Approaches and Issues in Offline Signature Verification System

Hemanta Saikia
Dept of Electronics & Communication Engineering
Sikkim Manipal Institute of Technology
Majitar, Sikkim, INDIA

Kanak Chandra Sarma
Department of Instrumentation & USIC
Gauhati University,
Guwahati, Assam, INDIA

ABSTRACT

Offline signature verification is one of most challenging area of pattern recognition. In this paper, we have presented a survey of various approaches and issues related to offline signature verification systems. We have presented some of the research works including comprehensive references as an aid for researchers working in the field.

General Terms

Pattern Recognition, Signature verification, Feature Extraction

Keywords

Offline Signature verification, Feature extraction

1. INTRODUCTION

Signature is one of the most popular and legally accepted biometrics used in person identification. Depending on data acquisition mechanism, there are two methods of signature verification - Online or Dynamic and Offline or Static. Online method requires special set of devices and instruments to capture the pen movements and pressure over the paper at the same time of the writing. On the other hand, the offline approach uses an optical scanner to obtain the signature in order to obtain a digital representation composed of M × N pixels. In offline signature verification, the signature image is considered as a discrete 2D function f(x, y), where x = 0, 1, 2, …, M and y = 0, 1, 2, …,. N denote the spatial coordinates. The value of f in any (x, y) corresponds to the grey level in that point [1]. Processing is done on the scanned images.

Offline signature recognition is more difficult than online as dynamic information are not available and it is difficult to recover them from the offline images. But requirement of acquiring the signature on some special arrangement makes the online method unsuitable for many of the practical uses. Offline has the advantage of using it in the same way as the existing manual recognition method.

2. TERMINOLOGIES IN SIGNATURE VERIFICATION

2.1 Types of Forgeries

In signature verification systems, forgeries may be classified in three basic types [2]:

1. Random forgery: The forger nor has access to the genuine signature neither has any information about the author's name. Forger reproduces a random signature.

2. Simple forgery: The forger has no access to the sample of the signature but he/she knows the author's name and the forger produces the signature in his/her own style.

3. Skilled forgery: The forger has access to the samples of the genuine signature and thus he/she is able to reproduce it.

2.2 Error Rate

In signature verification systems, the performance is evaluated in terms of error rates [2]. There are two types of errors: False Rejection and False Acceptance. Also, there are two types of error rates: False Rejection Rate (FRR) and False Acceptance Rate (FAR). The false rejection rate (FRR) is related to genuine signatures that were rejected by the system; that is, classified as forgeries, whereas the false acceptance rate (FAR) is related to forgeries that were misclassified as genuine signatures. FRR is known as type 1 and FAR is known as type 2 error. The Average Error Rate (AER) is the average of type 1 and type 2 errors [3]. Another factor that determines the efficiency of the system is the Equal Error Rate (EER). The EER is the location on a ROC or Detection Error Trade-off curve where the FAR and FRR are equal. Smaller the value of EER, better is the performance of the system.

3. STEPS IN OFFLINE SIGNATURE VERIFICATION

Offline signature verification is a pattern recognition problem and a typical pattern recognition system has the following steps [5][1]: (i) ***Data Acquisition*** – to capture the signature image (ii) ***Preprocessing*** – to simplify subsequent operations without loosing relevant processing (iii) ***Feature Extraction*** - to reduce the data by measuring certain "features" or "properties" (iv) ***Classification*** (called verification in the signature verification field) – to evaluate the evidence presented in the values of the features obtained from feature extraction and makes a final decision for classification (iv) ***Performance Evaluation*** – to evaluate the efficiency of the signature verification system.

Type of operations in Preprocessing, Feature Extraction and Classification depend on the signature pattern. During the last decade, there have been substantial amount of investigations in the field of offline signature verifications for various structured/scripted signatures such as English, Chinese, Arabic etc.

3.1 Data Acquisition

For offline signature verification system, images of the signatures are scanned using a digital scanner. Scanned images are stored digitally for offline processing.

3.2 Preprocessing

Signature preprocessing is a necessary step to improve the accuracy of Feature extraction and Classification and to reduce their computational needs. The purpose of pre-processing phase is to make signatures standard and ready for feature extraction. The pre-processing stage primarily involves some of the following steps: [3] [6]

1. Noise reduction: A noise filter (like median filter) is applied to remove the noise caused during scanning

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

3. Binarization: Transformation from color to grayscale, and then to binary

4. Thinning: The goal of thinning is to eliminate the thickness differences of pen by making the image one pixel thick. The aim of this is to reduce the character features to help in feature extraction and classification.

5. Clutter Removal: Any unconnected black dots are removed before processing. This is done by masking.

6. Skeletonization: Skeletonization is used to remove selected foreground pixels from the binary image. So the outcome is a representation of a signature pattern by a collection of thin arcs and curves. Skeletonization is performed on a binary image after the size of the image is fixed.

3.3 Feature Extraction

The success of a signature verification system greatly depends on Feature extraction. An ideal feature extraction technique extracts a minimal feature set that maximizes interpersonal distance between signature examples of various persons while minimizing intrapersonal distance for those belonging to the same person [1].

