REVIEW OF LITERATURE
CHAPTER II
REVIEW OF LITERATURE

The review of literature related to the system entitled “IMAGE INTERPRETATION OF DIGITIZED SIGNATURES USING FUZZY LOGIC” is discussed under the following heads.

2.1 Introduction
2.2 Neural Networks
2.3 Hidden Markov Algorithm
2.4 Wavelet Transformations
2.5 Stroke Analysis
2.6 Dynamic Programming Matching (DPM)
2.7 Fuzzy Concepts
2.8 Elastic Matching
2.9 Segmentation Methods
2.10 Other Related Techniques
   2.10.1 Multi expert system
   2.10.2 Data fusion method
   2.10.3 Feature Selection
   2.10.4 Biometric verification
   2.10.5 Hybrid Technology
   2.10.6 Minimum Distance Classifiers
2.11 Conclusion

2.1. INTRODUCTION

Signatures are a special case of handwriting, subject to intrapersonal variation and interpersonal differences. This variability makes it necessary to
analyze signatures as complete images and not as collection of letters and words. Signature verification problem is to determine if a particular signature is authentic or a forgery. It is obvious that the problem of signature verification becomes more and more difficult when passing from random to simple and skilled forgery, the latter being so difficult a task that even human beings make errors in several cases. In fact, exercises in imitating a signature often allow us to produce forgeries so similar to the originals that discrimination is practically impossible. In many cases, the distinction is complicated even more by the large variability introduced by some signers when laying their own signatures (Sansone and Vento, 2000).

2.2 NEURAL NETWORKS

Using neural networks for handwriting recognition is a field that is attracting a lot of attention. Signature verification is a real challenge for researchers because of the many difficulties that can arise during the process of creating such a system. In recent years, neural network techniques have been applied to signature verification with satisfactory results, which are potentially more tolerant and robust when dealing with the intricacies of real data. Researchers have applied new technologies based on neural networks, Hidden Markov Models and other structural algorithms, regional correlation and are continually introducing new ideas, concepts and algorithms.
It is difficult to compare the performance of different signature verification systems because each system uses different signature databases (Fang et al., 2002). Hence, a comprehensive coverage of all the systems involving neural networks would be impracticable. In this part of the review, the performance achieved by some of the systems is discussed.

The novel approach to offline tracing and representation of signatures using neural networks proposed by Lee and Pan (1992) could achieve about 97% recognition rate for the test patterns derived from the training patterns. In similar works reported by Ammar (1991) and Sabourin and Genest (1994), the average error rates for verification using neural networks was 22.8% and 17.8% respectively.

Kalera et al (2004) used Bayes classifier distance statistics and the k-nearest neighbor (k-nn) classifier techniques for offline neuro signature verification and the system produced an accuracy as high as 78.1% for verification and 93.18% for identification on a pure offline database. This technique, when combined with Dynamic Plane Warping algorithm, which was used to extract the dynamic features from the offline signatures and combined with the framework, improved the performance of the system (Leven and Pieraccini, 1992).

Xiao and Leedham (1999), further improved the verification of identifying skilled forgeries by the use of feedback neural network classifier to pay special
attention to local stable parts of signatures by weighting their corresponding node response through a feedback mechanism. The result of the system, gave an improved version to identify skilled forgeries.

A different approach proposed by Velez et al. (2003) based on the use of compression neural networks and automatic generation of the training set from only one signature from each writer reduced the False Acceptance Rate (FAR).

The usage of artificial neural networks in the process of signature verification and recognition system reduces the error rates and increases the system reliability, thus leading to a more robust system (MATLAB, Neural Network ToolBox).

This concept was employed by Oz (2005) and he has recently reported that by using two separate sequential neural networks, one for recognition (recognition network) and another for verification (verification network), the performance of the verification system could be improved tremendously.

The work proposed by Justino et al. (2005), supports the above concept in their system which used statistical learning theory and Hidden Markov Model to produce a robust recognition and verification system.

The usage of growing cell neural network in the offline signature recognition process can produce a fairly good recognition rate with a relatively low computation complexity (Medina et al., 2001). Using the same approach
with temporal coding for quick one-shot object learning and glance object recognition, Atsumi (2004) showed that self-organized learning is quickly and successfully performed in signature recognition.

