

# **Handwritten Signature Verification using Local Binary Pattern & KNN**

**A Project Report**

*Submitted by*

**Tejas Jadhav**

*Under The Guidance Of*

**Prof. Abhay Kolhe**

*in partial fulfillment for the award  
of the degree of*

**M. TECH.  
in  
COMPUTER ENGINEERING  
at**



**SVKM's NMIMS,  
Mukesh Patel School of Technology Management & Engineering,  
Mumbai**

**2018 - 19**

## **CERTIFICATE FROM INTERNAL MENTOR**

This is to certify that the project synopsis entitled “Handwritten Signature Verification using Local Binary Pattern & KNN” is the proposed work by Tejas Jadhav of M. Tech. (Computer Engineering), MPSTME (NMIMS), Mumbai, during the III/IV semester of the academic year 2018 - 2019 is verified by me.

The presentation for the same is also verified by me.

---

Prof. Abhay Kolhe

Internal Mentor

## **CERTIFICATE FROM EXAMINERS**

This is to certify that the project entitled “Handwritten Signature Verification using Local Binary Pattern & KNN” is the bonafide work carried out by Tejas Jadhav of M.Tech. (Computer Engineering), MPSTME (NMIMS), Mumbai, during the IV semester of the academic year 2018-2019 in fulfilment of the requirements for the award of the Degree of Masters of Technology as per the norms prescribed by NMIMS. The project work has been assessed and found to be satisfactory.

---

Examiner 1

---

Examiner 2

---

Head of Computer Engineering Department

Dr. Pravin Shrinath

## **DECLARATION**

I, Tejas Jadhav, Roll No. B002, M.Tech (Computer Engineering), IV semester understand that plagiarism is defined as anyone or combination of the following:

1. Un-credited verbatim copying of individual sentences, paragraphs or illustration (such as graphs, diagrams, etc.) from any source, published or unpublished, including the internet.
2. Un-credited improper paraphrasing of pages paragraphs (changing a few words phrases, or rearranging the original sentence order)
3. Credited verbatim copying of a major portion of a paper (or thesis chapter) without clear delineation of who did wrote what. (Source: IEEE, The institute, Dec. 2004)
4. I have made sure that all the ideas, expressions, graphs, diagrams, etc., that are not a result of my work, are properly credited. Long phrases or sentences that had to be used verbatim from published literature have been clearly identified using quotation marks.
5. I affirm that no portion of my work can be considered as plagiarism and I take full responsibility if such a complaint occurs. I understand fully well that the guide of the seminar/project report may not be in a position to check for the possibility of such incidences of plagiarism in this body of work. I declare that the written submission represents my ideas in my own words and where others ideas or works have included; I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any new idea/data/fact/source in my submission. I understand that any violation of the above will cause for disciplinary action by the institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

**Signature of the Student:**

Name: Tejas Jadhav

Roll No. B - 002

Place: Mumbai

Date:

## **Acknowledgement**

This has been the light of the day due to valuable contribution of certain individuals whose constant guidance, support and encouragement resulted in the realization of my project. I am grateful to my Guide Prof Abhay Kolhe for providing me the necessary help and encouragement whenever I needed, which has resulted in the success of my project.

I take this opportunity to thank Dr. N. T. Rao, Dean of Mukesh Patel School of Technology Management & Engineering, NMIMS University Mumbai for providing a healthy environment in the college, which helped me in concentrating on my task.

I would also like to thank Dr Pravin Srinath, HOD of Computer Science Department of Mukesh Patel School of Technology Management & Engineering, NMIMS University Mumbai for providing his invaluable guidance, comments and suggestions throughout the course of the project.

This project would not have been possible without the efforts of Prof Prashasti Kanikar and all the staff members of M.Tech Computer Science department, without whose constructive suggestions and valuable advice, the simple idea, which had born in me, would not have been able to blossom into a successful project.

Last but not the least, I am grateful to all my friends and my parents for their constant support throughout the course of this project.

