# Offline Signature Verification

A Dissertation Submitted in the Partial Fulfilment for the Award of

MASTER OF TECHNOLOGY
IN
SOFTWARE ENGINEERING

Submitted To
Mrs. Abhilasha Sharma
Asst.Professor
Delhi Technological University

Submitted By
Ankit Sachan
2K12/SWE/06

Department of Computer Engineering
Delhi Technological University
New Delhi
2013-2014

# CERTIFICATE

DELHI TECHNOLOGICAL UNIVERSITY
(Govt. of National Capital Territory of Delhi)
BAWANA ROAD, DELHI-110042
Date: ____________________

This is to certify that the thesis entitled ***Offline Signature Verification*** submitted by *Ankit Sachan (Roll Number: 2K12/SWE/06*), in partial fulfilment of the requirements for the award of degree of Master of Technology in Software Engineering, is a work carried out by him under my guidance.

Mrs. Abhilasha Sharma
Assistant Professor
Department of Computer Engineering
Delhi Technological University
Delhi

# ACKNOWLEDGEMENT

I take this opportunity to express my deepest gratitude and appreciation to all those who have helped me directly or indirectly towards the successful completion of this thesis.

Foremost, I would like to express my sincere gratitude to my guide ***Mrs. Abhilasha Sharma***, *Assistant Professor, Department of Computer Engineering, Delhi Technological University, Delhi* whose benevolent guidance, constant support, encouragement and valuable suggestions throughout the course of my work helped me successfully complete this thesis. Without her continuous support and interest, this thesis would not have been the same as presented here.

Besides my guide, I would like to thank the entire teaching and non-teaching staff in the Department of Computer Engineering, DTU for all their help during my course of work.

# ABSTRACT

*Biometrics has provided various techniques to recognize a person based on physical attributes. Biometric technologies are becoming foundation for highly secure identification solutions.The need for biometrics can be found in many local and government departments, military operations etc.Features measured can be any or combination of face, retina, handwriting, iris, signature and tone of voice.*

*Signatures are extensively used for the purpose of providing authenticity for a person.In various commercial applications like transactions,bank cheques; it is unrealistic to check manually all the person's signature in limited amount of time.So there is highly need for automated signature verification and identification techniques.Handwritten signature are different from other textuals, people used to draw a shape as their signature which is in static form.So we can infer lot of important information from these shapes and can use them for identification and verification purpose.*

*Signature can be done in two modes, when a signature is made on paper with a pen it is called an offline mode.If one does a sign on a tablet in real time it is called an online mode.In online mode of signatures some more information which is dynamic in nature can be inferred which is not possible to obtain in offline mode.Such dynamic information is pressure, time taken to put sign,pen angle etc. The present research work is done in the field of offline signature verification system by extracting some special features that make a signature difficult to forge. In this research work, existing signature verification systems have been thoroughly studied and a model is designed to develop an offline signature verification system.*

# List of Figure(s)

# List of Table(s)

# TABLE OF CONTENT

# CHAPTER 1

## AN OVERVIEW

## 1.1 INTRODUCTION

Signature is a socially accepted authentication method and is widely used as proof of identity in our daily life. Automatic signature verification by computers has received extensive research interests in the field of pattern recognition. Depending on the format of input information, automatic signature verification can be classified into two categories: online signature verification and offline signature verification. In the former case, a hand pad together with an instructed pen or a video camera is used to obtain the online information of pen tip (position, speed, and pressure). Therefore the input is a sequence of features. In the latter case, the input is a two-dimensional signature image captured by a scanner or other imaging device [1].

Signature verification is an important area in the field of person endorsement. The detection of human script is important concerning about the progress of the interface between human-beings and computers. If the computer is sharp enough to be aware of human handwriting it will provide a more eye-catching and economic mancomputer interface. In this area signature is a special case that provides secure means for authentication, attestation consent in many high security environment. The goal of the signature verification system is to differentiate between two classes: the original and the forgery, which are related to intra and interpersonal variability. The disparity among signatures of same person is called Intra Personal Variation. The variation between originals and forgeries is called Inter Personal Variation.

## 1.2 Type of Forgeries

There are three different types of forgeries categorization:

### 1.2.1 Random Forgery

The signer uses the name of the victim in his own style to create a forgery known as simple or random forgery. It is done by a person who doesn’t know the shape and structure of the original signature. This type of forgery is very easy to detect.

### 1.2.2 Casual Forgery

The casual forgery is done by a person who has a vague idea of the actual signature, but is signing without much practice.

### 1.2.3 Skilled Forgery

The last type is the skilled forgery, done by an expert person who has good knowledge about the original signature and is signing with proper practice. Naturally it is more difficult to detect skilled forgeries than other forgeries.

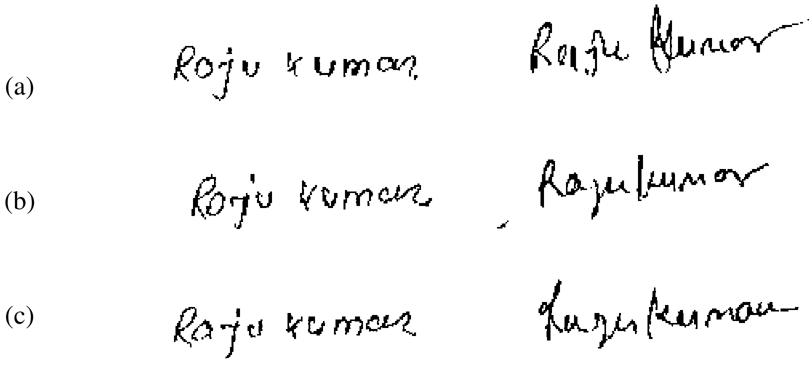


Figure 1.1 Type of Forgeries (a) Genuine and Corresponding Random Forgery (b) Genuine and Corresponding Skilled Forgery (c) Genuine and Corresponding Casual Forgery

## 1.3 Motivation of Work

There are several challenges in field of security. Using signature verification techniques in optimized way can reduce the security threats and risks. Doing authorization and identification manually is a big problem when data collection is huge. So by providing a new automatic verification model will be a next step. On line signature verification is more reliable than Offline signature verification. Accuracy % obtained in Online signature verification is close to 99% while for offline signature verification is much low comparatively.In real time use of online signature verification is still low as compare to offline signature verification as we can see in banking systems.Hence development of a new verification model with a reasonable high accuracy would be useful, which is the main motivation of this research work.

## 1.4 Goals of Thesis

Primary goal of this research work is to study the various techniques of Offline Signature Verification System, survey all these techniques and propose a new model for verification which can give optimized results.The goals of this thesis are:

- To survey the maximum verification methodologies which are being used by many researchers for verification.
- To propose a new model using wavelet features and support vector machine.
- Apply methodoloy proposed model on self created data set and validate it.

## 1.5 Contributions and Guided Tour of the Thesis

The remainder of the thesis is structured as follows:

*Chapter 2* gives brief idea about biometric systems, signature verification mode i.e.online and offline, general signature verification systems, classification systems.

*Chapter 3* describes charecteristics of forgeries, study of existing approaches for offline signature verification systems, study of verification techniques. It also highlights some of the most relevant works in the direction of field of work presented in the thesis.

*Chapter 4* describes implementation of proposed method which is combination of feature extraction using wavelet features and classification through Support Vector Machine.

*Chapter 5* gives complete analysis of result and comparison among other existing techniques.

The final section concludes the thesis with a summary of the results, and a discussion on possible future directions along with the references used.

# CHAPTER 2

## LITERARURE REVIEW

# LITERARTURE REVIEW

Biometric technologies can be implemented by obtaining two kinds of features physiological and behavioural.Physiological features are finger prints, iris, handwriting, facial recognitions. Behavioural features are voice and handwritten signatures.

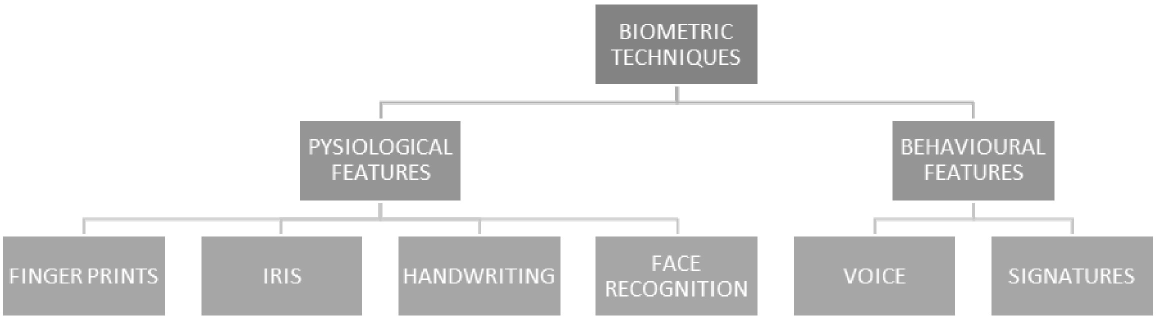


Figure 2.1 Hierarchies of Biometrics Techniques

Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Jain et al. [6] identified seven such factors to be used when assessing the suitability of any trait for use in biometric validation. Universality means that every person using a system should have power over the characteristic. Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another. Permanence relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm. Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets. Performance relates to the accuracy, speed, and robustness of technology used. Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed. Circumvention relates to the ease with which a trait might be imitated using an artifact [26].