Drouhard et al. (1999) used Back Propagation Network (BPN) for improving the performance of automatic handwritten signature verification system. He proved that the usage of BPN reduces the error minimization process in signature verification process.

Another method for off line signature verification based on geometric feature extraction and neural network classification was proposed by Huang and Yan (1997), which used artificially generated genuine and forgery samples from enrollment reference signatures to train the network. This method allowed definite training control, at the same time significantly reducing the number of enrollment samples required to achieve a good performance. Experiments showed 90% correct classification rate on a database of over 3000 signature images.

Sansone and Vento (2000) used the technique proposed by Huang and Yan (1997) to obtain the coded feature vector from a signature in their signature verification system. The results of the system was comparable with the work of Huang and Yan with higher FAR and FRR but achieved lower performance results.
Kaewkongka et al. (1999) used the Hough transform to extract the parameterized Houghspace from a signature skeleton as a unique characteristic feature of a signature. A back propagation neural network was used to evaluate the performance of the method. The system was tested with 70 signatures from different writers and a recognition rate of 95.24% was achieved.

Baltzakis and Papamarkos (2001) developed a two-stage neural network, in which the first stage gets the decisions from neural networks and Euclidean distance classifiers supplied by the global and grid and texture features and the second combines the four decisions using the boosting algorithm. The system used global features, grid features and texture features to represent each signature. A database was used which contained the signatures of 115 writers, with between 15 and 20 genuine signatures per writer. An average FRR and FAR of 3% and 9.8% respectively was obtained.

Liang et al. (2003) proposed multiple classifiers integration using the Boosting algorithm as given by Balzakis and Papamarkos (2001) along with a multi-stage neural network, to detect both random and simple forgeries. The experimental results showed that the integrated classifier can reach a better performance than individual classifier and the performance is insensitive to the order of the base classifiers. Moreover, the user adaptive thresholds free the system from manual parameter tuning.
The use of Hidden Markov Models (HMMs) is becoming more and more popular in both offline and online signature verifications and recognition. HMMs are finite stochastic automata and represent the most powerful tool for modeling time-varying dynamic patterns. Applications of HMMs in signature verification and recognition can be found in Rigoll et al. (1996), Kosmala et al. (1997) and Yang (1995) demonstrating the rising popularity of this technology in signature and document analysis. Hidden Markov Model have, in the last decade, attracted the attention of many researchers in the pattern recognition area, for example, the recognition of handwritten text (El Yacoubi et al., 1999), speech recognition (Rabaner and Juang, 1993) and recently the verification of on-line and offline signatures (Rigoll and Kosmala, 1998). This suggests the idea of using an HMM for training the characteristic signature cues of an individual and to use this HMM for the verification of a given signature by computing and evaluating the probability that this signature has been generated by the corresponding HMM. The following section describes the details of various verification and recognition algorithms using HMM and their results.

Justino et al. (2001) used a discrete observation HMM to detect random, casual and skilled forgeries. A grid segmentation scheme was used to extract the features of signatures. A cross validation procedure was used to dynamically define the optimal number of states for each model (writer). An FRR of 2.83% for
genuine and an FAR of 1.44%, 2.5% and 22.67% were reported for random, casual and skilled forgeries, respectively.

Coetzer et al. (2004) used Discrete Radon Transform (DRT) and Hidden Markov Model described above to develop a system that automatically authenticates offline handwritten signatures. Given the robustness of the algorithm and the fact that only global features were considered, satisfactory results were obtained. Using a database of 924 signatures from 22 writers, the system achieved an equal error rate (EER) of 18% when only high-quality forgeries (skilled forgeries) were considered and an EER of 4.5% in the case of only casual forgeries. These signatures were originally captured offline. Further using another database of 4800 signatures from 51 writers, the system achieves an EER of 12.2% when only skilled forgeries were considered. These signatures were originally captured online and then digitally converted into static signature images.

The usage of HMMs and cross validation principle for detecting random forgery was probed by El-Yacoubi et al. (2000). The system aimed to detect only random forgeries. Two experiments were conducted on two independent data sets, where each data set contained the signatures of 40 and 60 writers respectively. Both experiments used 20 genuine signatures for training and 10 for validation. The experimental results were calculated using an optimal acceptance / rejection decision threshold. The system produced an AERs of 0.46% and 0.91% respectively for each data set.
Shafiei and Rabiee (2003) proposed a new on-line handwritten signature verification system using Hidden Markov Model (HMM) which segmented each signature based on its perceptually important points and then computed for each segment a number of features that are scale and displacement invariant. The resulted sequence was then used for training an HMM to achieve signature verification. The system gave satisfactory results of 4% False Acceptance Rate (FAR) and 12% False Rejection Rate (FRR).