Features extracted for off-line signature verification can be broadly divided into three main categories [7]:

1. Global Features

2. Local Features

3. Geometric Features

3.3.1 ***Global features*** – The signature is viewed as a whole and features are extracted from all the pixels confining the signature image.

Based on the style of the signature, different types of Global features are extracted. Following global features are found in literatures [8][9][10][11][12]-

1. **Signature area (Signature Occupancy Ratio):** It is the number of pixels which belong to the signature. This provides information about the signature density.

2. **Signature height-to-width ratio (Aspect Ratio):** This is obtained by dividing signature height to signature width. Height-to-width ratio of one person's signatures is approximately equal.

3. **Maximum horizontal histogram and maximum vertical histogram:** The horizontal histograms are calculated for each row. The row with the highest value is taken as maximum horizontal histogram. Same is done vertically for every column to calculate maximum vertical histogram.

4**. Horizontal and vertical center of the signature**: These are the measurements indicating the Horizontal and Vertical location of the signature image.

5. **Edge point numbers of the signature:** Edge point is the pixel with only one neighbour.

6. **Signature height:** It is the height of the signature image, after width normalization.

7. **Image area:** It is the number of black (foreground) pixels in the signature image. In skeletonized signature images, it represents a measure of the density of the signature traces.

8. **Pure width:** The width of the image after removal of horizontal blank spaces.

9. **Pure height:** This is the height of the signature after removing the vertical blank spaces.

10. **Vertical projection peaks:** It is the number of the local maxima of the vertical projection histogram.

11. **Horizontal projection peaks:** It is the number of the local maxima of the horizontal projection histogram.

12. **Global slant angle:** The global slant angle represents the overall direction of line strokes in a skeleton signature.

13. **Local slant angle:** It represents the angle of long or dominant strokes in the skeleton Image.

14. **Number of edge points:** An edge point is defined as a signature point that has only one 8-neighbor.

15. **Number of cross points:** Cross point is a signature point that has at least three 8-neighbors.

16. **Number of closed loops:** It is the number of closed loops (Loops are connected regions in the image which are fully enclosed by "signature" pixels) in a skeletonized imaged.

17. **Baseline Slant Angle:** Baseline is the line imagined below the signature above which the signature is considered to rest. The angle between the base line and the horizontal line is the Slant Angle.

18. **Centre of Gravity:** There are Vertical Centre of Gravity and Horizontal Centre of Gravity. Vertical centre of gravity is a measurement indicating the vertical location of the signature image and Horizontal centre of gravity is a measurement indicating the horizontal location of the signature image.

19. **Baseline shift:** It is the difference between the vertical centre of gravity of the left and right part of the skeleton signature image. This indicates the overall orientation of the signature.

3.3.2 ***Local features*** – Local features are extracted from a portion or a limited area of the signature image [13]. Local features are applied to the cells of a grid virtually super imposed on a signature image or to particular elements obtained after signature segmentation. These features are calculated to describe the geometrical and topological characteristics of local segments, such as position, tangent direction, and curvature [14]. They represent a segment or limited region of the signature image, such as critical junctions and gradients. These features are generally derived

from the distribution of pixels of a signature, such as local pixel density or slant [7]. Some of the local features are the slant angle of an element, number of black pixels, length ratio of two consecutive parts, position relation between the global and local baseline, upper, central line features, corner line features, unballistic motion and tremor information in stroke segments, stroke elements, local shape descriptors, pressure and slant features and critical points etc [15].

Moreover, local features can be classified as contextual and non-contextual. If segmentation is performed in the signature for interpreting the text, the analysis is considered contextual. This type of analysis is not popular for two reasons: (1) it requires a segmentation process and it is very difficult and (2) it is not suitable for graphical signatures. On the other hand, if the signature is viewed as a drawing the analysis is considered non-contextual and it occurs in the majority of the works [1].

3.3.3 *Geometric features* – These features describe the characteristic geometry and topology of a signature and preserve their global as well as local properties.

Geometrical features have the ability to tolerate with distortion, style variations, rotation variations and certain degree of translation [16][6].

3.3.4 *Choice of Features*

The choice of using global or local features depends mainly on style of the signature as well as the types of forgeries to be detected by the system. A suitable combination of global and local features has been found to improve a classifier's ability to recognize forgeries and to tolerate intrapersonal variances (cited by [13]).

The global features are extracted at a low computational cost, and they have good noise resilience. These features are less sensitive to noise and signature variations. So it does not give a high accuracy for skilled forgeries, but it is suitable for random forgeries and is better to be combined with other types of features [16].

On the other hand, even though the local features are dependent on the zoning process, still they are more suitable to identify skilled forgeries [1]. Local features describe only a small portion of signature and extract more detailed information from the image. Local features are more sensitive to noise and they are not affected by other regions of the signature. Although they are computationally expensive, they are much more accurate than global features [17].