Adaptive biometric systems aim to auto-update the templates or model to the intra-class variation of the operational data. The two-fold advantages of these systems are solving the problem of limited training data and tracking the temporal variations of the input data through adaptation. Recently, adaptive biometrics has received a significant attention from the research community. This research direction is expected to gain momentum because of their key promulgated advantages. First, with an adaptive biometric system, one no longer needs to collect a large number of biometric samples during the enrollment process. Second, it is no longer necessary to re-enroll or retrain the system from scratch in order to cope with the changing environment [27]. This convenience can significantly reduce the cost of maintaining a biometric system. Despite these advantages, there are several open issues involved with these systems. For mis-classification error (false acceptance) by the biometric system, cause adaptation using impostor sample. However, continuous research efforts are directed to resolve the open issues associated to the field of adaptive biometrics.

- Biometrics has been used effectively for more than a decade for time and attendance and workforce management. Despite widespread use, confusion and misconceptions about the technology and its capabilities persist. These concerns are easily dispelled when the facts about biometrics are established.
- Biometrics offers unparalleled ability to quickly and accurately capture real-time, labor data and provide a nonrepudiated audit trail.
- Biometrics has undergone intense scrutiny and the results are in - when properly deployed, biometrics work well and are safe, secure, and accurate.
- Biometrics offers organizations a broader range of direct and indirect time, cost, and perational benefits than alternative time and attendance methods.

Today over one hundred thousand thriving organizations rely on Easy Clocking’s time & attendance systems to automate their employee attendance and as a result they are seeing a significant reduction in direct and indirect labour costs. The block diagram illustrates the two basic modes of a biometric system. First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person [20]. In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. Positive recognition is a common use of the verification mode, where the aim is to prevent multiple people from using same identity.

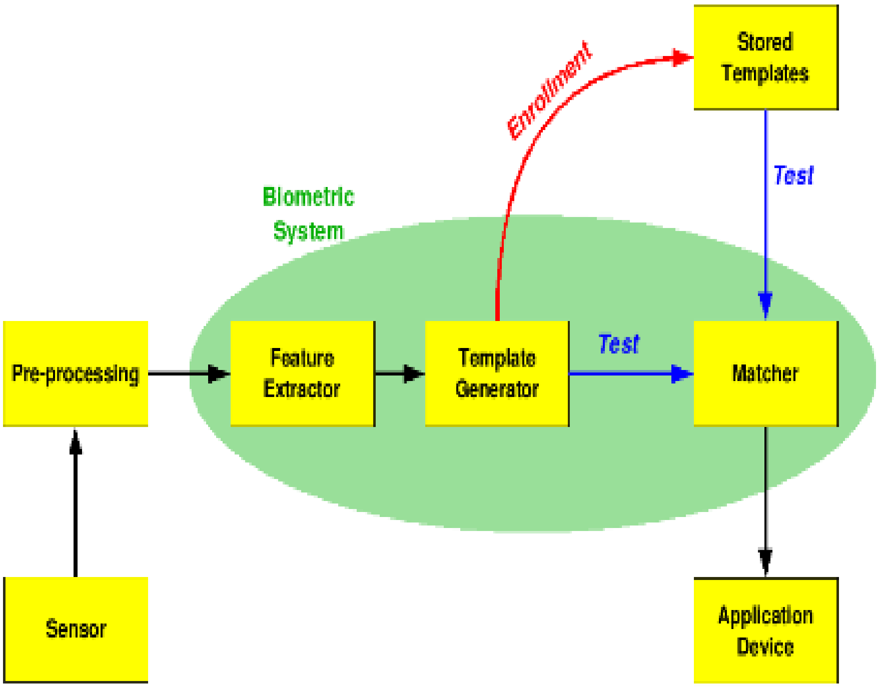


Figure 2.2 Block Diagram of Biometric Model [27]

The first time an individual uses a biometric system is called enrolment. During the enrolment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrolment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrolee. During the enrolment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area). Selection of biometrics in any practical application is depending upon the characteristic measurements and user requirements. We should consider Performance, Acceptability, Circumvention, Robustness, Population coverage, Size, Identity theft deterrence in selecting a particular biometric. Selection of biometric based on user requirement considers Sensor availability, Device availability, Computational time and reliability, Cost and power consumption.

There are growing concerns about the personal privacy implications and immutable issues whenever the biometric technology is discussed. Biometrics itself contains no personal information, it never reveals the real name or address like what identification card does, and thus it is more difficult to forge or steal. However, the real fear occurs when a biometric identifier and a person are linked together in a database. When the database is accessible by more people, basic privacy rights are eroded. Unlike names, addresses, or even physical appearances, which can changed or be altered over time, some biometrics are relatively stable and cannot be replaced once it is compromised. Therefore, the most serious privacy dilemma confronting biometric technology is not one of physical intrusiveness, but rather one of personal autonomy.

## 2.1 Signature Verification

Signatures Verifications are done either in online mode or offline mode.it depends upon what approach one wants to follow.If signatures are done online then online verification methodology is used. If signatures are done offline (on a paper) then offline verification techniques are deployed.When signatures are done on a stylus tablet in online mode then we can infer more dynamic features such as time taken by a person to do a single signature, how much pressure is applied while taking signatures, we can also infer inclination angles via horizontal or vertical axis.

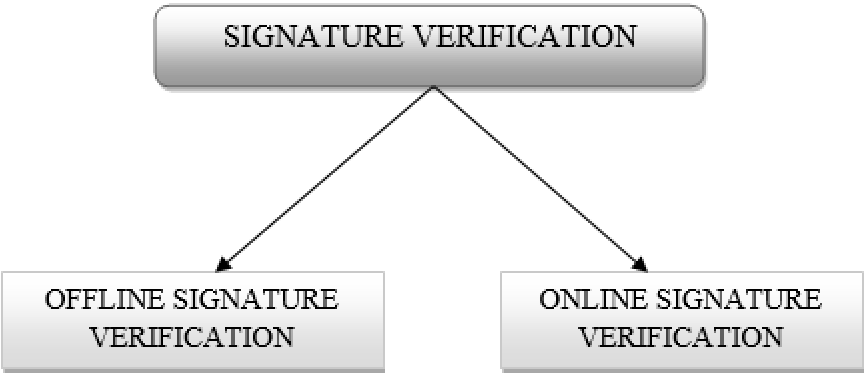
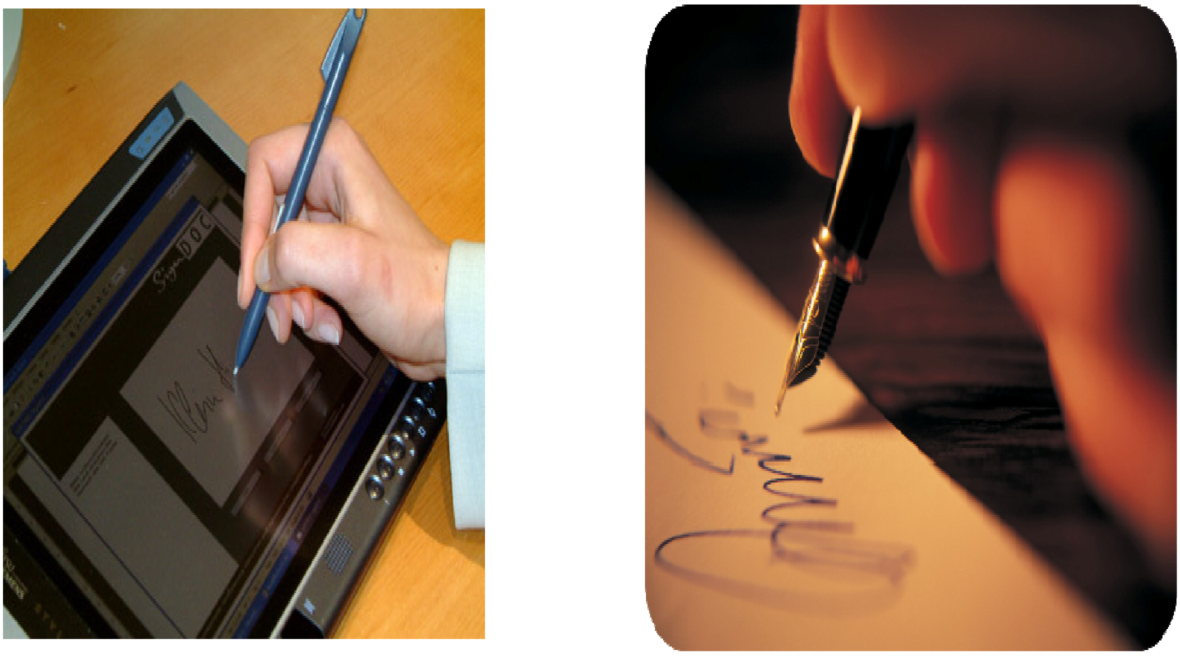


Figure 2.3 Mode of Signature Verification

When signatures are done manually on a paper with pen in static form, one can not collect dynamic information for a static image.Only static features can be collected from that image. Such static features are area, height, width, and height to width ratio, horizontal projection, vertical projection, centre of gravity and many more.