In a similar fashion, Justino et al. (2002) used a novel approach based on Hidden Markov Model (HMM) classifier to observe the influence of interpersonal and intrapersonal variability influences in offline signature verification. The experimental results showed the error rates variability in different forgery types, random, simples and skilled forgeries. The mathematical approach and the resulting software also reported considerations in a real application problem.

Rigoll and Kosmala (1998) used Hidden Markov Model for offline signature verification on a database of 14 authors, in which smaller training data and forgeries were used. In this work, the signature was obtained online and then transformed offline. This gave the advantage of no binarization or noise problem. The system was able to produce an error rate of 1.9%. The error rate increased when the signatures were obtained directly using offline methods.
A radically different method of signature analysis based on Fusion of two machine experts was described by Fierrez-Aguilar et al. (2004). Of the two machine experts, one was based on global image analysis and a statistical distance measure while the other was based on global image analysis and Hidden Markov Models. Experimental results were given on a subcorpus of the large signature database for random and skilled forgeries. It was shown that the machine expert based on local information outperforms the system based on global analysis in all reported cases. The two proposed systems were also shown to give complementary recognition information, which was exploited with a simple fusion strategy based on the sum rule.

2.4 WAVELET TRANFORMATIONS

Wavelets are mathematical functions that cut up data into different frequency components and then study each component with a resolution matched to its scale (Meyer, 1993). Wavelets were developed independently in the fields of mathematics, quantum physics, electrical engineering and seismic geology (Meyer, 1993; Masters, 1994). Exchange of ideas between these fields during the last ten years has led to many new wavelet applications, such as image compression (Vetterli and Herley, 1992), turbulence, human vision (Mallat, 1996; Schroder, 1996).
The hybrid opto-electronic method for the fast automatic verification of handwritten signatures is described by Fasquel and Bruynooghe (2004). This method, combined several statistical classifiers and consisted of three steps. The first step aimed to transform the original signatures using the identity and four gabor wavelet. For each image transform, the second step inter-correlated the analyzed signature with the similarity-transformed signatures of the learning database. Finally the third step performed the verification of the authenticity of signatures by fusing the decisions related to each transform. Image transforms and inter correlation were computed in a real time using a high-speed optical correlator. The different decisions and their fusion were then digitally performed. The opto electronic implementation method was simulated on a large database, taking into account the specific constraints of the optical implementation. Satisfactory results were obtained allowing a rejection of 62.4% of the forgeries and 99% of genuine signatures were correctly recognized.

The work of Fadhel and Bhattacharyya (1999) is another approach to signature verification system based on a steerable wavelet transform technique. In this method, the signatures were treated as a two dimensional image and used the wavelet as a tool of data reduction and feature selection. Feed forward neural network was used for both training and classification. The small length of the wavelet, coefficients vector, which was used as a feature vector reduced the complexity of the neural network in terms of the number of neurons and time of
training result based on the 300 signatures from 30 persons, which showed that wavelet had great potential for offline signature verification.

As per Deng et al. (1999), a wavelet based offline handwritten signature verification system can automatically identify useful and common features which consistently exist within different signatures of the same person and based on these features, verify whether a signature is a forgery or not. The system started with a closed contour algorithm. The curvature data of traced closed contours were decomposed into multi-resolutional signals using wavelet transforms. The zero crossings corresponding to the curvature data were extracted as features for matching. Moreover, a statistical measurement was devised to decide systematically which closed contours and their associated frequency data of a writer were most stable and discriminating. Based on this data, the optimal threshold value which controls the accuracy of the feature extraction process was calculated. This method could be applied to both online and offline signature verification systems. Experimental results showed that the average success rates for English signatures and Chinese signatures are 92.57% and 93.68% respectively.

2.5 STROKE ANALYSIS

In any offline Signature Verification and Recognition system, stroke analysis plays an important role in identifying the genuine and forged signatures.
The various parts of an ordinary signature when carefully measured bear a certain proportion to each other, which is surprisingly uniform, says Osborn (1990) and Bradford and Bradford (1992). By careful analysis of the strokes in the signatures, the performance of any ASV system can be improved.