The global features can deliver limited information for signature verification [14]. Small distortions in isolated regions of the signature do not cause a major impact on the global feature vector. They are, however, dependent upon the overall position alignment and therefore highly susceptible to distortion and style variations [1].

On the other hand, local features provide rich descriptions of writing shapes and are powerful for discriminating writers, but the extraction of reliable local features is still a hard problem [14].

The local features based approaches are more popular in online verification than in the offline. Because as compared to 2D images, it is much easier to calculate local shape features and to find their corresponding relations in 1D sequences [14].

In manual verification, global features are observed and it is seen that the intra personal variations with respect to the global aspect is very low.

Some global features can also be applied locally, and vice versa. For instance, contour-based features can be extracted at global level or at local level [18]. A suitable combination of global and local features will produce more distinctive and effective features, and the idea of localizing global features will allow the system to avoid the major drawbacks of both and the advantages of both can be exploited [17].

3.4 CLASSIFICATION

The major approaches to off-line signature verification systems are the Template Matching approach, Statistical approach, Structural or Syntactic approach, Spectrum Analysis approach and Neural Networks approach [6][17][19].

3.4.1 *Template Matching Approach* – The template matching is the simplest and earliest but rigid approach to pattern recognition. Because of its rigidness, in some domains, this approach has a number of disadvantages. It may fail if the patterns are distorted due to the imaging process, viewpoint change or large intraclass variations among the patterns as in the case of signatures. It can detect casual forgeries from genuine signatures successfully. But it is not suitable for the verification between the genuine signature and skilled ones. The template matching method can be categorized into several forms such as graphics matching, stroke analysis and geometric feature extraction, depending on different features.

3.4.2 *Statistical Approach* – In the statistical approach, each pattern is represented in terms of d features and is viewed as a point in a d-dimensional space. Features should be chosen such a way that the pattern vectors belonging to different categories occupy compact and disjoint regions in a d-dimensional feature space. The effectiveness of the representation space (feature set) is determined by how well patterns from different classes can be separated. Hidden Markov Model (HMM), Bayesian these are some statistical approach commonly used in pattern recognition. They can detect causal forgeries as well as skilled and traced forgeries from the genuine ones.

3.4.3 *Structural Approach* - Structural approaches mainly related to string, graph, and tree matching techniques and are generally used in combination with other techniques [18]. When the signature image is considered as a whole entity, the structural approach is used for the signature verification. It shows good performance detecting genuine signatures and forgeries. But this approach may demand a large training set and very large computational efforts.

3.4.4 *Spectrum Analysis Approach* – To decompose a curvature-based signature into a multi-resolution format, spectrum analysis approach is introduced. This method can be applied to different languages, including English and Chinese. Moreover this approach may be useful especially for long signatures like some of the Indian scripted signature.

3.4.5 *Neural Network Approach* – Neural networks are massively parallel computing systems consisting of an extremely large number of simple processors with many interconnections. The main characteristics of neural networks are that they have the ability to learn complex nonlinear input-output relationships, use sequential training procedures and adapt themselves to the data. Neural Networks approach offers several advantages such as, unified approaches for feature extraction and classification and flexible procedures

for finding good, moderately nonlinear solutions. When it is used in off-line signature verification, it also shows reasonable performance.

Each of these approaches has its own advantages and disadvantages. And the result of an off-line signature verification system using only one approach is not reasonable. Combination of different approaches may give better result. The designer of a pattern recognition system need to give careful attention to these issues [19]: definition of pattern classes, sensing environment, pattern representation, feature extraction and selection, cluster analysis, classifier design and learning, selection of training and test samples and performance evaluation.

4. SOME APPROACHES IN OFFLINE SIGNATURE VERIFICATION

To improve the efficiency of the signature verification systems, researchers have tried different methods with various approaches. Some of them have employed two or three expert systems that evaluate the signature in two/three different ways and verify whether it is genuine or forgery.

J. B. Fasquel and M. Bruynooghe [20] proposed one offline signature verification system combining some statistical classifiers. The signature verification system consisted of three steps – the first step is to transform the original signatures using the identity and four Gabor transforms, the second step is to intercorrelate the analyzed signature with the similarly transformed signatures of the learning database and then in the third step verification of the authenticity of signatures by fusing the decisions related to each transform. The proposed system allowed the rejection of 62.4% of the forgeries used for the experiments when 99% of genuine signatures were correctly recognized.

Sharifah Mumtazah Syed Ahmad et al. [21] presented an automatic off-line signature verification system built with several statistical techniques. They used Hidden Markov Modeling (HMM) technique to build a reference model for each local feature. The verification phase had three layers of statistical techniques. In the first layer, HMM-based log-likelihood probability match score was computed. In the second layer this score was mapped into soft boundary ranges of acceptance or rejection through the use of z-score analysis and normalization function. Then Bayesian inference technique was used for deciding acceptance or rejection of the given signature sample. For random and skilled forgeries FAR were 22% and 37% respectively.