To report any robust system which is able to perform classification into forged and genuine signature class it is mandatory to collect maximum no of features so that results can be more optimized.



(a) Online Signature (b) Offline Signature

Figure 2.4 Mode of Offline Signature [28]

## 2.2 Steps Involved in Offline Signature Verification

Various steps are involved in offline signature verification system.Verification can be done phasewise.Steps can be named as Database Creation , Pre-processing, Feature Extraction, Feature Comparision and Classification etc.Output of the first step or task is the input for next step.

Database can be collected manually by collecting signatures by individual persons, before collection of signature samples from different writers following important issues should be considered:

- No of samples collected from different persons should cover a person's inter variability.
- More no of samples used for training and testing would give more optimal results.

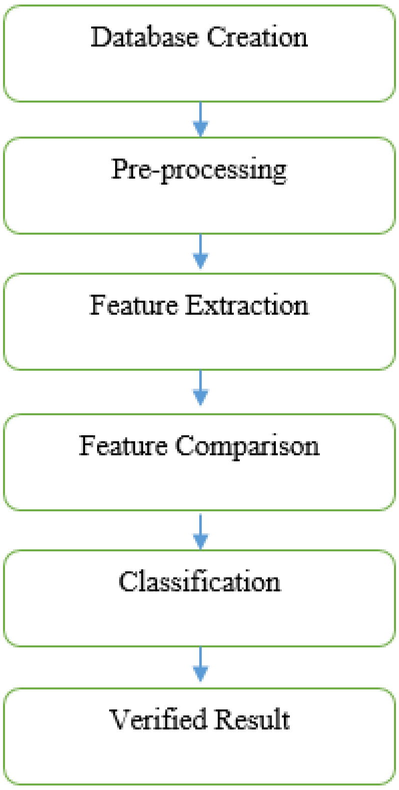


Figure 2.5 Block Diagram of Signature Verification System

## 2.2.1 Database Creation

Signature samples from different users are collected in such a way that personal variance should be covered.If a person signs twice one can see small changes in between two signature samples,so this personal variability should be covered while collecting samples it is recommended that collect maximum no of samples from one user itself.if sufficient samples are taken from individual users it will be helpful at the time of comparision or matching in between the features and error rates can be minimized.Some research oriented organizations are providing datasets and one can also create datasets manually.

## 2.2.2 Pre-processing

Preprocessing is very important aspect in verification.Once you collect signature samples, samples need to be normalized because every person has its own style to do signature and they can highly differ in size i.e.length, width.In preprocessing various steps are performed to remove noise.Some important steps are discussed as follows.

- **Scaning and Background Elimination**

Signature image is scanned through scanner and data area cropping must be done for extracting features.

- **Noise Reduction**

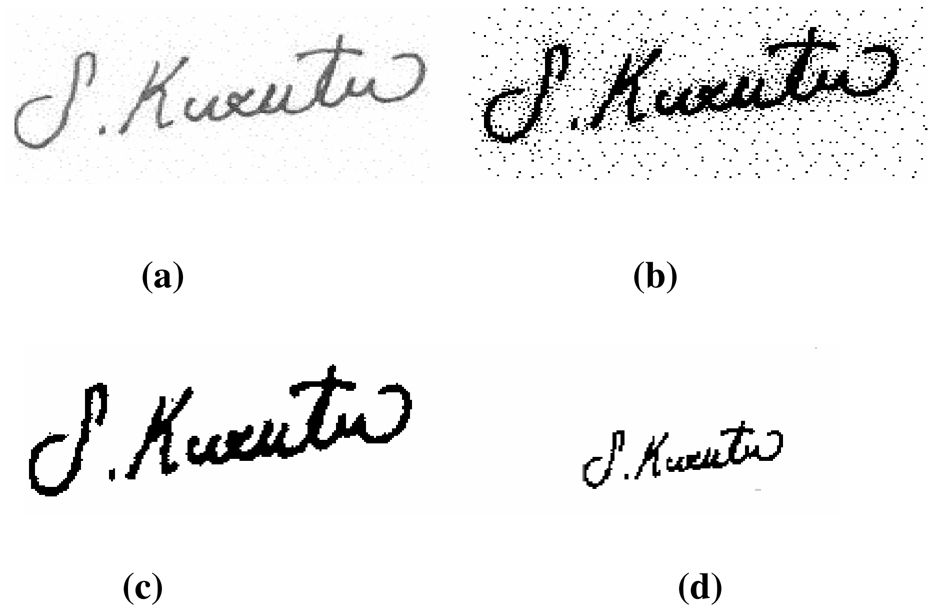
A noise reduction filter is applied to the binary image for eliminating single black pixels on white background. 8-neighbors of a chosen pixel are examined. If the number of black pixels is greater than number of white pixels, the chosen pixel will be black otherwise it will be white.

- **Width Normalization**

Signature dimensions may have intrapersonal and interpersonal differences. So the image width is adjusted to a default value and the height will change without any change on height-to-width ratio.

- **Thinning**

The goal of thinning is to eliminate the thickness differences of pen by making the image one pixel thick.



**(a)** **(b)**

**(c)** **(d)**

Figure 2.6 Pre-processing Steps (a) Scanned Image (b) Background Elimination (c) Noise Removal (d) Width Normalization [8]

## 2.3 Feature Extraction

Various important features are extracted from the signature samples.Many researchers have computed different features like global features, local features, and wavelet features.

### 2.3.1 Type of Features

There are various types of features and few are listed below.

#### a) Global Features

*Signature area* is the number of pixels which belong to the signature. This feature provides information about the signa-ture density.

*Signature height to width ratio* is obtained by dividing signature height to signature width. Signature height and width can change. Height-to-width ratios of one person's signatures are approximately equal.

*Maximum horizontal histogram and maximum vertical histogram* the horizontal histograms are calculated for each row and the row which has the highest value is taken as maximum horizontal histogram. The vertical histograms are calculated for each column and the column which has the highest value is taken as maximum vertical histogram.

*Local maxima numbers of the signature* the number of local maxima of the vertical and horizontal histogram is calculated.

*Edge point numbers of the signature* edge point is the pixel which has only one neighbour, which belongs to the signature [8].

#### b) Moments Feature

Moments are used for the purpose of image analysis.Images are rotataed in between $0^0$ to $360^0$ .Image feature are computed by normalizing central moments throughorder three, that are invariant to object scale, position, and orientation.

#### c) Grid Features

Image is divided in grids and pixel values either in horizontal or vertically or in both directions is computed and feature vectors are obtained. Grid segmentation is a technique that is used for signature detail analysis. A grid of 12 x 8 segments are depends on the pre-processed image and the features mentioned below are calculated for each of the segment.

- *Pixels Density*

  This pixel density gives the number of black pixels of each segment.

- *Pixels Distribution*

  It gives the pixel geometric distribution in a cell (intersection of row and column).

- *Predominant Axial Slant*

  It is a value representing the predominant inclination of each cell.

## Trisurface Feature

The surface area of two visually different signatures could be the same. For the purpose of increasing the accuracy of a feature describing the surface area of a signature, the 'triSurface' feature was investigated as an extension in which the signature was vertically separated into three equal parts. The surface area feature is the surface covered by the signature, including the holes contained in it. The total number of pixels in the surface was tallied, and the proportion of the signature's surface over the total surface of the image was calculated. This process was used for the three equal parts of the signature, giving three values between 0 and 1.

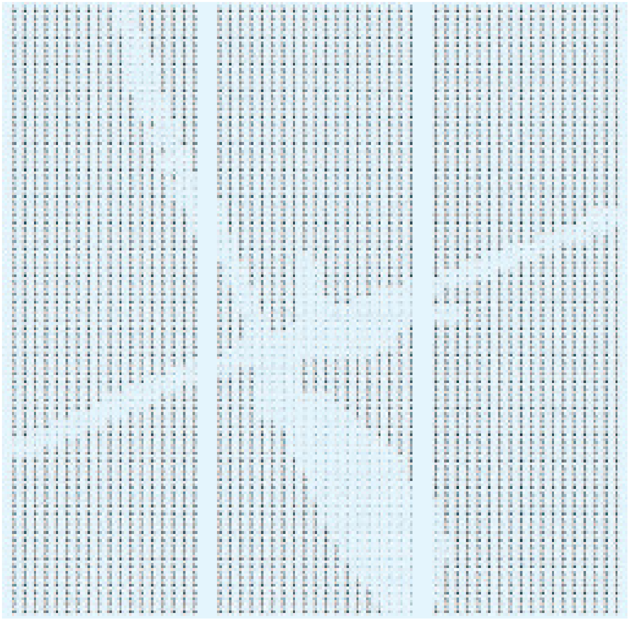


Figure 2.7 Trisurface Concept [17]

### d) Sixfold Surface Feature

This feature is different from the TriSurface feature mainly in two ways. Firstly, the number of feature values obtained is doubled to six with the Sixfold Surface. Secondly, centers of gravity are determined to assist in the calculation of the Sixfold Surface features.

The Signature image is first divided into three parts vertically. The center of gravity is calculated for each of the three parts, and the signature surface above and below the horizontal line of the center of gravity (giving two subsections for each part) was calculated. The result was a set of six feature values corresponding to the surface of the six sub-sections.