Ferrer et al. (2005) conducted a research of a set of geometric signature features for offline 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 points arithmetic and tested with Hidden Markov Models, support vector machines and Euclidean distance classifier. The experiments showed promising results in the task of discriminating random forgeries.

The problem faced in offline signature verification using a pattern matching is that variation of signature stroke widths and a registered signature selected from a set of reference samples affect the verification performance. To solve this problem Ueda (2003) proposed a modified pattern matching method for the offline Japanese signature verification, which is independent of stroke widths and an appropriate selection method of a registered signature. The performance of the verification methods was evaluated using the error rate at which FRR and FAR are equal. The average error rates yielded 9.1% by the pattern matching method, 14.8% by the modified pattern matching method and 19.2% by the conventional pattern matching method. Comparing these results, the modified pattern matching
method with stroke width normalization and the optimal selection of a registered signature were able to reduce the average error rate of about 10.1% and 5.7% respectively.

According to Fang (2002), there are inevitable variables in the signature patterns written by the same person. The variations can occur in the shape or in the relative positions of the characteristic features. Set of training signature samples were arrived by two approaches. One approach measures the positional variations of the one-dimension projection profiles of the signature patterns, while the other determines the statistical variations in relative stroke positions of the two dimensional signature patterns. Given a signature to be verified, the positional displacements were determined and the authenticity was decided based on the static’s of the training samples. A matrix estimation technique was also used to obtain a better estimation of the co-variance matrix for dissimilarity computation. Results showed that the system compared favorably with other methods.

Perez-Hernandez (2004) made a simple adaptive offline signature recognition method based on the feature analysis of extracted significant strokes for a given signature. The system correctly decided on the majority of tested patterns which include both simple and skilled forgeries. This approach was used as a front-end recognition filter which decided on the most easy-to-analyze signature patterns and would filter the most difficult ones to a more sophisticate automatic recognition system. The implemented system provided a good trade off.
between short response time and reasonable correct recognition results. Robustness on moderate captures noise and invariance to geometrical transformations was also achieved.

2.6 DYNAMIC PROGRAMMING MATCHING (DPM)

Different methods have been proposed to provide a measure of the similarity between two signatures. Among the different algorithms used to compare signatures, DPM is a technique that finds the correspondence between sample points of two signatures, using some predefined metric. Given this correspondence, it is possible to calculate a "distance" between the signatures. The use of DPM for comparison was initially proposed in the field of speech recognition by Sakoe and Chiba (1978) and is described in detail by Rabaner and Juang (1993) with the name of Dynamic Time Warping (DTW). DPM has been successfully used for signature verification by many researchers (FairHust, 1997; Hastie et al., 1991; Munich and Perona, 1999; Munich and Perona, 2001; Nalwa, 1997; Parizeau and Plamondon, 1990; Wirtz, 1995). DPM can be used to match position, velocity, speed, acceleration, pressure derived from the signatures.

Sato and Kogure (1982) proposed to use DPM in order to align the shape of signatures consisting only of pen-down strokes, after having normalized the data with respect to translation, rotation, trend and scale. They further used the result of DPM to compute the alignment of the pressure function and to calculate a measure
of the difference in writing motion. They perform the classification based on three measures: the residual distance between shapes after time alignment, the residual distance between pressure functions and the distance between writing motions.

Parizeau and Plamondon (1990) evaluated the use of DPM for signature verification by aligning either horizontal or vertical position, horizontal or vertical acceleration. In this work, complete signing trajectories were used which consisted on both pen down and pen up strokes and were able to produce satisfactory results.

Hastie et al. (1991) obtained a statistical model of signatures that allows for variations in the speed of writing as well as affine transformation. DPM was used to find the correspondence between speed signals of pairs of signatures. The distance measure provided by DPM was used as the classification parameter. During training, the signature with the lowest distance to all others was chosen as the reference and its speed signal was used to perform letter segmentation. All other signatures were also segmented into letters by using the correspondence provided by DPM. Letter templates were extracted from the segmented signatures and were used for comparison and classification during testing. In this work, again the use of DPM reported satisfactory results.