H. Baltzakis and N. Papamarkos [10] proposed system was based on global, grid and texture features. For each one of the feature sets a special two stage Perceptron OCON (one-class-one-network) classification structure was implemented. In the first stage, the classifier combined the decision results of the neural networks and the Euclidean distance obtained using the three feature sets. The results of the first-stage classifier feed a second-stage radial base function (RBF) neural network structure, which made the final decision. FAR was 9.81% and FRR was 3%.

Abhay Bansal, Divye Garg, Anand Gupta [22] proposed a contour matching algorithm. They used the geometrical properties of the signature and considered the inevitable intrapersonal variations for the user set A. The system was trained with 8 original signatures and given a test sample. Verification was done by a triangle matching algorithm. FAR in case of Random Forgery was found to be 0.08% and in case of Simple and Skilled forgery it was 13.02%. FRR was 2.64%.

To tackle the problem of detecting skilled forgeries in off-line signature verification B. Fang et al. [23] proposed an approach based on a smoothness criterion. They observed that skilled forgery signatures consisting of cursive graphic patterns are less smooth on a detailed scale than the genuine ones. They derived a smoothness index from such signatures and was combined with other global shape features and used for verification.

Ramachandra A C et al. [4] proposed a Cross-validation for Graph Matching based offline Signature Verification (CGMOSV) algorithm. The dissimilarity measure between two signatures in the database was determined by (i) constructing a bipartite graph (ii) obtaining complete matching in and (iii) finding minimum Euclidean distance by Hungarian method. Using Cross-validation principle reference signatures were selected and an optimum decision threshold value was determined. The threshold value was used to compare and authenticate the test signature. They observed that FRR, FAR and EER values were improved compared to the existing algorithm.

Vu Nguyen et al. [13] used the total energy that a writer uses to create his/her signature as a global feature. They extracted energy information from the boundary of the whole signature image. This energy information was decomposed into horizontal and vertical components. The features extracted were the values from the signature width divided by horizontal energy (e_h), signature height divided by vertical energy (e_v), and $\min(e_h,e_v)/\max(e_h,e_v)$. The second feature was information from the vertical and horizontal projections of a signature, focusing on the proportion of the distance between key strokes in the image, and the height/width of the signature. They combined these features with the Modified Direction Feature (MDF) and Support Vector Machines were employed to construct the signature models. Obtained AER was 17.25%.

Daramola Samuel and Ibiyemi Samuel [24] proposed an off-line signature verification technique that used three new feature sets extracted from a static image of signatures. The three feature sets were image cell size, image centre angle relative to the cell lower right corner and pixels normalized angle relative to the lower right corner. The proposed system had an FAR of 1% and FRR of 0.5%.

M. Fakhlai and H. Pourreza [25] proposed an offline signature recognition approach based on three different kinds of feature extractors - wavelet, curvelet and contourlet transform. The curvature and orientation of a signature image was used as feature. They utilized Support Vector Machine (SVM) as a tool to evaluate the performance of the proposed methods. The recognition rates of the three transforms were: Wavelet 80.75%, Curvelet 89.87% and Contourlet 96.55%. So contourlet transform could extract better features among them.

In a paper [26] Miguel A. Ferrer et al. used a set of geometric signature features for offline automatic signature verification based on the description of the signature envelope and the interior stroke distribution in polar and Cartesian coordinates. The features were calculated using 16 bits fixed-point arithmetic and were tested with different classifiers, such as Hidden Markov Models, Support Vector Machines and Euclidean distance classifier. The experiments showed that for a set of twelve signatures, for random forgery FRR was lowest of 2.2% with the use of HMM and FAR was lowest of

2.65% with SVM. In case of simple forgery, FRR and FAR both were lowest (14.1% and 12.67%) with HMM.

Emre Özgündüz et al. [8] proposed an off-line signature verification and recognition system using the global, directional and grid features of signatures. Global features used were Signature area, Aspect Ratio of the signature, Maximum horizontal histogram and maximum vertical histogram, Horizontal and vertical center of the signature,. Local maxima numbers of the signature and Edge point numbers of the signature. SVM was used for classification. Their obtained recognition rate was 95%.

An offline signature verification system based on two neural networks classifier and three features (global, texture and grid) was proposed by Mohammed A. Abdala & Noor Ayad Yousif [27]. The first NN classifier they used was three Back Propagation NNs and the second classifier consisted of two Radial Basis Function NNs. When two back propagation NNs of the first classifier recognized the signature, the recognition rate of the system was 95.955%, on the other hand when all three back propagation NN recognized recognition rate was 99.31%.

V A Bharadi and H B Kekre [28] had designed a multi algorithmic signature recognition system considering the conventional features like Number of pixels, Picture Width, Picture Height, Horizontal max Projections, Vertical max Projections, Dominant Angle-normalized, Baseline Shift etc. For extracting information in pixel distribution of the Signature, they proposed Walsh Coefficients, Vector Histogram, Grid and Texture Feature as global as well as cluster based Features. The system reported an accuracy of 95.08%.