## Table of Contents

<b>Chapter no</b>	<b>Title</b>	<b>Page no</b>
	List of Figures	i
	List of Tables	ii
	Abstract	iii
<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>1.1</b>	Real life applications	1
<b>1.2</b>	Types & methods of Signature Verification	2
1.3	Performance evaluation parameters	2
<b>2</b>	<b>Motivation</b>	<b>3</b>
<b>3</b>	<b>Problem definition</b>	<b>4</b>
<b>4</b>	<b>Literature review</b>	<b>5</b>
<b>5</b>	<b>Proposed work (algorithm/ techniques/ experimental setup)</b>	15
<b>5.1</b>	Algorithm to be used	15
<b>5.2</b>	Otsu thresholding	16
<b>5.3</b>	Local Binary Patterns	17
<b>5.4</b>	K-Nearest Neighbours	22
<b>5.5</b>	Implementation tools end setup	23
<b>5.5.1</b>	Python using PyCharm	23
<b>5.5.2</b>	Database using MySQL	24
<b>6</b>	<b>Work done</b>	<b>25</b>
<b>6.1</b>	Research	25
<b>6.2</b>	Dataset preparation	25
<b>6.3</b>	Implementation	26
<b>6.3.1</b>	Main.py	26
<b>6.3.2</b>	Dataset.py	27

<b>6.3.3</b>	PreProcessing.py	28
<b>6.3.4</b>	NormalFeat.py	29
<b>6.3.5</b>	LocalBinaryPattern.py	30
<b>6.3.6</b>	LbpFeat.py	32
<b>6.3.7</b>	Classification.py	33
<b>6.3.8</b>	Evaluation.py	33
<b>6.3.9</b>	Signature_verifier.sql	35
<b>7</b>	<b>Comparative study</b>	36
<b>7.1</b>	Dataset	36
<b>7.2</b>	Preprocessing	36
<b>7.3</b>	Model used	36
<b>7.4</b>	Evaluation	37
<b>8</b>	<b>Conclusion &amp; Future Work</b>	38
<b>9</b>	<b>References</b>	39
<b>10</b>	<b>Appendix</b>	42

## List of Figures

<b>Chapter no</b>	<b>Title</b>	<b>Page no</b>
<b>1</b>	Performance evaluation graph	2
<b>4</b>	Flowchart of paper [1]	5
	Dynamic Time warping	5
	Data from tablet and pen.	6
	Flowchart for paper [8]	7
	Polar scale normalization	9
	DTW algorithm of paper [16]	9
	Flowchart of paper [17]	10
	Flow Diagram for Paper [23]	11
	Flowchart of system in paper [31]	12
	Flow chart of paper [32]	13
<b>5</b>	Block diagram of the proposed approach	15
	Different thresholding methods	17
	The first step in constructing a LBP.	18
	The second step in constructing a LBP.	18
	The third step in constructing a LBP.	19
	Computing the LBP representation (right) from the original input image (left).	19
	Histogram for LBP image	20
	Three neighborhood examples with varying p and r used to construct Local Binary Patterns.	21
	data points set 1	22
	data points set 2	22
	Python logo	23
	PyCharm logo	23
	SQL logo	24
	MySQL logo	24

<b>6</b>	Dataset prepared	25
	Python program files prepared in PyCharm	26
	Main.py and GUI	26
	Test An image UI	27
	dataAnalysis.txt	27
	DataSet analysis popup UI	27
	Dataset.py	28
	Varying thresholds	28
	Preprocessing signature image	29
	Progress meter bar GUI while training and testing	29
	Normal features printed on console	30
	LBP image conversion algorithm	31
	LBP image conversion: (a) Grey image; (b) LBP image	31
	8-neighbour pixels	32
	LBP texture features printed on console	32
	Classification printed on console	33
	Line Graph for analysis different LBP Variants	34
	Evaluation popup UI	36
	Feature vectors in python console	36
	Tables in MySQL database	36
<b>7</b>	Existing project	38

## List of Tables

<b>Chapter no</b>	<b>Title</b>	<b>Page no</b>
<b>4</b>	Local radon transform features	6
<b>7</b>	Expermintatal Analysis of different LBP Variants	34
<b>7</b>	Expermintatal Analysis with different values of K	35

## **ABSTRACT**

Whether one signs a petition, work documents, contract, or wants to approve payment of a check, he/she uses personal signature to do all those things. An offline signature verification method has been described in this designed project and the subsequent project report. Handwritten signature has been critical person identification technique for decades. The objective of this paper is to give away an efficient biometric signature recognition and verification techniques. The study intends to give away information all about the application of biometrics i.e. signature detection and also about the various stages that are necessary to be studied by a designer while creating an application that will use it. The system works in different stages which includes pre-processing, LBP image conversion, feature extraction, and classification. A total of 40 different signature recognition approaches were read and studied before designing the system here that are been taken from different research papers. The output obtained is evaluated in the papers itself by performing experimental analysis and can be compared with another existing system in this paper.

