate memory addresses to accumulate data. Instead, information is controlled in the general activation 'state' of the network. 'Knowledge' is represented by the network itself, which is fairly more than the summation of its individual components. Although there are many different types of knowledge rules used by neural networks, this expression is concerned with the delta rule. The delta rule is

frequently use by the most ordinary class of ANNs called 'back propagation neural networks'. With the delta rule, 'learning' is a organized process that take place with each cycle during a forward activation stream of outputs, and the backwards error propagation of weight regulation. Levenberg-Marquardt backpropagation algorithm [19] trains a neural network using error backpropagation training algorithm [20].

IV. PROPOSED WORK

A multilayer Perceptron with single hidden layer having approx 15-30 nodes in hidden layers with learning rates ranging from 0.05 to 0.95 with increment of 0.5 and sigmoidal activation function. Backpropogation (unsupervised) training algorithm would be used [6]. Data might vary with experimentation.
After relating 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 [20,22].
False Acceptance Rate (FAR), False Rejection Rate (FRR), Overall Error Rate (OER) and Correct Classification Rate (CCR) are the three constraint used for measuring performance of system. All these constraints are calculated [22] by following equations [20],

FAR = (Number of forgeries accepted/Number of forgeries tested) * 100
FRR = (Number of originals rejected/Number of original tested) * 100
OER=FAR_FRR
CCR = (Number of samples correctly Recognized/Number of samples tested) * 100

V. CONCLUSION

Recognition and verification ability of the system can be increased by using additional features in the input data set to reduce to a minimum the cases of forgery in business transaction [19,20,32]. Hence I propose a Handwritten Signature Verification System using Artificial Neural Networks for classification on random, simple and skilled forgeries using more no. of feature sets for better accuracy.

REFERENCES

[1] Meenakshi S. Arya, Vandana S. Ianmdar, “A Preliminary Study on Various Off-line Hand Written Signature Verification Approaches” International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 9 2010.
[2] Vu Nguyen; Blumenstein, M.; Muthukkumarasamy V.; Leedham G., “Off-line Signature Verification Using Enhanced Modified Direction Features in Conjunction with Neural Classifiers and Support Vector Machines”, in Proc. 9th Int Conf on document analysis and recognition, vol 02, pp. 734-738, Sep 2007.
[3] MI C. Fairhurst, “Signature verification revisited: promoting practical exploitation of biometric technology”, Electronics & communication engineering journal, December 1997.
[4] Rasha Abbas and Victor Ciesielski, “A Prototype System for Off-line Signature Verification Using Multilayered Feed forward Neural Networks,” February 1995.
[5] Bhattacharyya Debnath, Bandyopadhyay Samir Kumar, Das, Poulami, Ganguly Debashis, Mukherjee Swarnendu, “Statistical approach for offline handwritten signature verification”, Journal of Computer Science March 01, 2008.