H.N. Prakash and D. S. Guru [29] proposed an approach for offline signature verification based on score level fusion of distance and orientation features of centroids. The proposed method used symbolic representation of offline signatures using bi-interval valued feature vector. Distance and orientation features of centroids of offline signatures were used to form bi-interval valued symbolic feature vector for representing signatures. With 9 training samples per class 31 centroids and Threshold = 233, they achieved FRR of 27.77% and FAR of 26.11%, with 63 centroids and threshold = 977, FRR and FAR were 20.22% and 29.51% respectively.

Madasu Hanmandlu et al. [30] proposed an offline signature verification and forgery detection approach based on fuzzy modeling that used a model called the "Takagi–Sugeno (TS) model". The TS model involved structural parameters in its exponential membership function. Signature verification and forgery detection were carried out using angle features extracted from box approach. They tried the TS model with fixed and adapted consequent coefficients and observed that TS model with fixed consequent coefficients performed better.

Hai Rong Lv et al. [31] used HMM approach to offline signature verification. They represented each of the signature images as landmark point set, which included turning points, isolated points, trifurcate points, intersection points and termination points on signature skeleton. They proposed a deformable grid partition technique. Based on landmark point matching, they built the matching relations between planar regions to get the deformable grids, and then extract grid features from them. To represent the grids of a signature image, they used features like pixels Density (numbers of pixels inside the cell), gravity center (gravity center distance in each cell), stroke curvature (curvature angle of the bigger stroke inside the cell), slant (predominant slant inside the cell) and grid area. By using HMM the proposed method produced an EER rate of 6.4%.

J. F. Vargas et al. [32] proposed an offline signature verification system based on grey level information using texture features. They analyzed the co-occurrence matrix and local binary pattern and used as features. Genuine samples and random forgeries were used to train an SVM model. Random and skilled forgeries were used for testing. For skilled forgeries, they were able to achieve an EER of 12.82%,

Stephane Armand et al. [33] proposed a method for off-line signature verification and identification. In their method, the contour of the signature was determined from its binary representation. Using combination of the Modified Direction Feature (MDF) (this technique employs a hybrid of two other feature extraction techniques - Direction Feature and the Transition Feature) some unique structural features were extracted from the signature-contour. They employed Neural Network based classifiers. A Resilient Back Propagation neural network and a Radial Basis Function neural network were compared. Obtained verification rate was 91.12%.

A method for signature verification using local Radon Transform was proposed by Vahid Kiani et al. [15]. The authors used Radon Transform locally for line segments detection and feature extraction. The classifier was SVM. Some of the advantages of the proposed method the authors found were robustness to noise, size invariance and shift invariance. In the proposed method, FRR and FAR were 4% and 17%.

M. Taylan DAS and L. Canan DULGER [34] presented a technique for off-line signature verification based on a neural network (NN) approach trained with Particle Swarm Optimization (PSO) algorithm. Authors examined all the three types of forgeries to test the performance of the proposed PSO-NN algorithm. For skilled forgeries, 40% of the signatures were detected correctly.

In [35] L. Basavaraj and R. D Sudhaker Samuel proposed an offline signature verification scheme using two different features – stroke angle and stroke speed. In order to obtain the speed of the stroke, they considered the intensity of the stroke assuming that intensity increases proportionally with the speed of the stroke. They conducted several experiments to demonstrate the ability of the proposed scheme in discriminating the genuine signatures from the forgeries. Obtained FRR was 14.5%, while FAR was 16.5%.

D. Bertolini et al. [36] proposed a method of off-line signature verification through ensemble of classifiers. They tried to simulate the shape of the signature by using Bezier curves and then extracted features from those curves. They used an ensemble of classifiers based on graphometric features to improve the reliability of the classification thereby reducing the false acceptance. For simulated forgery, they achieved a minimum FAR of 6.48% and for Random and simple forgeries it was 3%.

To reduce the FAR and FRR with lesser training time M. Bhuyan et al. [37] proposed an offline signature recognition and verification scheme based on extraction of features including one hybrid set from the input signature and compared them with the already trained forms. Feature points were classified using statistical parameters like mean and variance. The scanned signature was normalized in slant. The

slant correction was aided by the use of an Artificial Neural Network (ANN). Authors used four ANNs in their approach. The first ANN was trained with Euclidian distances obtained from vertical sectioning of the signature, the second one was trained with Euclidian distances from horizontal sectioning of the signature images, the third ANN was trained with the other two feature sets together and the fourth ANN was trained with image skeleton. They observed that gradient descent with momentum and adaptive learning rate back propagation had produced the best results in training. To evaluate error rate authors used random forgeries and the minimum FER and FAR were 10% when all the four ANNs were used to classify.

From results obtained by the researchers in the field of offline signature verification, it is noticed that the statistical approach, (HMMs, Bayesian etc) can detect causal and skilled forgeries. Recognition rate of 95% was reported to be achieved using SVM [8].

Template matching is the simplest and easiest approach, but it is rigid. So, it cannot detect skilled forgery. Still it is suitable for detecting casual forgeries from genuine signatures.