# **1. Introduction**

Biometrics is currently perceived as a vital technology for setting up secure access control. It utilizes physiological qualities of humans for recognizing individual, and signature is one of the characteristics usable for biometrics. Singular recognizable proof technology utilizing human countenances, more often than not called confront acknowledgment technology, has been concentrated primarily in western nations since 1990s. It has been the most widespread tool for paper documents verification for many decades. In real life the human-expert can verify handwritten signatures easily, but it is a complicated task for doing by machines today.

## **1.1 Real life applications**

This application of Image processing has number of uses in the real world and are seen to be very critical in many industries. Some of them are as follows:

1. Finance: IT-Processing firms of German savings banks are offering their customers solutions to embed dynamic signatures securely into electronic documents in an Adobe Live Cycle environment
2. Insurance: Signing an insurance contract and documenting the consulting process that is required by EU legislation have caused several insurance companies to go paperless with either signature capturing tablets connected to a notebook or a tablet PC.
3. Real Estate: Increasingly popular among real estate agents in USA are options of paperless contracting through signing on Tablet PCs.
4. Health: The hospital of Ingolstadt is capturing and verifying the signatures of their doctors that fill electronic patient records on tablet PCs. The “National Health Service” organization in the UK has started such an implementation.
5. Telecom: Signing phone and DSL contracts in the telecom shops is another emerging market.

## **1.2 Types & methods of Signature Verification**

There are two types of signature verification methods:

### **1. Offline Signature Verification Methods:**

In this method, system makes use of a simple scanner or a camera that can take in image having signature & process the image further with whatever features it gets. This method can be seen useful in many applications such as banking cheques, medical certificates & prescriptions etc.

### **2. Online Signature Verification Methods:**

Here the system makes use of special acquisition devices like stylus pens and tablets that can take in signature features in real time and may give better accuracy

### 1.3 Performance evaluation parameters

#### 1. FAR – False Acceptance Rate :

The false acceptance rate in simple words is rate of falsely accepted signatures. This is given by the following formula:

$$FAR = \frac{\text{Total Number Imposter Signatures Accepted as Genuine}}{\text{Total Number of Forgery Tests Performed}}$$

#### 2. FRR – False Recognition Rate : Rate of falsely rejected signatures

The false acceptance rate in simple words is rate of falsely rejected signatures. This is given by the following formula:

$$FRR = \frac{\text{Total Number Genuine Signatures Rejected as Imposter}}{\text{Total Number of Genuine Matching Tests Performed}}$$

#### 3. EER – Equal Error Rate

The Equal Error Rate (EER) corresponds to the error value for which false acceptance rate is equal to false rejection rate. These rates determine the quality of an authentication system, but the acceptable values depend on the level of security desired for a specific application.

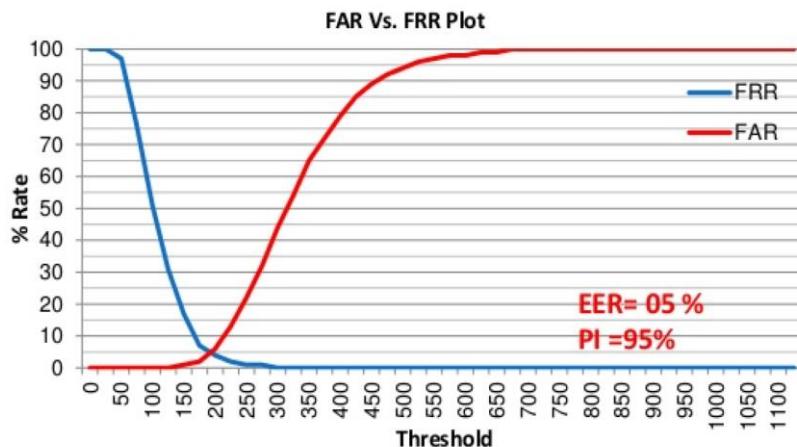


Figure 1: Performance evaluation graph

#### 4. PI – Performance Index

Performance index is nothing but the opposite of the Equal error rate. This is calculated easily by the following formula:

$$PI = 100 - EER$$

## **2. Motivation**

Today the human signature of a person is used as an identification of person because we are all know that the each person has distinct signature and every signature has its own physiology or behavioral characteristics. So the human signature used as an identification of person in various work like bank checks etc. The fraud person can easily generated the signature instead of unique signer in fraud way so we need a signature identification system

Nowadays, person identification is very important in security and resource access control. A reliable signature recognition system can be seen as an important part of law enforcement, finance & banking and many business processes. In such applications, an accurate recognition of person through his handwritten signature is critical.