Huang and Yan (1995) presented the use of DPM for matching signature strokes by finding a warp path that minimizes the cost of aligning the shape, the
velocities and the accelerations of the individual strokes. Pen-up strokes are merged with pen-down strokes in the preprocessing phase of their algorithm.

Nalwa (1997) parameterized the pen-down strokes of the signature using arc length instead of time, a number of characteristic functions such as coordinates of the center of mass, torque and moments of inertia were computed using a sliding computational window and moving coordinate frame. A simultaneous DPM over arc length of all these characteristic functions for the two signatures under comparison provided a measure of similarity to be used for classification. The experimental results showed acceptable results while comparing genuine with specimen signatures.

A novel stroke-based algorithm for Dynamic signature verification (DSV) was proposed by Qu et al. (2004) which used the behavioral biometrics of a handwritten signature to confirm the identity of a computer user. The algorithm converted the sample signatures to a template by considering their spatial and time domain characteristics and by extracting features in terms of individual strokes. Individual strokes were identified by finding the points where there is a decrease in pen tip pressure, decrease in pen velocity and rapid change in pen angle. A significant stroke is discriminated by the maximum correlation with respect to the reference signatures. Between each pair of signatures, the local correlation comparisons were computed between portions of pressure and velocity signals using segment alignment by elastic matching, Experimental results were obtained
for signatures from 10 volunteers. The result shows that stroke based features contain robust dynamic information and offer greater accuracy for dynamic signature verification, in comparison to results without using stroke features.

2.7 FUZZY CONCEPTS

The application of fuzzy concepts in the field of signature verification and recognition is effective since much of the uncertainty in decision making is derived from the fuzziness of the problem and the similarity between genuine and forged samples. Instead of having a threshold that separates forged and genuine samples, the use of fuzzy feature definition rather than sharp thresholds can improve the performance. The use of fuzzy concepts was proposed by many researchers (Liu et al., 1994; Schwartz, 1992; Pal and Majumder, 1986; Franke et al., 2002; George and Yuan, 1997; Madasu et al., 2000).

Ismail and Gad (2000) investigated the use of fuzzy concepts in the offline signature verification system and found out that the fuzzy usage increased the recognition rate to 95% and verification rate to 98%. They also demonstrated the efficiency and robustness of the system when compared with other techniques of signature recognition and verification system.

Madasu et al. (2003) made an innovative approach for extracting signatures from bank cheque images and other documents, which was based on the integration of the crop method with the sliding window technique. The
approximate area in which the signature lies was estimated using the sliding window technique. In this approach, a window of adaptable height and width was moved over the image; one pixel within the window was calculated. This density was then used to find the entropy, which in turn helped to fit the box that can segment the signature. The signature thus extracted was fed to a known fuzzy based offline signature verification and forgery detection system. This method produced almost 100% success in several bank cheques in India, Malaysia and Australia.

Madasu et al. (2000) made verification of offline handwritten signatures and detection of simple forgeries through neural network based approach and fuzzy modeling techniques. The angle distribution within the signature box constituted the features needed for the modeling of the signatures. The angle made by signature pixels was computed with respect to a reference point which was taken on the left hand corner of the box. This angle distribution was then clustered using the fuzzy C-means algorithm. Considering the clusters so obtained over the several samples as fuzzy sets, a Takagi-Sugeno model was constructed for the twin purpose of verification and forgery detection. The same features were also fed to the Back Propagation Neural Network (BPNN). The results for the both approaches were demonstrated on sample signatures of four persons.

As per Sabourin (1998), the recent advances in offline signature verification research and related work pertain to structural interpretation of signature images,
directional PDF used as a global shape factor, the extended shadow code (ESC) and the fuzzy ESC, a cognitive approach based on the fuzzy ARTMAP and shape factors related to visual perception. Experimental results could be compared only if the same experimental protocol and database were used for the evaluation of different verification schemes.

Quek and Zhou (2002) investigated the feasibility of using a pseudo-outer product based fuzzy neural network for skilled forgery detection. They used global baseline features, pressure features and slant features to conduct two types of experiments. The first group of experiments used genuine signatures and forgeries as training data, while the second group of experiments used only genuine signatures as training data. These experiments were conducted on the signatures of 15 different writers, that is, 5 writers from 3 different ethnic groups. When genuine signatures and forgeries were used as training data, the average of the individual EERs is 22.4%. Comparable results were obtained when using only genuine signatures as training data.