When the signature image is considered as a whole entity, the structural approach is useful. But computational complexity in this approach is very high as it requires large training sets. The performance is reported to be better when number of training set is sufficiently large. One additional advantage in using structural pattern recognition is that this approach also provides a description of the given pattern.

Signatures with most of the Indian scripted languages are usually long in nature. For such long signatures, spectrum analysis approach (like Curvelet, Contourlet or Wavelet transform) can be better. In [25] authors have found that the contourlet transform could extract better features as an AER of 96.55% was obtained with Contourlet transform.

Neural Networks based approaches have the advantages of being flexible and adaptive. Using three back propagation NNs, a recognition rate of 99.31% was obtained [27]. Neural network based approaches are unified approaches for feature extraction and classification and flexible procedures for finding good, moderately nonlinear solutions. Due to the advent of new learning algorithms and seemingly low dependence on domain specific knowledge, neural network is becoming more popular in the field of pattern recognition. In addition, existing feature extraction and classification algorithms can also be mapped on neural network architectures for efficient (hardware) implementation [19].

5. ISSUES IN OFFLINE SIGNATURE VERIFICATION

In the past decade, there have been ample amount of research in the field of pattern recognition and also in the field of offline signature verification. A bunch of solutions has been introduced, to overcome the limitations of off-line signature verification and to compensate for the loss of accuracy.

Researchers come across two problems in offline signature verification – (i) Most of the dynamic information in the signature is lost and (ii) Low quantity of available signature samples versus high number of extracted features.

The first issue is addressed by some researchers [35] [38]; but this is still a challenging problem.

Luana Batista et al. [1] have mentioned some remedies for the second issue; they are -

1. Select the most discriminating features

2. Use regularization techniques to obtain a stable estimation of the covariance matrix

3. Generate synthetic samples

4. Use dissimilarity representation

5.1 Characteristics of forgeries

In offline signature verification, some general characteristics of genuine signatures and forgeries need to be understood. Knowledge of these characteristics is important for determining those aspects or features of the signatures that are most important for automatic signature verification. In [7] Vamsi Krishna Madasu and Brian C. Lovell have mentioned few such characteristics outlined by several document examiners in the past in various literatures:

1. Enlargement of characters: A forgery is usually larger than the original signature. As compared to the original author, a forger takes more time drawing each letter in the signature. This makes a forgery larger than the original both in terms of the size of letters and the size of the entire signature.

2. Tendency of curves to become angles: Curved letters are often observed in the forgery as being more angular. The forger takes care to obtain the correct letter shape by using a slower speed to produce the curve accurately. This results in more angular letters as greater time elapses in the making of the curves. In the same way, angled letters in the original signature can become smooth curves.

3. Retouching: Many times the forger makes correction at later stage after the imitation has already been. Due to this retouching, in the forge signature, lines may appear to be thicker at these points, or there may be lines that do not follow the continual flow of the pen as in the original signature.

4. Poor line quality: The pressure put on the paper by the pen is not same in case of forged and original signature. It is found that the pressure used for the questioned signature is harder than that of the real signature. The ink reveals variation in light and shade, pressure and speed, with either more or less ink appearing on the page. However, in a forged signature sometimes a lighter pressure can be detected. But this may cause a tremor caused by trembling of the hand, poor line quality, or writing too slowly [23].

5. Hesitation: In the process of creating a forgery, the forger may pause to consult the genuine signature and then continue duplicating it. This can often create blobs.

6. Punctuation: In forgery full stops, dots on small letter 'i' are found to be in the wrong place, missing or added.

7. Differing pressure: It is hard to vary pen pressure in the same way as a genuine signer. Forger cannot imitate identical pen pressure profile as like as the genuine author. The pen pressure may be too heavy or too light, depending on the style of the forger. Pressure differences occur at different places from the genuine signature.

8. Sudden endings: Sudden endings are a characteristic feature of a forgery. It is seen that in many cases the original signature trails off, but the forgery just stops. It is very difficult to trail off in the same way as the genuine.

9. Forger's characteristics: Everyone has his/her own characteristics of handwriting. The forger unconsciously exposes his/her own handwriting characteristics when doing the forgery. It is observed that forger cannot avoid revealing some of his/her writing characteristics like the basic letter shapes, spacing and position of letters in relation to base line even in a forgery.

10. Baseline error: The imaginary line that runs across the base of the signature is not similar in the forged signature and the genuine signature. The baseline in a signature is not horizontal and any notable variances in the baseline indicate forgery.

11. Spacing: Imitating the spacing between individual letters, whole words, and between punctuation and letters is difficult. These spacing may be larger or smaller that cannot be copied by tracing a signature.

12. Bad line quality: A slow forgery results hesitant or shaky pen strokes and domino effect is bad line quality.

13. Forming characters not appearing in signatures: When the forgers know the name of the author of genuine signature that they are trying to forge, unconsciously they include letters in the forgery that do not actually appear in the genuine signature. On the other hand, if the forger is unsure about the name, then incorrect letters may appear clearly in the forgery.