Thus the motivation behind this project is the growing need for a full proof signature verification scheme which can guarantee maximum possible security from fake signatures. The idea behind the project is also to ensure that the proposed scheme can provide comparable and if possible better performance than already established offline signature verification schemes. The prospect of minimizing the memory space for storing signature image by the preprocessing extracted feature and the training is completed in acquiring less time and provide better accuracy. The need to make sure that only the right people are authorized to access high-security systems has paved the way for the development of systems for automatic personal authentication

### **3. Problem definition**

Signature Recognition is the procedure of determining to whom a particular signature belongs to, as said earlier. This problem is a huge research topic under the Image Processing domain. But this problem is also sometimes crossed with Machine Learning domain along with the Image Processing domain. This is not as simple as said it seems. It is just easier said than done.

Thus the system to be designed must have an algorithm that will extract features and recognize and verify the signer's authentication. System would take as input signature images and tell us following things: If the signature is forged or genuine (Signature Verification)

## 4. Literature review

This section lists down the various algorithms that we are to study. Most of them work in 3 stages, which are pre-processing, main processing i.e. feature extraction and then post-processing stage which includes decision making or classification. There are a high number of algorithms that can be implemented for recognition of handwritten signatures these days, but following are the algorithms which give other newly formulated algorithms a backbone.

In paper [1] the researchers are considering some simple parameters like speed, acceleration, pen down time, distance, etc. and based on the literature studies they discuss how these features can be used in the Image processing environment to improve the performance of handwritten signature. The approach provides a PI of 97.5 %.

Features extracted and used for comparison include total Euclidian distance D of the pen travelled, Speed Vx and Vy express the functions of time, Acceleration Ax and Ay, Total time taken Tk, Length-to-width ratio, Amount of zero speed in direction x and y directions Nvx and Nvy , Amount of zero acceleration in direction x and y directions Nax and Nay

The paper [2] presents a crowdsourcing experiment to establish the human baseline performance for signature recognition tasks and a novel attribute-based semi-automatic signature verification system inspired in FDE analysis. It combines the DTW algorithm with Attribute based algorithm to obtain better accuracy and increase the recognition rate. With EER of 5%, we can say that recognition rate is 95%. Attribute based recognition features include Shape, Proportionality, Text-loops, Order, Punctuation, Flourish-characteristics, Hesitation, Alignment to the baseline, Slant of the strokes, Strokes-length, Character spacing

The dynamic time warping algorithm finds an optimal match between two sequences of feature vectors which allows for stretched and compressed sections of the sequence.

The proposed system in paper [3] functions in three stages. Pre-processing stage; this consists of grey scale conversion, binarisation and fitting boundary box. Feature extraction stage where total 16 radon transform based projection features are extracted which are used to distinguish the different signatures. Finally in the classification stage; an efficient BPNN, Back Propagation Neural Network is prepared and trained with 16 extracted features. The average recognition accuracy of this system ranges from 87% - 97% with the training set of 10–40 persons. Global features include\_Height of the signature, Width of the signature, and Centroid along both X axis, Centroid along both Y axis

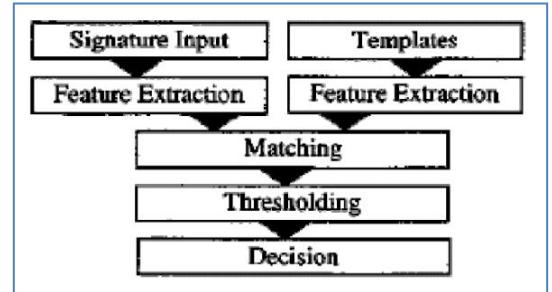


Figure 2: Flowchart of paper [1]

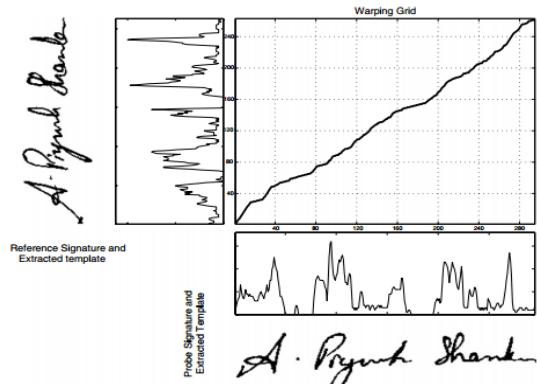


Figure 3: Dynamic Time warping

The radon transform derives projections of the image matrix along predefined directions. A projection of a two dimensional function  $f(x,y)$  is a group of line integrals. The radon transform calculates the line integrals from multiple sources along parallel paths, or beams, in a predefined direction. The beams are spaced one pixel unit apart. To represent an image, the radon transform takes multiple, parallel-beam projections of the image from different angles by rotating the source around the centre of the image. Radon transform of a signature image  $I$  for the angles specified in the vector ‘theta’ is computed using the Matlab function `radon()`.