2.8 ELASTIC MATCHING

Fang and Tang (2004) described two methods to tackle the sparse data problem in off line signature verification. The first one artificially generated additional training samples from the existing training set using an elastic matching technique. Feature statistics were estimated by using the expanded training set.
The second type applied regularization technique to the sample co-variance matrix to overcome the problem of inverting an ill conditioned covariance matrix and obtained stabilized feature statistics. Both techniques produced significantly improved verification accuracy when implemented with a set of peripheral features.

You et al. (2005) desired to employ straightforward means to measure similarity between 2-D static signature graphs. Two signature patterns were globally registered using weak affined transformations and correspondences of feature points between two signature patterns were determined by applying an elastic local alignment algorithm. Similarity was measured as the mean square of sum Euclidean distances of all found corresponding feature points based on a match list. The similarity measurement computed was able to provide sufficient discriminatory information and verification performance in terms of equal error rate was 18.6% with four training samples.

Fang et al. (2001) developed a system that is based on the assumption that the cursive segments of forged signatures were generally less smooth than that of genuine ones. Two approaches were proposed to extract the smoothness feature: a crossing method and a fractional dimension method. The smoothness feature was then combined with global shape features. Verification was based on a minimum distance classifier. An iterative leave-one-out method was used for training and for testing genuine test signatures. A database with 55 writers was used with 24
training signatures and 24 skilled forgeries per writer. An AER of 17.3% was obtained.

Fang et al. (2002) also developed a system that uses an elastic matching method to generate additional samples. A set of peripheral features, which is useful in describing both the internal and external structures of signatures, is employed to represent a signature in the verification process. Verification is based on a Mahalanobis distance classifier. An iterative leave-one-out method is used for training and for testing genuine test signatures. The same database that used in Fang's previous work (Fang et al., 2001) is again used here. The additional samples generated by this method reduced the AER from 15.6% to 11.4%.

2.9 SEGMENTATION METHODS

In any signature verification and recognition system, one of the first steps a forger has to do is to look into a signature to extract its perceptually important points. Consequently, a segmenting algorithm must be able to find accurately the apex of each peak present along the handwritten curve. However, according to Fishler and Bolles (1986), different goals for the segmenting of a continuous curve could result in different segmentation points, even if the curve is very simple. Several interesting techniques that segment signatures in various ways have already been proposed in the literature in the fields of Automatic Signature Verification (ASV) (Brault and Plamondon, 1989; Fishler and Bolles 1986;
Freeman and Davis (1977); Kruse and Rao (1978); Pavlidis and Horowitz (1974); Plamondon, 1992).

The split and merge algorithm proposed by Pavlidis and Horowitz (1974) is based on an iterative approximation of a curve by straight segments that drive an error norm under a specified threshold. This method is suitable for the approximation of a curve by a polygonal line but has a tendency to result in too many segmentation points; moreover, they are not always well centered on the apex of the peaks.

The technique proposed by Kruse and Rao (1978) is based on calculating a sliding correlation between a mathematical model of a corner or vertex and portions of the curve joining ‘s’ points. The apex of the corner must correspond to the local maxima of the correlation function. The main shortcomings of the method are the too restrictive definition of the corner model and the arbitrary fixed domain of every possible vertex. Consequently it would make it impossible to adequately quantify the importance of a vertex made up of much more than ‘s’ points.

Freeman and Davis (1977) proposed another type of segmentation technique, similar to the one above, that also involves a sliding analysis of portions of the curve joining ‘s’ points. In this case, however, the ‘s’ points are
used to locate the discontinuities along the curve. This method gave better results when compared with the above, but was not able to detect long and smooth corner.

The segmentation algorithm proposed by Brault and Plamondon (1993) is roughly similar to the methods proposed by Kruse and Rao [1978] and by Freeman and Davis [1977]. The major difference is that Brault and Plamondon (1993) considered that a corner could be made of any number of points and the algorithm itself must determine the length and specific domain of every potential vertex. The method had been applied especially to a signature database, and the location and relative importance of the segmentation points were generally in agreement with human perception. The method was well tested on a number of signatures that required different kinds of segmentation decisions.