Even though the above mentioned points will help detecting forgery, it is very difficult to apply most of these points to computerized signature verification.

6. CONCLUSION

A human expert is able to identify skilled forgeries with an error rate of 1%. But when tested against skilled forgeries, even the best system is not able to deliver error rates less than 5% [12]. To overcome this, it is essential to identify, understand and compensate for the different sources of error in the algorithms. Cost of an error in signature verification is very high. An automatic signature verification system can come into existence only when its error rate is equal or below the human error rate (1%). User acceptance, level of security required, accuracy, Cost & Implementation these are the basic parameters that must be considered while designing a signature verification system [39].

The major problem associated with signature verification is the availability of limited data. As signature data are legally accepted as the authentication means for many financial or other official works, this is difficult to have a sufficient amount of data required to develop a signature verification system. As a result, robust parameter estimation on limited sample sets is still one of the major research issues in this field. One technique to address this problem is to extend the techniques of classical model adaptation for discriminative training.

The other challenging problem in offline signature verification is the feature extraction process. Choice of features depends on the style of the signatures and hence different styled-signatures will have different characteristic features. So, it is difficult to develop one general system to classify every style of signatures. Signatures in different scripts may not recognized by a single classifier or even a classification system. It has been observed that most of the researchers have proposed or developed their systems for a limited type of signatures. However achieving an acceptable accuracy in various individual signature styles will make it possible to working out a general signature verification system. In the literatures, it is observed that fusion of multiple classifiers with different types of features delivers a better result in the signature recognition system. Future work should focus on adapting the classification function dynamically to the signature for authentication, and thus combining the advantages of different approaches.

7. REFERENCES

[1] Batista, L., Rivard D., Sabourin R., Granger E., Maupin P. 2007. State of the art in off-line signature verification. In: Verma B., Blumenstein M. (eds.), Pattern Recognition Technologies and Applications: Recent Advances, (1e). IGI Global, Hershey (2007)

[2] Coetzer J., Herbst B., & du Preez J. 2004. Off-line signature verification using the discrete radon transform and a hidden Markov model. EURASIP Journal on Applied Signal Processing

[3] Guler I and Meghdadi M. 2008. A different approach to off-line handwritten signature verification using the optimal dynamic time warping algorithm Digital Signal Processing (Science Direct) 18 (2008) (pp 940–950)

[4] Ramachandra A C, Pavithra K, Yashasvini K, Raja K B, Venugopal K R and Patnaik L M. 2008. Cross-Validation for Graph Matching based Offline Signature Verification. India Conference INDICON 2008

[5] Duda R O and Hart P E. 2006. Pattern Classification (2e). Wiley India Private Limited.

[6] Arya M S and Inamdar V S. (2010). A Preliminary Study on Various Off-line Hand Written Signature Verification Approaches. 2010 International Journal of Computer Applications. Volume 1, No. 9 (pp 0975 – 8887)

[7] Madasu V K and Lovell B. C. 2007. An Automatic Off-Line Signature Verification and Forgery Detection System. In: Verma, B., Blumenstein, M. (eds.) Pattern Recognition Technologies and Applications: Recent Advances, 1st ed. IGI Global, Hershey (2007)

[8] Özgündüz E, Şentürk T and M. Karslıgil E. 2005. Offline Signature Verification and Recognition by Support Vector Machine, Eusipco-2005, 4-8 September, 2005, Antalya, Turkey, pp. 113-116

[9] Biswas S. Kim T. and Bhattacharyya D. 2010. Features Extraction and Verification of Signature Image using Clustering Technique. International Journal of Smart Home, Vol.4, No.3, July, 2010

[10] Baltzakis H and Papamarkos N. 2001. A new signature verification technique based on a two-staged neural network classifier. Engineering Applications of Artificial Intelligence 14 (2001) (pp 95-103)

[11] Qi Y. and Hunt B. R. 1994. Signature verification using global and grid features, Pattern Recognition, 27(12), 1621-1629 (1994)

[12] Kovari B, Toth B, Charaf H. 2009. Classification Approaches in Off-Line Handwritten Signature Verification. WSEAS TRANSACTIONS on MATHEMATICS Issue 9, Volume 8, September 2009

[13] Nguyen V, Blumenstein M and Leedham G. 2009. Global Features for the Off-Line Signature Verification

Problem. 2009 10th International Conference on Document Analysis and Recognition (IEEE)

[14] Yu Qiao, Jianzhuang Liu and Xiaoou Tang. 2007. Offline Signature Verification Using Online Handwriting Registration. IEEE Conference on Computer Vision and Pattern Recognition CVPR '07, Minneapolis

[15] Kiani V, Pourreza R and Pourreza H R. 2009. Offline Signature Verification Using Local Radon Transform and SVM. International Journal of Image Processing (IJIP) Volume(3), Issue(5), (pp 184 – 194)

[16] Yazan M. Al-Omari, Siti Norul Huda Sheikh Abdullah and Khairuddin Omar. 2011. State of the art Offline signature verification system. IEEE International Conference on Pattern Analysis and Intelligent Robotics 28-29 June 2011, Putrajaya, Malaysia