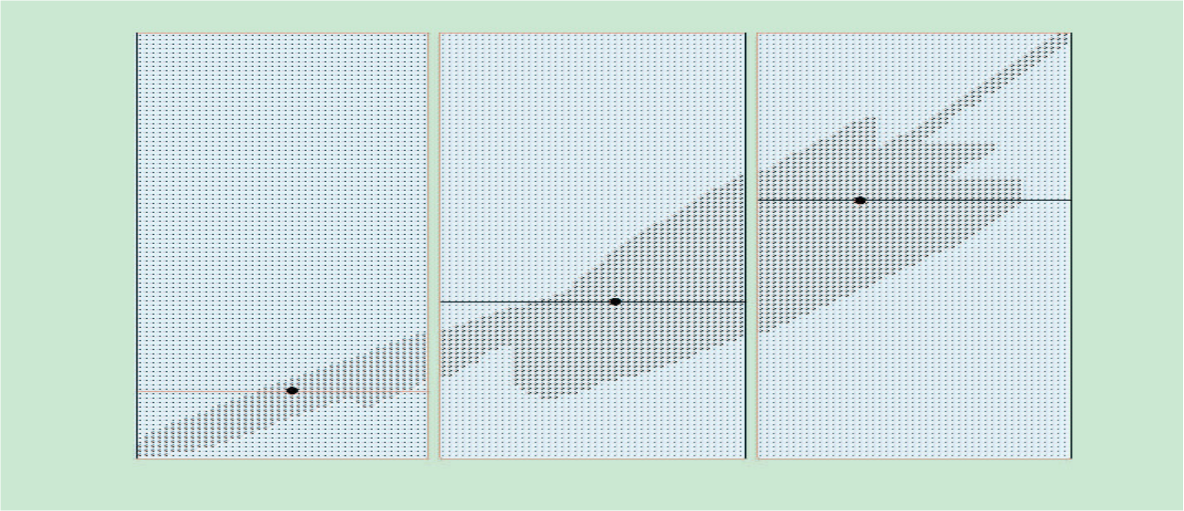


Figure 2.8 Six Fold Surface Features [17].

### e) Best-Fit Features

The line of best fit usually attempts to represent a scatter of points in an area. In order to obtain an approximation for the signature's skew; the line of best fit was calculated using minima and maxima from the bottom edge of the signature. Similarly the line of best fit from the top of the signature was also calculated. The angles between each of these lines and the X-axis were calculated, giving two features. The surface area enclosed between the two lines became the third feature.

### 2.3.2 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 [18].

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 [24].

On the other hand, even though the local features are dependent on the zoning process, still they are more suitable to identify skilled forgeries [14]. 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 [23].

The global features can deliver limited information for signature verification [25]. 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 [14].

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 [25].

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 [25]. 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.

## 2.4 Discrete Wavelet Transform

In recent years, the wavelet transform emerged in the field of image/signal processing as an alternative to the well-known Fourier Transform (FT) and its related transforms, namely, the

Discrete Cosine Transform (DCT) and the Discrete Sine Transform (DST). In the Fourier theory, a signal (an image is considered as a finite 2-D signal) is expressed as a sum, theoretically infinite, of sines and cosines, making the FT suitable for infinite and periodic signal analysis. For several years, the FT dominated the field of signal processing, however, if it succeeded well in providing the frequency information contained in the analysed signal; it failed to give any information about the occurrence time. This shortcoming, but not the only one, motivated the scientists to scrutinise the transform horizon for a "messiah" transform. The first step in this long research journey was to cut the signal of interest in several parts and then to analyse each part separately. The idea at a first glance seemed to be very promising since it allowed the extraction of time information and the localisation of different frequency components.

Formally, the wavelet transform is defined by many authors as a mathematical technique in which a particular signal is analysed (or synthesised) in the time domain by using different versions of a dilated (or contracted) and translated (or shifted) basis function called the wavelet prototype or the mother wavelet. However, in reality, the wavelet transform found its essence and emerged from different disciplines and was not, as stated by Mallat, totally new to mathematicians working in harmonic analysis, or to computer vision researchers studying multiscale image processing[29].

Discrete Wavelet Transform (DWT) algorithms have become standards tools for processing of signals and images in several areas in research and industry. The first DWT structures were based on the compactly supported conjugate quadrature filters (CQFs). However, a drawback in CQFs is related to the nonlinear phase effects such as image blurring and spatial dislocations in multi-scale analyses. On the contrary, in biorthogonal discrete wavelet transform (BDWT) the scaling and wavelet filters are symmetric and linear phase. The BDWT algorithms are commonly constructed by a ladder-type network called lifting scheme. The procedure consists of sequential down and uplifting steps and the reconstruction of the signal is made by running the lifting network in reverse order.

At the beginning of the 20th century, Haar, a German mathematician introduced the first wavelet transform named after him (almost a century after the introduction of the FT, by the (French J. Fourier). The Haar wavelet basis function has compact support and integer coefficients. Later, the Haar basis was used in physics to study Brownian motion since then;

different works have been carried out either in the development of the theory related to the wavelet, or towards its application in different fields. In the field of signal processing, the great achievements reached in different studies by Mallat, Meyer and Daubechies have allowed the emergence of a wide range of wavelet-based applications. In fact, inspired by the work developed by Mallat on the relationships between the Quadrature Mirror Filters (QMF), pyramid algorithms and orthonormal wavelet bases, Meyer constructed the first non-trivial wavelets [15]. However, the most important work was carried out by Ingrid Daubechies. Based on Mallat's work, Daubechies succeeded to construct a set of wavelet orthonormal basis functions, which have become the cornerstone of many applications [7]. Few years later, the same author, in collaboration with others [3], presented a set of wavelet biorthogonal basis function, which later found their use in different applications, especially in image coding.

This kind of two-dimensional DWT leads to a decomposition of approximation coefficients at level j in four components the approximation at level j + 1, and the details in three orientations (horizontal, vertical, and diagonal).

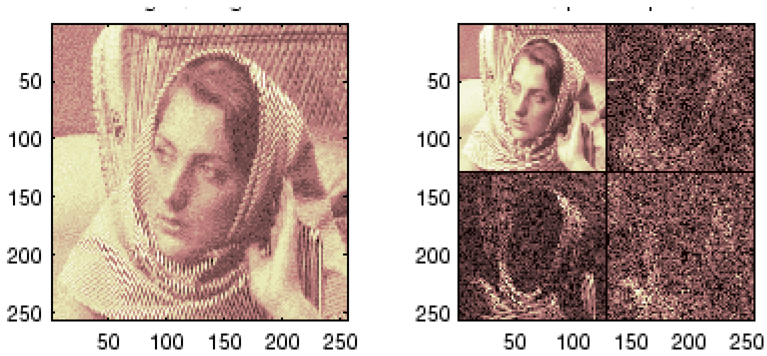


Figure 2.9 Dwt2 Command Outputs [31]

The Haar wavelet basis function has compact support and integer coefficients. Later, the Haar basis was used in physics to study Brownian motion since then; different works have been carried out either in the development of the theory related to the wavelet, or towards its application in different fields. In the field of signal processing, the great achievements reached in different studies by Mallat, Meyer and Daubechies have allowed the emergence of a wide range of wavelet-based applications.

The following chart describes the basic decomposition steps for images:

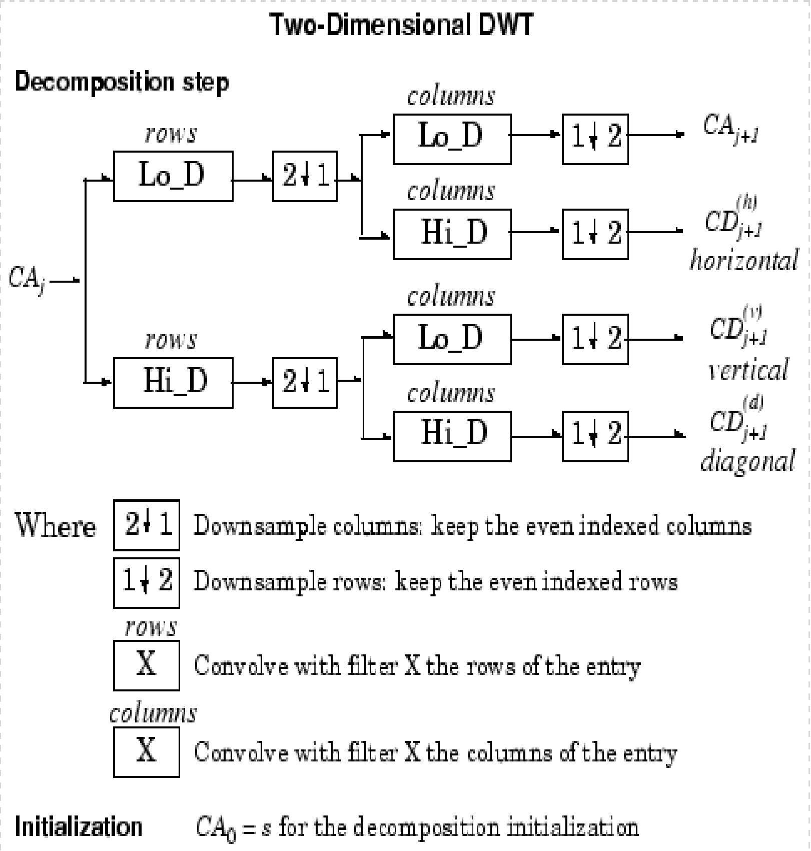

Two-Dimensional DWT
Decomposition step
rows
Lo_D
2↓1
columns
Lo_D
1↓2
$CA_{j+1}$
columns
Hi_D
1↓2
$CD^{(h)}_{j+1}$
horizontal
$CA_j$
rows
Hi_D
2↓1
columns
Lo_D
1↓2
$CD^{(v)}_{j+1}$
vertical
columns
Hi_D
1↓2
$CD^{(d)}_{j+1}$
diagonal
Where
2↓1 Downsample columns: keep the even indexed columns
1↓2 Downsample rows: keep the even indexed rows
rows
X Convolve with filter X the rows of the entry
columns
X Convolve with filter X the columns of the entry
Initialization $CA_0 = s$ for the decomposition initialization

Figure 2.10 Decomposition Steps [31]

Image is decomposed in 4 sub images , firstly it is passed through Low Pass filter then again it is passed through Low Pass filter and one sub image is computed.Image which was earlier passed through Low Pass filter is now passed through High Pass filter and another sub image is computed.To compute all four sub images,original image is passed through High Pass and Low Pass filters then again these two sub images are passed through High Pass filter and Low Pass filters and all four sub images are computed.