In a work proposed by Plamondon (1992), general segmentation framework for the analysis of handwriting is based on a theory of rapid movements. According to this theory, handwriting is made of curvilinear and angular strokes that are partially superimposed due to some anticipation effects occurring in the generation of fast complex movements. Since the beginning and end of these strokes are partially hidden in the signal, it is shown that a consistent handwritten segmentation theory should take into account large units of handwritten signals because one of the most effective ways to extract these underlying strokes is to perform an analysis by synthesis experiment over a whole component.
Zhang et al. (2000) provided a solid basis for comparing function features of two handwritten signatures. Corner points of the signatures were first extracted based on velocity information. The characteristics of curvilinear velocity and angular velocity were combined successfully by functions based on membership criteria. The signatures to be compared were then segmented at landmarks obtained by corner matching based on similarity measures. In the last step, the corresponding pairs of segments were mapped by a point-to-point matching algorithm, minimizing curve deformation energy. The segmentation step significantly reduces the difficulty of signature comparisons. These techniques were applied to a set of 188 signatures from 19 volunteers. The resulting point-to-point matching of signature pairs was satisfactory in all cases where there was a visual agreement between the signatures.

2.10 OTHER RELATED TECHNIQUES

Various other techniques used in the field of signature verification and recognition systems are discussed in the following subsections.

2.10.1 Multi Expert System (MES)

The idea of using a MES has recently been investigated in the literature of signature verification. The rationale of the multi-expert approach lies in the assumption that, by combining the results of a set of experts according to a combing criteria, it is possible to compensate for the weakness of each single
expert while preserving its own strength (Suen et al., 1992). Experimental analysis on different areas has demonstrated that the performance of the MES can be better than that of any single expert, especially when using complementary experts (Rahman and Fairhurst, 1998; Kittler, 1999; Cordella et al., 1999).

Murshed et al. (1997) proposed a cognitive approach to offline signature verification in which a two-stage verification system was proposed. In this system, the input image was divided into areas of equal size and a set of features was extracted by evaluating in each area the occurrence of some graphical segments. Eventhough the system produced agreeable results, the work of Sansone and Vento (2000) proved that the fact that there is no final combination of the decisions made by the two stages and the thresholds used to decide upon the acceptance or rejection of a signature are a priori fixed, reduced the performance of the system.

A multi-expert system for dynamic signature verification was described by Lecce et al. (2003) in which a combined three expert complementor behaviour was achieved by using different features and verification strategies. The expert base of features and perform signature verification by a holistic analysis, the second and third expert used special features and performed signature verification by a regional analysis.
2.10.2. Data Fusion Method

Data fusion is a formal framework in which are expressed the means and tools for the alliance of data originating from different sources. It aims at obtaining information of greater quality; the exact definition of greater quality will depend upon the application (Wald, 1999). A number of authors have explained different data fusion methods such as Probability theory, possibility theory, Dempster-Shafer evidence theory, fuzzy logic, neural networks and voting/ranking methods (Bloch, 2000; Van and Schomaker, 2000; Lefevre, 2001; Loonis et al., 2001; Minot and Gentric, 2003; Oussalah et al., 2001; Xu et al., 1992).

Arif and Vincent (2003) described data fusion and its methods for an offline signature verification problem. Three data fusion methods such as Dempster-shafer evidence theory, possibility theory and Borda count method (a ranking/voting method) were employed for fusion of multiple distance classifiers at the final decisional step in an offline signature verification problem. The system developed used an efficient data fusion method by modifying any existing method which meets better to the specific needs of the problem. Among these three methods, experimental result obtained with Dempster-shafer theory was more reliable than others. Further, the results showed a total failure of Borda count method in this application.
2.10.3 Feature Selection

Feature selection is an integral part of verification process and its function, which extends beyond simply minimizing error rates were considered to provide a mechanism for defining a personally optimized verification framework, encompassing all aspects of performance. The process of heuristically assessing the features involves comparing the error rates generated by a localized verification procedure when presented with authentic and non-authentic signatures (Fairhurst et al., 1992).

The feature selection method suggested by Brittan and Fairhurst (1994) has addressed the problem of the implementation of algorithms for the support of a novel and efficient automatic system for handwritten signature verification. Two level of parallelism have been identified within the computationally intensive task of selecting features, first, within the evaluation of the criterion function and second, within the task of assessing and selecting the feature.