It returns a vector ‘r’ for each angle in theta containing the Radon Transform. Mean and standard deviation of all the vectors ‘r’ are calculated and taken as local features.

The number of neurons in the first layer is  $n$  ( $n=16$  in this work) which is equal to the dimensionality of the input pattern vectors (Number of input nodes equals number of input features used). The number of neurons in the output layer is 5 which are equal to the number of pattern classes.

**Table 1:** Local radon transform features

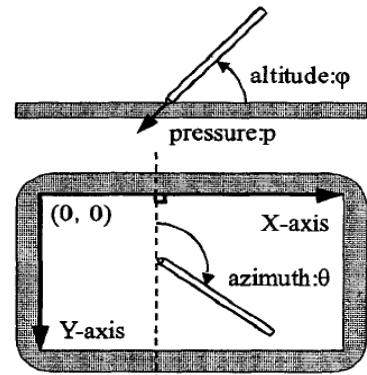
1	Height	9	Mean90
2	Width	10	Std90
3	Centroid of X axis	11	Mean120
4	Centroid of Y axis	12	Std120
5	Mean30	13	Mean150
6	Std30	14	Std150
7	Mean60	15	Mean180
8	Std60	16	Std180

The developed BPNN is trained with signature from different persons. Large numbers of images are required to ensure proper training of the NN.

In paper [4], researchers propose a new on-line writer authentication system using the pen altitude, pen azimuth, shape of signature, and writing pressure in real time. It is well expected that altitude and the azimuth of gripped pen under signing depends on the shape of writer's hand and the habit of writing. After individuality in the altitude and the azimuth of gripped pen under signing is explained, the experimental result with writing information by 24 writers is shown. It is found that the authentication rate of 98.2% is obtained.

The data set prepared is based on the following Features to be calculated dynamically at every instance of time: X-coordinate:  $x(t)$ , Y-coordinate:  $y(t)$ , Pressure:  $p(t)$ , Azimuth:  $\theta(t)$ , Altitude:  $\phi(t)$

In paper [5], researchers propose a new on-line writer authentication system that uses the pen azimuth, point positions of signature, and writing pressure in real time for creating 7 fuzzy characteristics. The stability of the altitude and the azimuth under signing is also compared with the bit-mapped data and the pen pressure along time for one writer.



**Figure 4:** Data from tablet and pen.

Researchers used collection of signatures for testing this system. Signature verification experiment has been conducted with 100 users across 25 original and 25 fake signatures for each user. The recognition rate shown was 99.8%. A 28-dimensional feature vector for the signature is formed.

In this paper [6] researchers present an off-line signature verification and recognition system using the global, directional and grid features of signatures. Support Vector Machine (SVM) was used to classify & verify the signatures and a classification ratio of 0.95 was obtained. Thus 95% accuracy is obtained as the recognition of signatures represents a multiclass problem SVM's one-against-all method was used.

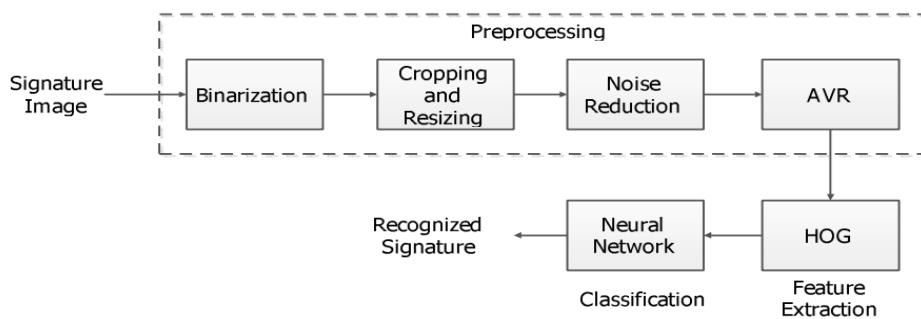
The system researchers introduced is divided into two major sections: (i) Training signatures, (ii) Verification or recognition of given signature.

Features used were Signature area, Signature height-to-width ratio, Maximum horizontal histogram and maximum horizontal histogram, Maximum vertical histogram and maximum vertical histogram, Horizontal and vertical center of the signature are calculated using the formulas

In this system, a multi class system is constructed by combining two class SVMs, radial basis function is used which gave the best results. In the training phase, for each person 8 positive (genuine) and 82 ( $39 \times 2 + 4$ ) negative (forgery) examples are taken.