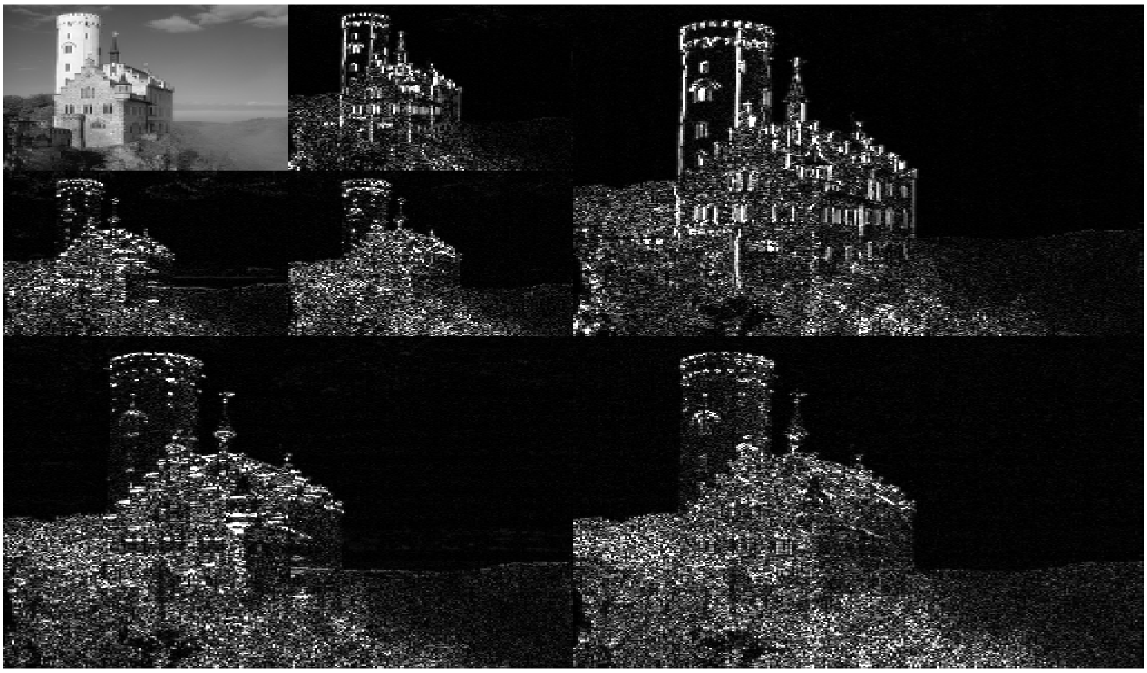


Figure2.11 2D Wavelet Transform [30]

An example of the 2D discrete wavelet transforms. The original image is high-pass filtered, yielding the three large images, each describing local changes in brightness (details) in the original image. It is then low-pass filtered and downscaled, yielding an approximation image; this image is high-pass filtered to produce the three smaller detail images, and low-pass filtered to produce the final approximation image in the upper left.

## 2.5 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[23][12].

### 2.5.1 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 intra-class 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.

### 2.5.2 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.

### 2.5.3 Structural Approach

Structural approaches mainly related to string, graph, and tree matching techniques and are generally used in combination with other techniques [6]. 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.

### 2.5.4 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.

## 2.6 Error Measurements

Two types of errors are calculated in verification system.

### 2.6.1 False Acceptance Rate

In this type of error % of those kind of signatures are computed which does not belong to genuine class but mistakenly they classified into genuine class .It can be defined as ratio of the no of false acceptance divided by total no of recognition attempts.

### 2.6.2 False Rejection Rate

In this type of error % of those kind of signatures are computed which belong to genuine class but falsely classified as forged class. It can be defined as ratio of no of false rejections divided by total no of recognition attempts.

# CHAPTER 3

# VERIFICATION TECHNIQUES

## 3.1 Some Approaches in Offline 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 [26] 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.

- Emre Özgündüz et al. [9] 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 centre of the signature, Local maxima numbers of the signature and Edge point numbers of the signature. SVM was used for classification.

- 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 [1]. The first NN classifier they used was three Back Propagation NNs and the second classifier consisted of two Radial Basis Function NNs.

- V A Bharadi and H B Kekre [2] 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.

- H.N. Prakash and D. S. Guru [19] 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. 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. [11] 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. [10] 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.

- J. F. Vargas et al. [22] 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. [21] 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.

- A method for signature verification using local Radon Transform was proposed by Vahid Kiani et al. [14]. 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.

- 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.

## 3.2 Verification Techniques

There are various verification techniques which researchers have been proposed for different purposes like support Vector Machine, Bayesian Learning, Hidden Markov Model, Neural Network etc. and each verification method gives optimal result when they are used in specific class of input patterns. HMM is a strong and effective statistical tool for modelling generative sequences, characterized by an underlying process that generates an observable sequence. Neural network is a mathematical model that can learn from examples and based on that knowledge can solve many problems such as pattern recognition.

### 3.2.1 Bayesian Learning

Bayesian reasoning estimates the posterior probability of a hypothesis given some initial knowledge or previously available data. Prior knowledge is combined in Bayesian learning along with the observed data to obtain posterior probability of the hypothesis. Bayesian method computes the posterior probability of the hypothesis according to Bayes' rule:

$$P(h \mid D) = \frac{P(D \mid h)P(h)}{P(D)} \qquad \text{...........................(1)}$$

It is a probabilistic approach, given prior probabilities of data and hypothesis, the most likely posterior hypothesis can be determined using this technique. This approach overcomes the limitation of having limited number of genuine samples [13]. Other techniques may require forgery samples as well, but this method overcomes this limitation as well. The most significant application of this method is that it just does not simply accept or reject a sample but it gives a probability as output of how likely the signature sample belongs to an individual, as a result a confidence value can be attached to all the probable choices. Bayesian method gives a probabilistic output for example this signature is 83% genuine or 90% forged. New instances can also be classified by combining the predictions of multiple hypotheses. Regarding signature verification, Bayesian learning can be implemented as follows: the hypothesis space can be defined as H = {genuine, forged}, and the data D can be the features of the signature samples such as velocity, pressure, no. of strokes etc. On the basis of the prior knowledge of these hypotheses and data, the posterior hypothesis can be estimated using Bayes’ theorem.

### 3.2.2 Hidden Markov Model (HMM)

HMM is a strong and effective statistical tool for modeling generative sequences, characterized by an underlying process that generates an observable sequence. HMMs have been applied in many application areas such as signal processing, speech recognition, pattern recognition and can be effectively implied in signature verification as well. HMM is a generalization of Markov Model. It is a robust method to model the variability of discrete time random signals where time or context information is available [13]. It can manage time duration varying signals such as signatures speech etc. For this reason it is popular for speech and signature recognition applications [6]. The signing process is divided into several states that constitute the markov chain. Each of the signature segments corresponds to each state in the model. A sequence of probability distributions of the different features that are used in the verification task are taken and a matching is done on it [26]. The verification score in these systems is usually obtained as the signature log-likelihood. An important part in generative model-based signature verification systems is the verification score normalization [9]. The verification score is a score that determines whether a particular signature is genuine or forged using a threshold value. These threshold values can be writer dependent or feature dependent. The disadvantages of using HMM in signature verification is that it requires huge number of features to be set, and the number of data to train the model is very large as a result of which its time complexity is very high.

### 3.2.3 Neural Network

Neural network is a mathematical model that can learn from examples and based on this knowledge can solve many problems such as pattern recognition. A number of genuine and forged samples are stored in the database which is used for learning and thus judging whether a given test signature is genuine or forged. An Artificial Neural Network is trained to recognize the variation that exists in the target signature with respect to the sample signature. Handwritten signature samples are considered input for the artificial neural network model and typically weights are learned during training a NN. The major factors of using ANN are Expressiveness, ability to generalize, sensitivity to noise, and graceful degradation. The major drawback of using ANN model is that it takes a lot of time for training.