[6] Edson J. R. Justino, Flávio Bortolozzi and Robert Sabourin, "Off-line Signature Verification Using HMM for Random, Simple and Skilled Forgeries", in International Conference on Document Analysis and Recognition, vol. 1, pp. 105–110, Seattle, Wash, USA, 2001.
[7] M. Ammar, Y. Yoshido and T. Fukumura, "A new effective approach for offline verification of signatures by using pressure features", in Proc. 8th Int. Conf. Pattern Recognition, 1986, pp. 566-569.
[8] R. N. Nagel and A. Rosenfeld, "Computer detection of freehand forgeries", IEEE Trans. Comput. , 1997, pp. 895- 905.
[9] Stuart Inglis ,Ian H. Witten, "Compression-based Template Matching", Proc. IEEE Data Compression Conference, pp. 106-115, Los Alamitos, CA, 1994.
[10] Alan McCabe, Jarrod Trevathan and Wayne Read, "Neural Network-based Handwritten Signature Verification", Journal of computers, vol. 3, no. 8, August 2008.
[11] Ian W. McKeague, "A statistical model for signature verification", May 14, 2004.
[12] M. Blumenstein, X. Y. Liu, and B. Verma, "A Modified Direction Feature for Cursive Character Recognition," in International Joint Conference on Neural Networks, pp. 2983- 2987, 2004.
[13] Wei Tian, Yizheng Qiao and Zhiqiang Ma, "A New Scheme for Off-line Signature Verification Using DWT and Fuzzy Net", 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing.
[14] S. Gupta, "Recognition of signature offline", MulticonW 2014.
[15] H. Anand, D.L. Dhombe, "Relative study of signature verification and recognition system", International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 5 (June 2014) http://ijirae.com.
[16] V. Pandey, S. Shantiya, " Signature Verification Using Morphological Features Based on Artificial Neural Network " International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X www.ijarcsse.com.
[17] Kalenova," Personal Authentication using Signature Recognition",D.2005.
[18] 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.
[19] A. Kapil, J. Singh, V. Srivastava, "A Hybrid Approach for Offline Signature Verification using Artificial Neural Networks", International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 12 (2014), pp. 1113-1121 © International Research Publications House http://www. irphouse.com.
[20] S. Sthapak, M. Khopade, C. Kashid, "Artificial Neural Network Based Signature Recognition & Verification", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 8, August 2013).
[21] O.C Abikoye M.A Mabayoje R. Ajibade "Offline Signature Recognition & Verification using Neural Network", Department of Computer Science University of Ilorin P.M.B 1515, Ilorin, Nigeria, International Journal of Computer Applications (0975 – 8887) Volume 35– No.2, December 2011.
[22] Ashwini Pansare, Shalini Bhatia "Off-line Signature Verification Using Neural Network", International Journal of Scientific & Engineering Research, Volume 3, Issue 2, February-2012 1 ISSN 2229-5518.
[23]S.T. Kolhe, S. E. Pawar, Dept. of Computer Engg, AVCOE, Sangamner, India, " Offline Signature Verification Using Neural Network", International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.3, May-June 2012 pp-1171-1175.
[24] Cemil OZ, Sakarya University Computer Eng.Department, Sakarya, Turkey, Fikret Ercal,UMR Computer Science Department, Rolla, MO 65401, Zafer Demir, Sakaraya University electric electronic eng. Department sakarya , Turkey, "Signature Recognition and Verification with ANN".
[25] Baltzakis H., Papamorkos N., "A new signature verification technique based on a two-stage neurol network classifier.", PergomanEngineering Aplication of Intelligence 14, pp.95-103, 2001.
[26] A. McCabe, J. Trevathan and W. Read, "Neural Network-based Handwritten Signature Verification", JOURNAL OF COMPUTERS, VOL. 3, NO. 8, AUGUST 2008.

[27] P. Gallinari, S. Thiria, F. Badran and F. Fogelman-Soulie. *On the Relations between Discriminant Analysis and Multilayer Perceptrons.* Neural Networks, Vol. 4, pp 349–360, 1991.
[28] E. Zois and V. Anastassopoulos. *Methods for Writer Identification.*Proceedings of the Third IEEE International Conference on Electronics, Circuits and Systems (ICECS), 1996.
[29] "An Introduction to Artificial Neural Systems" by Jacek M. Zurada, West Publishing Company 1992.
[30] H. Baltzakis, N. Papamarkos, "A new signature verification technique based on a two-stage neural network classifier", Engineering Applications of Artificial Intelligence 14 (2001) 95±103, 0952-1976/01/$ - PII: S 0 9 5 2 - 1 9 7 6 (0 0) 0 0 0 6.
[31] M. Arathi, A. Govardhan, "An efficient offline signature verification system", International Journal of Machine Learning and Computing, Vol. 4, No. 6, December 2014.
[32] H.B.Kekre, V.A.Bharadi, S.Gupta, A.A.Ambardekar, V.B.Kulkarni, "Off-Line Signature Recognition Using Morphological Pixel Variance Analysis", ICWET'10.