The proposed system of paper [7] functions in three stages. Pre-processing stage consists of four steps namely gray scale conversion, binarization, thinning and fitting boundary box process in order to make signatures ready for the important feature extraction. Feature extraction stage consists total 59 global and local wavelet based energy features to be extracted which are used to classify the different signatures. Finally in classification, a simple Euclidean distance classifier is used as decision tool. The average recognition accuracy obtained using this model ranges from 90% to 100% with the training set of images of 10 to 30 persons.

The proposed method in paper [8] is based on the hypothesis; reducing the variability of signatures leads to boost up the recognition rate. Therefore, the variance reduction technique is applied to normalize offline handwritten signatures by means of an adaptive dilation operator. Then the variability of signatures is analyzed in terms of coefficient of variation (CV). The optimal CV is obtained and used as a threshold limit value to be acceptable variance reduction. The average recognition rate after experimental analysis is found to be 94.87%.



**Figure 5:** Flowchart for paper [8]

The paper [9] proposed a SIFT and a SURF algorithm which is used for enhanced offline signature recognition. This process, Bag-of-word features, was operated by making vector quantization technique, which outlined the key points for each training image inside a unified dimensional histogram. They put features of bag-of-word inside multiclass Support Vector Machine (SVM) classifier established upon the radial basis function (RBF) for a training and testing. They used Open CV C++ as an image processing tool and tool for feature extraction. In this paper, we compare the performance of SIFT on SVM based RBF kernel with SURF on SVM based RBF kernel. It was found out that the use of SIFT with SVM-RBF kernel system, it has an accuracy of 98.75% compared that of SURF with SVM-RBF kernel it has an accuracy of 96.25%. The SURF algorithm (speeded up robust transform) is composed mainly two parts. In the first part, locate the interest point in the image. The surf features are calculated and points are matched between the input and out signatures. The surf features are computed and points are matched across the input and out signatures. SURF detectors are looked in the significant points in the image, and descriptors are used to get the feature from vectors at each interest point just as in the SIFT. Hessian-matrix approximation consists of SURF to put through and locate the key points rather than variant aspects of the Gaussians (DOG) filter prepared in SIFT. This algorithm is very much similar to SIFT algorithm. But, it is actually three times faster than SIFT. About 64 dimensions can be used in SURF to save the time consumption for the two traits which are the matching and the computation.

Scale Invariant Feature Transform is one of several computer vision algorithms which is clearly aimed at extracting distinctive and invariant features from images. Features are extracted by making the SIFT algorithm invariant to image scale, rotation, and partially robust to modifying viewpoints and changes in illumination.

In paper [10], we proposed and implemented an innovative approach based on upper and lower envelope and Eigen values techniques. Envelope represents the shape of the signature. The feature set consists of features such as large and small Eigen values computed from upper envelope and lower envelope and its union values. Both the envelopes are combined by performing union operation and their covariance is calculated. The ratios and the differences of high and low points of both these envelopes are calculated. Lastly average values of both the envelopes are obtained. These features set are coupled with support vector machine classifier that lead to 98.5% of accuracy.

In the paper [11] researchers, use this daily based biometric characteristic for identification and classification of students' papers and various exam documents used at University of Mostar. Paper uses a number of Global features, Grid Features, SIFT features. For classification, Support Vector Machine is used and the accuracy obtained is of 88.97%. Global features includes Aspect ratio, number of pixels that belong to the signature, Baseline shift, Global Slant Angle, Number of Edge Points, Number of Cross-Points and Spatial Symbols, Horizontal and vertical Center of gravity, Length name, Length surname, Maximal horizontal and vertical histogram, the length and ratio of Adjacency Columns, Heaviness of signature, Ratio of first vertical pixel to height, Number of Closed Loops.

In paper [12], a bank cheque is taken and the signature is collected from the bank cheque by taking it out by cropping the area of interest. The image is then trained and stored into the trained database using an efficient Feed forward artificial neural network. Then signatures to be tested are compared with the signatures that are stored into the test database. The accuracy of the system is tested out to be 85.00%. In pre-processing, Otsu's thresholding

or binarization algorithm is used which is one of the finest one, allows image object to be separated from its background and later Gaussian low pass filter is applied to remove unwanted noise.