In modelling of a signature verification system Neural Network can be used as follows: As training data, a vector of *n* number of sensors can be used where *n* is the number of features of the signature considered for verification. Here each of these vectors would estimate the similarity of the target feature with respect to the features of genuine signature samples. The ANN used for this purpose is a multilayer feed forward network which consists of *n* number of input units, one output unit signalling genuine or not genuine, and some units in one or more hidden layer. Back propagation algorithm is used for training.

### 3.2.4 Support Vector Machine (SVM)

Support vector machines are supervised learning models whose foundations stem from statistical learning theory. The support vector machine takes a set of input data sample and predicts, for each given input, which of two possible classes the output belongs, which makes it a non-probabilistic binary linear classifier. SVM has been considered a good choice for solving the signature verification problem as it is frequently used for pattern recognition applications, classification and regression problems [9]. An SVM maximally separates hyper plane that determines clusters by mapping input vectors to a higher dimensional space [10]. An SVM takes a set of input data and determines to which of the two classes the input data belongs.

| Technique | Approach | Basis | Type |
|---|---|---|---|
| **Support vector Machine** | Predictive Modelling | Principle of structural minimization | Statistical, Supervised Learning |
| **Neural Network** | Machine Learning | Adaptive system changing its Structure during a learning phase | Supervised Learning |
| **Bayesian Learning** | Probabilistic | Use of priori information to obtain posteri information | Statistical |
| **Hidden Markov Model** | Probabilistic | The hidden variables control the mixture component to be selected for each observation | Statistical |

Table 3.1 Different Classification Techniques

| **Author** | **Publication** | **Year** | **Extracted Features** | **Verification Method** |
|---|---|---|---|---|
| **A. Rathi, D. Rathi,P. Astya** | Using Pixel Based Method | 2012 | Pixels | Fuzzy Neural Network |
| **Julian Fieer** | Using Contour Features | 2008 | Length-based and direction - based | EuclideanDistance Method |
| **Julian Fieer** | Fusion Static Image | 2009 | Contour Features | Euclidean Distance Method |
| **Eric Granger and Robert** | A Multi-Hypothesis Approach | 2009 | States of signature | Hidden Markov Model |
| **Sargur N. Srihari** | Learning Strategies and Classification | 2004 | Combination of features | Distance Statistics |
| **DakshinacRanjan Kisku, Phalguni Gupta** | Fusion of Multiple Classifiers | 2010 | Global and Local Features | Support Vector Machine |
| **S. Daramola** | Offline Signature Recognition | 2010 | DCT Features | Hidden Markov Model |
| **Sargur Srihari** | Using Distance Statistics | 2004 | Gradient, 2004 Structural Concavity | Bayes Classifier |

Table 3.2 Comparative Study of Various Methods of Offline Signature Verification

## 3.3 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. 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 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.

# CHAPTER 4

## PROPOSED WORK

## PROPOSED WORK

The main objective of this work is to design a robust offline signature verification system. Proposed method is based on wavelet features then after SVM classifier is used for training and testing.This methodology consists of some crucial steps which need to follw in sequential order.All steps are discussed below.

### 4.1 Dataset Creation

Datasets are created manually by collecting samples of signature from each person.Every individual person has signed on a paper.No of samples from a single person has taken in a way such that personal variance should be covered so 10 signature samples are take from single person.

### 4.2 Pre-processing

To normalize the scanned signature images, some preprocessing steps have to be applied. The purpose in this phase is to make signatures to be of standard size and ready for feature extractionPreprocessing steps are very necessary to remove noise from the signature image and strictly need to be follow.Some crucial steps are listed below.

(a) *Grey Scale Conversion*

Since the scanned images are stored in database as a colour image, a three dimensional image (MXNX3) is not suitable for further processing, and should be converted into a grayscale image where each pixel is represented by a value in the range 0 to 255.'rgb2gray' command is used for this purpose.

(b) *Resize*

Every person signs in different way so all images need to kept in same dimension. So every image is resized into [128,128] standard size.'imresize' command is used for that purpose.

(c) *Binary Conversion*

It allows to reduce image information by removing background so that the image is black & white type. This type of image is much easier for further processing.

(d) *Image Cropping*

Individual signature images are automatically cropped to the actual size of the signature.

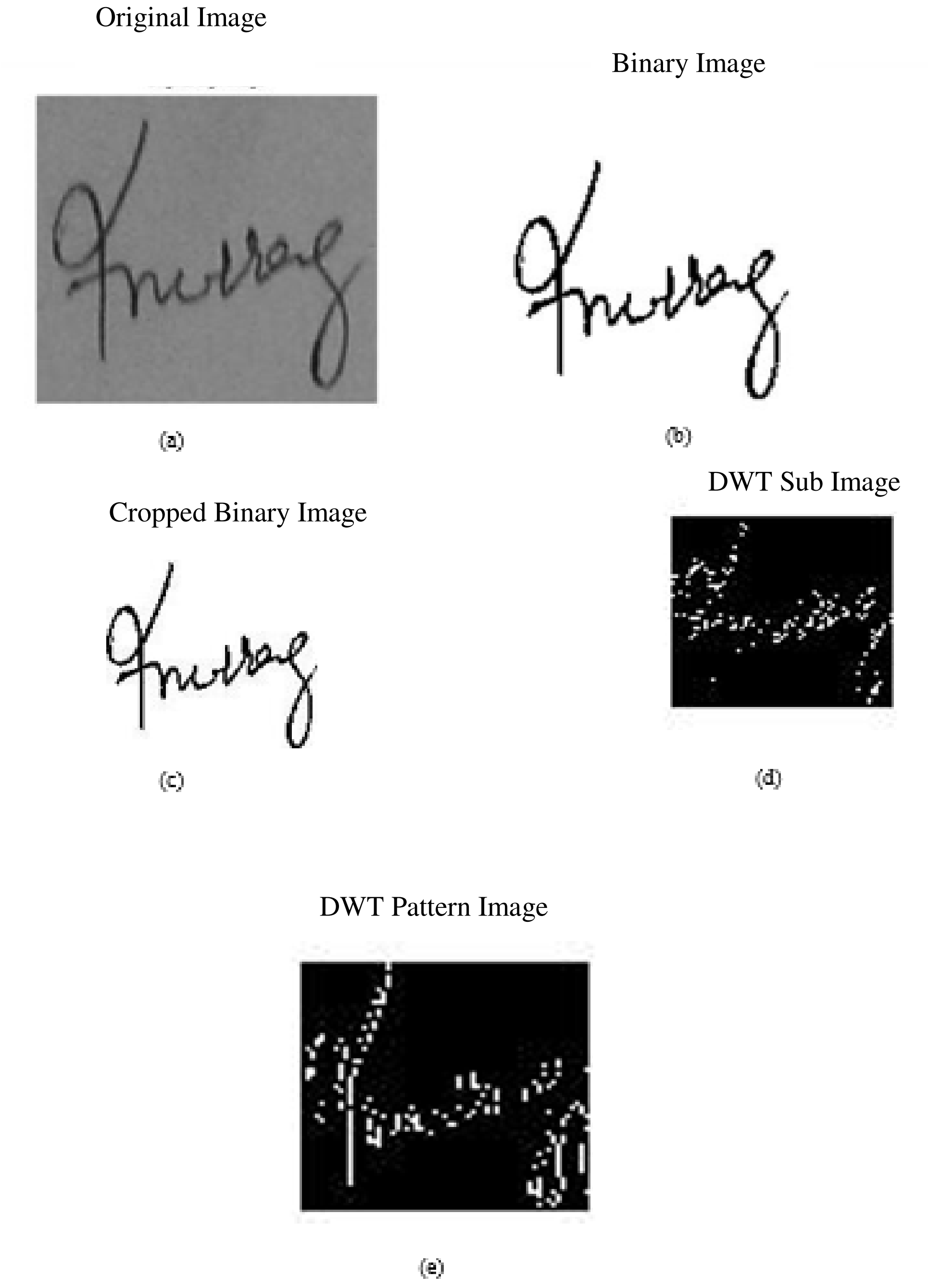


Figure 4.1 (a) Original Image (b) Binary Converted Image (c) Cropped Binary Image

## 4.3 Feature Extraction

In this step, suitable global and local wavelet features are extracted from the image. The procedure employed in this stage is described in the following steps. First- the global features such as height, width and area are extracted from whole image. Second- DWT (Discrete Wavelet Transform) is applied on signature image and maximum vertical projection position and maximum horizontal projection position features are extracted from each of the 3 sub images. Third- image is divided into 16 blocks and DWT is applied to each block to get 16*3 sub-images. Fourth- the energy features, are extracted from each of the sub images.

- The row, which has highest signature pixels, is taken as maximum horizontal projection.
- The column, which has highest signature pixels, is taken as maximum vertical projection position.

These two features are extracted from the sub images obtained when the DWT is applied on whole image. Discrete wavelet transform dwt2 is applied on image which can be seen as:
dwt2 - Single-level discrete 2-D wavelet transform. This MATLAB function computes the approximation coefficients matrix cA and details coefficients matrices cH, cV, and cD (horizontal, vertical, and diagonal, respectively), obtained by wavelet decomposition of the input matrix X.

## 4.4 Computation of Horizontal and Vertical Projection Features

DWT 2 command is applied on original (genuine) images of an individual person and as well as all corresponding forged images included (random, semi skilled and skilled forgery images).For all images horizontal and vertical projections are calculated. These computed values are used to train SVM classifier. For one single user all ten authentic samples horizontal and vertical projection values are computed then these projection values are computed for corresponding forged images. This process is repeated for all individual users.