2.10.4 Biometric Verification

Biometrics is the general term to refer to the utilization of physiological characteristics (e.g. face, iris, fingerprint) or behavioral traits (e.g. signature, keystroke dynamics) for verifying the identity of an individual. Authentication actually refers to two separate problems: identification and verification. In identification, Biometric authentication is gaining increasing popularity as a more
trustable alternative to password or key based security systems. Signature is a behavioral biometric: it is not based on the physical properties, such as fingerprint or face, of the individual, but behavioral ones.

According to Fairhurst and Kaplani (2003), the handwritten signature is a common biometric which was regularly used, but with authentication decisions traditionally made by human visual inspection. Biometric based access control whether it is with respect to places, restricted information or personal data, has become an increasingly important consideration in many situations. Some important issues relating to signature complexity and authentication decisions point to the increasing need for an understanding of both human and machine based perceptual mechanisms as biometric processing were investigated. The human computer interface developed for future generations of automated biometric systems can benefit significantly from a detailed study of the processes by which human biometric checking are carried out, and the important issues underlying this aspect of signature verification performance were analyzed.

A recent trail of a biometric identity verification system was described by Grifford and Edwards (2005). The prototype system developed provided a means of automatically issuing pass cards providing access to a major site. The description about the access control to a major industrial site, and the potential benefits of a biometric system was discussed. The description of a prototype
access control system, and a review of dynamic signature verification as a biometric technique were tested with good results.

Munich et al. (2003) proposed new camera-based biometric visual signature identification. The importance of the parameterization of the signature in order to achieve good classification results, independently of variations in the position of the camera with respect to the writing surface was discussed. The offline arc-length parameterization performed better than conventional time and Euclidean arc-length ones. The system verification on performance was better than 4 per cent error on skilled forgeries and 1 percent error on random forgeries, and its recognition performance was better than 1 percent error rate, comparable to the best camera-based biometrics. Offline systems deal with a static image of the signature. A signature verification or recognition system has to be designed to meet a set of requirements in terms of performance, training set size, and robustness conditions (Fairhurst, 1997; Plamondon and Lorette, 1989).

2.10.5 Hybrid Technology

Zimmer and Ling (2004) suggested a new hybrid signature verification system where the online reference data acquired through a digitizing tablet serves as the basis for the segmentation process of the corresponding scanned offline data. Local foci of attention over the image were determined through a self-adjustable learning process in order to pin-point the feature extraction process.
Both local and global primitives were processed and the decision about the authenticity of the specimen was defined through similarity measurements. The global performance of the system was measured using two different classifiers. Off-line systems have poorer performance and usually require a large database space. Instead of a well-known offline grid-like segmentation (Sabourin and Genest, 1994), a window focused segmentation process was suggested. Results indicated that equal error rates of about 5% for 5 reference signatures and about 1% for 10 reference signatures could be achieved by the use of common Euclidean Distance measurements.

2.10.6 Minimum Distance Classifiers

Mizukami et al. (2002) proposed an offline signature verification system based on a displacement extraction method. The optimum displacement functions were extracted for any pair of signatures using minimization of a functional. This functional can be defined as the sum of a squared Euclidean distance between two signatures and a penalty term requiring smoothness of the displacement function. A coarse-to-fine search method was applied to prevent the calculation from storing at local minima. Based on the obtained displacement function, the dissimilarity between a questionable signature and the corresponding authentic one was measured. The proposed system achieved error rate of 24.9% in an experiment.
Sabourin et al. (1997) used granulometric size distributions for the definition of local shape descriptors in an attempt to characterize the amount of signal activity exciting each retina on the focus of a superimposed grid. He then used a nearest neighbour and threshold-based classifier to detect random forgeries. A total error rate of 0.02% and 1.0% was reported for the respective classifiers. A database of 800 genuine signatures from 20 writers was used.

2.11 CONCLUSION

Offline signature verification is a much more different problem, since many desirable author sensitive characteristics are not available readily. The process of identifying, verifying and recognition has attracted a lot of researchers owing to the fact that it is widely used in many security related areas. But considering the fact that there exists difficulties in identifying the genuine and forged signatures, the need for research in efficient automatic solutions for ASV has increased. The current market scenario needs an ASV system which is efficient, has high speed and use less memory and most importantly identifies all types of forgeries. Keeping this in mind the new system has been formulated and the methodology pertaining to the same is discussed in Chapter III.