[17] Weiping HOU, Xiufen Ye and Kejun. 2004. A Survey of Off-line Signature Verification, Wang Proceedings of the 2004 International Conference on intelligent Mechatronics and Automation Chengdu,China August 2004

[18] Impedovo D. and Pirlo G. 2008. Automatic Signature Verification – The State of the Art. IEEE Transactions on Systems, Man and Cybernetics - PART C: Applications and Reviews, Vol. 38, No. 5, September 2008

[19] Jain A K, Duin R P W, and Mao J. 2000. Statistical Pattern Recognition: A Review. IEEE Transactions on Pattern Analysis and Machine Intelligence, (pp 4 – 37) Vol. 22, No. 1, JANUARY 2000

[20] J. B. Fasquel and M. Bruynooghe. 2004. A hybrid opto-electronic method for fast off-line handwritten signature verification. International Journal on Document Analysis and Recognition (2004)

[21] Ahmad S M S, Shakil A, Faudzi M A, Anwar R M and Balbed M A M. 2009. A Hybrid Statistical Modeling, Normalization and Inferencing Techniques of an Off-line Signature Verification System. 2009 World Congress on Computer Science and Information Engineering

[22] Bansal A, Garg D, and Gupta A. 2008. A Pattern Matching Classifier for Offline Signature Verification. First International Conference on Emerging Trends in Engineering and Technology (IEEE Computer Society)

[23] Fang B, Wang Y Y, Leung C H, Tang Y Y, Kwok P C K, Tse K W and Wong Y K. 1999. A Smoothness Index Based Approach for Off-line Signature Verification. Proceedings of the Fifth International Conference on Document Analysis and Recognition ICDAR'99

[24] Samuel D and Samuel I. 2010. Novel Feature Extraction Technique for Offline Signature Verification System. International Journal of Engineering Science and TechnologyVol. 2(7), 2010, (pp 3137-3143)

[25] Fakhlai M, Pourreza H. 2008. Off line Signature Recognition Based on Wavelet, Curvelet and Contourlet Transforms. 8th WSEAS International Conference on Signal Processing and Computational Geometry and Artificial Vision (ISCGAV'08), Rhodes, Greece, August 20-22, 2008

[26] Miguel A. Ferrer, Jesu´s B. Alonso and Carlos M. Travieso. 2005. Offline Geometric Parameters for Automatic Signature Verification Using Fixed-Point Arithmetic. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 27, No. 6, June 2005

[27] Abdala M. A. and Yousif N. A. 2009 Offline Signature Recognition and Verification Based on Artificial Neural Network Eng & Tech. Journal, Vol.27, No.7, 2009

[28] Bharadi V A and Kekre H B. 2010. Off-Line Signature Recognition Systems. 2010 International Journal of Computer Applications Volume 1, No. 27, (pp 0975 - 8887)

[29] Prakash H N and Guru D S. 2010. Offline Signature Verification - An Approach Based on Score Level Fusion. 2010 International Journal of Computer Applications Volume 1, No. 18, (pp 0975 - 8887)

[30] Hanmandlu M, Hafizuddin M. Yusof M. and Madasu V K. 2005. Off-line signature verification and forgery detection using fuzzy modeling. Pattern Recognition 38 (2005) (pp 341 – 356)

[31] Hai Rong Lv, Wen Jun Yin and Jin Dong. 2009. Offline Signature Verification based on Deformable Grid Partition and Hidden Markov Models. IEEE International Conference on Multimedia and Expo ICME 2009, New York

[32] Vargas J. F., Ferrer M. A., Travieso C. M. and Alonso J. B. 2011. Off-line signature verification based on grey level information using texture features. Pattern Recognition 44 (2011) (pp 375–385)

[33] Armand S, Blumenstein M and Muthukkumarasamy V. 2006. Off-line Signature Verification based on the Modified Direction Feature. The 18th IEEE International Conference on Pattern Recognition (ICPR'06)

[34] DAŞ M T and DÜLGER L C. 2007. Off-Line Signature Verification with PSO-NN algorithm. 22nd International Symposium on Computer and Information Sciences 2007, ISCIS 2007, Ankara.

[35] Basavaraj L and Sudhaker Samuel R D. 2009. Offline-line Signature Verification and Recognition - An Approach Based on Four Speed Stroke Angle. International Journal of Recent Trends in Engineering, Vol 2, No. 3, November 2009

[36] Bertolini D, Oliveira L S, Justino E and Sabourin R. 2010. Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers. Pattern Recognition 43 (2010), (pp 387 – 396)

[37] Bhuyan M, Sarma K K, Das H. 2010. Signature Recognition and Verification using Hybrid Features and Clustered Artificial Neural Network (ANN)s. World Academy of Science, Engineering and Technology 68 (pp 451-456)

[38] Zimmer A and Ling L L. 2003. A Hybrid On/Off Line Handwritten Signature Verification System. Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR 2003)

[39] Jain A K, Ross A and Prabhakar S. 2004. An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004