After applying dwt on image 3 coefficient matrices horizontal, vertical, and diagonal, respectively are obtained, for every matrix and every row, column highest pixel value is computed which is known as horizontal and vertical projections are computed so 6 feature values are computed which are known as :

HPH: HORIZONTAL PROJECTION OF HORIZONTAL COMPONENT
VPH: VERTICAL PROJECTION OF HORIZONTAL COMPONENT
HPV: HORIZONTAL PROJECTION OF VERTICAL COMPONENT
VPV: VERTICAL PROJECTION OF VERTICAL COMPONENT
HPD: HORIZONTAL PROJECTION OF DIAGONAL COMPONENT
VPD: VERTICAL PROJECTION OF DIAGONAL COMPONENT

After computation of these projection features energy features are computed, before calculation of energy features image is divided into 16 blocks then on each block dwt is applied and 48 energy features are computed.

## 4.5 Calculation of Energy Feature

For each subdivided image dwt is applied and energy features are computed using equation

$$E = I(i, j) / MXN$$

I (i , j) total no of white pixels, MXN is size of sub image, E is energy value computed

So this is how all 59 features are computed which are combination of global and energy features.

| S.NO | FEATURE | S.NO | FEATURE | S.NO | FEATURE | S.NO | FEATURE |
|---|---|---|---|---|---|---|---|
| **1** | HEIGHT | 16 | VEV2 | 31 | VEV7 | 46 | VEV12 |
| **2** | WIDTH | 17 | DEV2 | 32 | DEV7 | 47 | DEV12 |
| **3** | AREA | 18 | HEV3 | 33 | HEV8 | 48 | HEV13 |
| **4** | CENTROID X | 19 | VEV3 | 34 | VEV8 | 49 | VEV13 |
| **5** | CENTROIDY | 20 | DEV3 | 35 | DEV8 | 50 | DEV13 |
| **6** | HPH | 21 | HEV4 | 36 | HEV9 | 51 | HEV14 |
| **7** | VPH | 22 | VEV4 | 37 | VEV9 | 52 | VEV14 |
| **8** | HPV | 23 | DEV4 | 38 | DEV9 | 53 | DEV14 |
| **9** | VPV | 24 | HEV5 | 39 | HEV10 | 54 | HEV15 |
| **10** | HPD | 25 | VEV5 | 40 | VEV10 | 55 | VEV15 |
| **11** | VPD | 26 | DEV5 | 41 | DEV10 | 56 | DEV15 |
| **12** | HEV1 | 27 | HEV6 | 42 | HEV11 | 57 | HEV16 |
| **13** | VEV1 | 28 | VEV6 | 43 | VEV11 | 58 | VEV16 |
| **14** | DEV1 | 29 | DEV6 | 44 | DEV11 | 59 | DEV16 |
| **15** | HEV2 | 30 | HEV7 | 45 | HEV12 | | |

Table No3.3 Features Extracted in Proposed Model

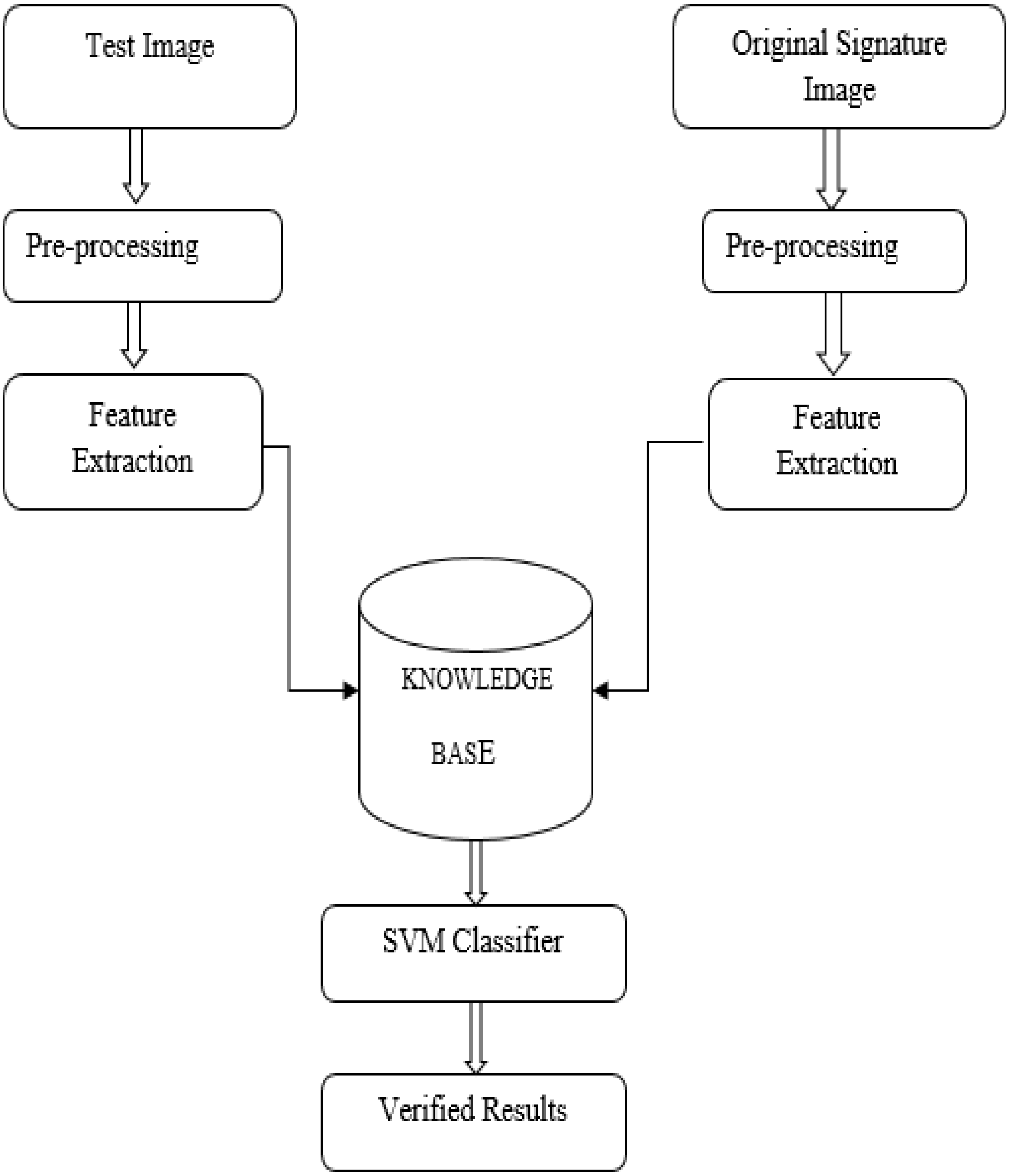


Figure 4.2 Block Diagram for the Flow of Proposed Model

## 4.6 SVM Classification

Support vector machines are supervised learning models whose foundations stem from statistical learning theory. The support vector machine takes a set of input data sample and predicts, for each given input, which of two possible classes the output belongs, which makes it a non-probabilistic binary linear classifier. SVM has been considered a good choice for solving the signature verification problem as it is frequently used for pattern recognition applications, classification and regression problems [9]. SVM maximally separates hyper plane that determines clusters by mapping input vectors to a higher dimensional space [10]. SVM takes a set of input data and determines to which of the two classes the input data belongs.

### 4.6.1 SVM Training

SVM is trained with 10 feature vectors; first five are genuine signature samples feature vector, rest five belongs to forged signature feature vector.So SVM is trained with these feature vectors. For every single user SVM is trained in this way.

### 4.6.2 SVM Testing

In testing next five samples from every users either from genuine class or forged class is tested i.e for a single user 10 genuine signature samples were collected and 10 forgeries so from these two classes signatures which used earlier in training are left and rest were used for testing.

```
ip = xlsread ('features2.xlsx');

train = zeros (10, 59);

test =zeros (10,59);

train (1:5,:)=ip (1:5,:);

train (6:10,:)=ip (11:15,:);

 test (1:5,:)=ip (6:10,:);

test (6:10,:)=ip (16:20,:);

Group = [1, 1,1,1,1,-1,-1,-1,-1,-1]';

SVMStruct = svmtrain (train', Group);
```

# CHAPTER 5

# RESULT ANALYSIS

## RESULT ANALYSIS

In this section proposed technique's result are shown and comparison with exixting method is also described. The experiments conducted indicate that as the number of different signatures increases the performance accuracy is decreased. Also with the increase of training samples the performance accuracy has been increased.Support vector machine was successfully trained with the 59 features of each sample of class forged and genuine.SVM successfully classified among forged and genuine class with system accuracy up to 90%.