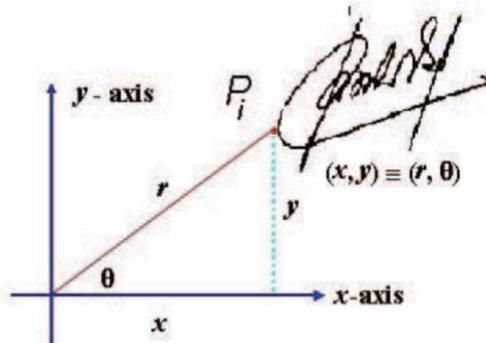
Fuzzy Logic and Artificial Neural Network Based Off-line Signature Verification and Forgery Detection System is presented in paper [13]. As there are distinct and necessary variations in the feature set of each signature, so in order to match a particular signature image with the database image, the structural features of the signatures and also the local feature variations in the signature characteristics are used. The paper suggests that, variation in personality of signatures, because of age, sickness, geographic location and emotional state of the person actuates the problem

A new approach to document image retrieval based on signature is described in paper [14]. The database consists of document images with English text combined with headlines, logo, ruling lines, trade mark and signature. In searching a particular repository of business documents, the actual work to be done is using a query signature image to retrieve from a database. DT-RCWF and DT-CWT are used for extraction features and recognition rate of images is of 79.32%.

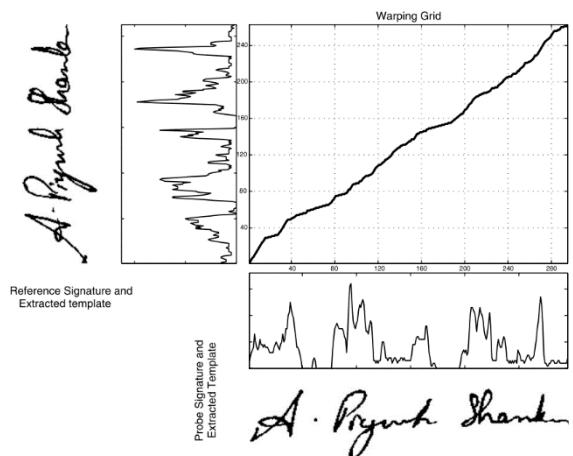
This paper [15] focuses on the pre-processing phase, which is an alternative way to improve the accuracy and to make such factors stable. This research is basically based on the hypothesis that, a table signature size is able to boost up the efficiency which means the recognition rate. Polar Scale Normalization, Adaptive Variance Reduction, Histogram of Oriented Gradients are the techniques used in the system and 98.39% of accuracy is shown.

The pre-processing techniques include Binarization, Complementation, Cropping, and Resizing. The classification of the test data is done using an efficient artificial neural network.

A signature verification system based on Dynamic Time Warping (DTW) is proposed in paper [16]. Pre-processing techniques have Maximum Length Vertical Projection (MLVP) method, Minimum Length Horizontal Projection (MLHP) method. The technique basically works by extracting the vertical projection based features from signature images and by comparing probe and reference feature templates using elastic matching classification. A 98% accuracy is gained and show promising results.

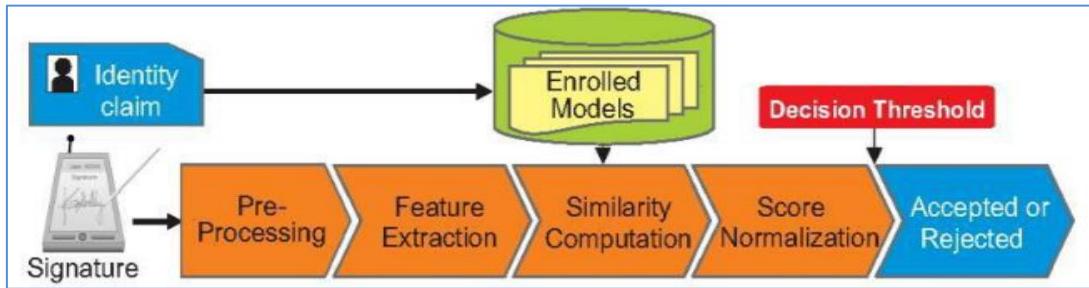


**Figure 6:** Polar scale normalization



**Figure 7:** DTW algorithm of paper [16]

Present paper [17] focuses on different steps including browsing a bank cheque, pre-processing, feature extraction, recognition. The paper extracts and uses features such as Contrast, Homogeneity, Energy and Entropy for comparing two different signature images.



**Figure 8:** Flowchart of paper [17]

SIFT and a SURF algorithm which is used for enhanced offline signature recognition is used in paper [18]. This process, Bag-of-word features, was operated by making vector quantization technique, which outlined the key points for each training image inside a unified dimensional histogram. Accuracy obtained is 98.75%. SVM classification has limitations in speed and size while both phase of try and test of the algorithm and the chosen of the kernel function parameters.