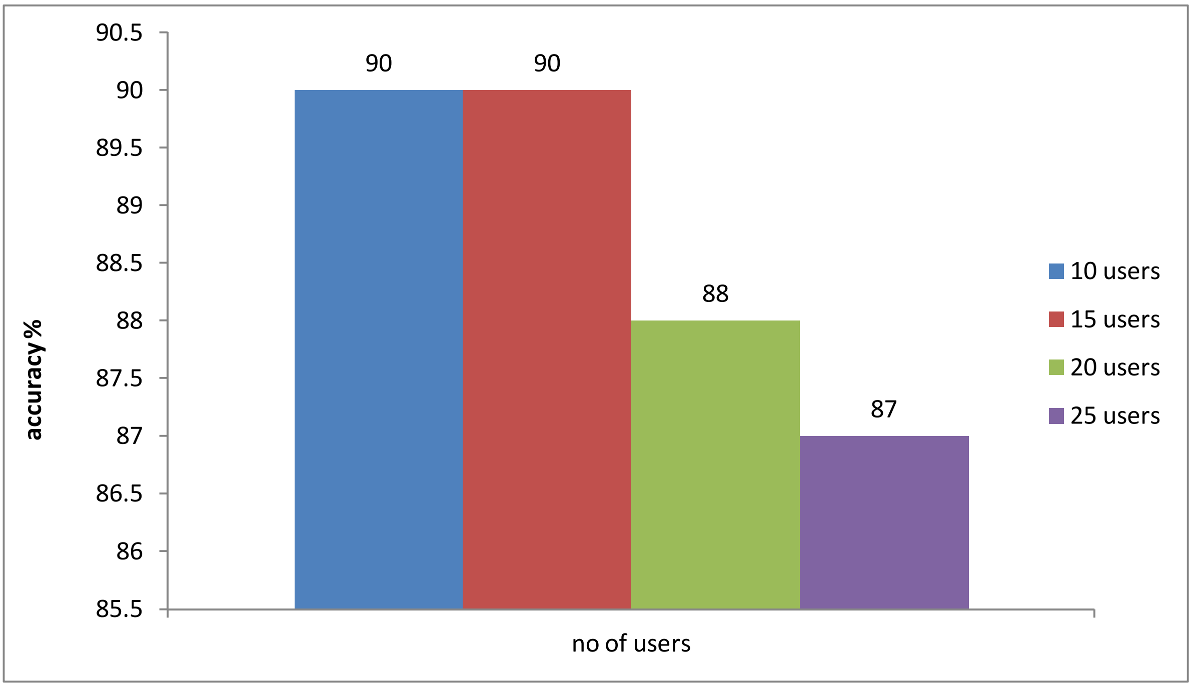


Figure 5 Performance Measure Graph

## 5.1ERROR RATE

Maximum optimized error in terms of false accepted rate and false rejected are 10% in both.

| **PROPOSED** | **FAR (%)** | **FRR (%)** |
|---|---|---|
| **METHOD** | **10** | **10** |

Table 4.1 Error Rate of Proposed Model

## 5.2 Result Comparison with Other Methods

| Author | Method | FAR (%) | FRR (%) |
|---|---|---|---|
| **Vu Nguyen et al** | Compact Size Feature Set | 17 | 13 |
| **Muhammad Reza Pourshahabi et al** | Contourlet Transform | 14.50 | 12.50 |
| **Sepideh Afsardoost et al** | Geometric Center Features | 15 | 14 |
| **A. Ismail et al** | Principal Components Analysis | 17 | 15 |
| **Amit Kishore Shukla et al** | Grid and Tree Based Feature Extraction | 17 | 13 |
| **Debasish Jena et al** | Feature Point Extraction | 19.3 | 20.83 |
| **J. Coetzer,** | Discrete Radon Trans-form | 18.79 | 17.79 |
| **Bin Fang and Yuan Yan Tang** | Class Statistics Estimation for Sparse Data | 23.3 | 23.5 |
| **Tai-ping Zhang, Bin Fang** | Envelope Curvature Descriptor | 18 | 23 |
| **Proposed Method** | Discrete Wavelet Transform | 10 | 10 |

Table 5.1 Error Rate Comparison with Existing Techniques

## CONCLUSION AND FUTURE WORK

A handwritten signature is a result of complex psychological procedure and therefore it is very difficult to estimate it using any method therefore it is required to find out the most optimal method that approximates the distinguishing features of a signature and use it to verify an individual.In this work, an off-line signature recognition system designed using 3 stages namely pre- Processing, feature extraction and classification stage in order to make the right decision is presented. This signature recognition is based on 59 powerful global and local wavelet features of different signatures. Experimental evidence has shown that this method has provided substantial improvements up to 90%.This accuracy can be improved still with the more number of samples of each signature used. This accuracy can be improved still with the more number of samples of each signature used. One problem faced, is the lack of samples needed to build a reliable signature recognition system and asses the performance. Future avenues of this work include an analysis of new features of signature image and combining those with the feature vectors used in this work to obtain better accuracy than the accuracy of present work. Some of the future works for the proposed methodology are:

- No of samples for a single person should be increased so that system will perform better and results will be more optimized.
- At the preprocessing steps morphological operators and no of filters used to remove noise should applied in optimal way.

## LIMITATIONS

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

(ii) Low quantity of available signature samples versus high number of extracted features.

The first issue is addressed by some researchers, but this is still a challenging problem. Luana Batista et al. 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

# REFERENCES

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

[2] 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).

[3] Cody, M. A. (1994). The Wavelet Packet Transform, Dr. Dobb's Journal, Vol. 19, Apr. 1994 Daubechies, I. (1988). Orthonormal Bases Of Compactly Supported.

[4] C. Gruber, T. Gruber, S. Krinninger, and Bernhard Sick, “Online Signature Verification With Support Vector Machines Based on Lcss Kernel Functions,” IEEE Transactions on Systems, Man, And Cybernetics—Part B: Cybernetics, Vol. 40, No. 4, Pp. 1088-1100, August 2010.

[5] D. Pu and S. N. Srihari, “A Probabilistic Measure for Signature Verification Based on Bayesian Learning,” International Conference on Pattern Recognition, IEEE, Pp. 1188-1191, 2010.

[6] D. Impedovo and G. Pirlo, “Automatic Signature Verification: The State of The Art,” IEEE Transactions on Systems, Man, and Cybernetics Partc: Applications and Reviews, Vol.38, No. 5, September 2008.

[7] Daubechies, I. (1992). Ten Lectures on Wavelets, Siam, Philadelphia.

[8] Emre Özgündüz, Tülin Şentürk and M. Elif Karslıgil “Off-Line Signature Verification and Recognition by Support Vector Machine” Computer Engineering Department, Yıldız Technical University Yıldız, Istanbul, Turkey 2013

[9] E. A. Rúa and J. L. Alba, “Online Signature Verification Based On Generative Models,” IEEE Trans. Syst., Man, Cybern. B, Vol. 42, No. 4, Pp. 1231-1242, Aug. 2012.

[10] 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.

[11] Hanmandlu M, Hafizuddin M. Yusof M. and Madasu V K. 2005." Off-Line Signature Verification and Forgery Detection Using Fuzzy Modelling". Pattern Recognition 38 (2005) (Pp 341 – 356).

[12] 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.

[13] J. Fierrez, J. O. Garcia and D. Ramos, "HMM-Based On-Line Signature Verification: Feature Extraction and Signature Modelling," Pattern recognition Letters, Elsevier, Vol. 28, No. 16, Pp. 2325-2334, December 2007.

[14] 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).

[15] Meyer, Y. (1987).Wavelet With Compact Support. Zygmund Lectures, University Chicago.

[16] Md. Asraful Haque, Tofik Ali "Improved Offline Signature Verification Method Using Parallel Block Analysis" Department of Computer Engineering Aligarh Muslim University 2010.

[17] M. Arya And V. Inamdar, "A Preliminary Study On Various Off-Line Hand Written Signature Verification Approaches", International Journal Of Computer Applications, Vol. 9, Pp. 77-S3, 2010.

[18] Nguyen V, Blumenstein M and Leedham G. 2009 "Global Features For The Off-Line Signature Verification" International Journal Of Computer Applications (0975 – 8887) Volume 42– No.16, March 2012 52 Problem. 2009 10th International Conference on Document Analysis and Recognition (IEEE).

[19] 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).

[20] R. S. Kashi, J. Hu, W. L. Nelson, and W. L. Turin, “A Hidden Markov Model Approach To Online Handwritten Signature Verification,” Int. J. Doc. Annual. Recognit. (IJDAR), Vol. 1, No. 2, Pp. 102–109, 1998.

[21] Stéphane Armand, Michael Blumenstein and Vallipuram Muthukkumarasamy Griffith University, Australia IEEE Magazine 2007.

[22] 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).

[23] 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

[24] Yazan M. Al-Omari, Siti Norul Huda Sheikh Abdullah and Khairuddin Omar. “State of the Art Offline Signature Verification System”. IEEE International Conference on Pattern Analysis and Intelligent Robotics 28-29 June 2011, Putrajaya, Malaysia

[25] Yu Qiao, Jianzhuang Liu “Offline Signature Verification Using Online Handwriting Registration” Department of Information Engineering the Chinese University Of Hong Kong 2014

[26] http://en.wikipedia.org/wiki/biometrics

[27] http://en.wikipedia.org/wiki/Biometrics#mediaviewer/File:Biometric_system_diagram

[28] https://www.kaggle.com/c/icdar2013-stroke-recovery-from-offline-data

[29]http://cdn.intechopen.com/pdfs/34963/InTechThe_wavelet_transform_for_image_processing applications.pdf

[30] http://en.wikipedia.org/wiki/Discrete_wavelet_transform

[31] www.mathswork.com