A writer independent offline handwritten signature verification model, also known as global model, for signature verification is proposed in the paper [19]. Otsu's thresholding is used for pre-processing the image. System uses Local Binary Pattern based feature vector extraction along with its variants and classifies the images using SVM. An accuracy of 95.75% is received and the results shown are promising.

An offline signature verification using neural network is projected in paper number [20], where the signature is written on a paper are obtained using a scanner or a camera captured and presented in an image format. In pre-processing, color to grayscale, and finally to black and white, Resizing the image, thinning. Features extracted include Eccentricity, Skewness, Kurtois, Orientation Entropy, Euler number, Solidity, Mean, Standard deviation. The classification is done using a Cascaded feed-forward back-propagation networks and recognition rate of 92.5% is obtained.

System converts a scanned signature to a shape form and Eigen-signature construction is proposed for extracting the feature vector from a shape formed signature. The test feature vector is said to belong to  $i^{\text{th}}$  class, if it possess minimum distance with  $i^{\text{th}}$  class sample when compared to other class samples Thus paper [21] shows accuracy of 91.40%. The pre-processing techniques include binarizing or thresholding. Noise is eliminated using a simple morphological filter, thinned. The test feature vector is said to belong to  $i^{\text{th}}$  class, if it possess minimum distance with  $i^{\text{th}}$  class sample when compared to other class samples.

The purpose in paper number [22] is to select relevant features from those features set. For doing that, researchers compute the importance score of each features using two methods: Information Gain Ratio and Correlation. Over 440 Histogram features, 550 Fresh features, 220 DCT features were extracted an accuracy obtained was 95.5%. Limitations seen are rotation normalization and time normalization. Once all the global features are extracted well, the next trick is ranking these features. Ranking score is obtained from Information Gain Ratio and Correlation. So the result obtained are two list of 1210 features set ranked in order of their Gain. From each list, the features set are then divided into sub features set having 10 first ranked features, 20 first ranked features, 30 first ranked features, and up to 1210 features. So each ranked list will produce sub features set of 121 features.

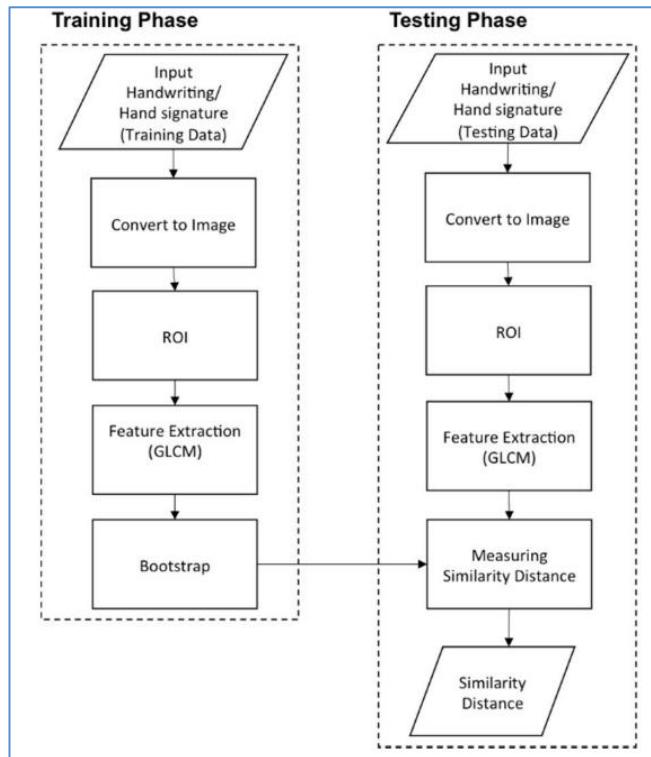
Signature and handwriting recognition on a mobile device using the Gray Level Co-occurrence Matrix (GLCM) for texture-based feature extraction and the bootstrap for performing single classifier model is proposed in the paper [23]. The accuracy obtained is 88.46%.

The paper [24] examines authentication systems based on handwritten signature and the main informative parameters of signature such as size, shape, velocity, pressure, etc. along with DCT, DFT. System using K-Nearest neighbors' algorithm and Random forest algorithm for classification and the accuracy of 95% is shown.

An offline signature recognition system which uses histogram of oriented gradients is presented. Pre-processing techniques used are color normalization, median filtering, angle normalization and exact bounding box, resized into  $256 \times 512$  pixels. Feature extraction is done with Gradient Computation, Gradient Vote, and Normalization Computation. A three layered feedforward backpropagation neural network is used for classification and the recognition rate of paper [25] is 96.87%

In this paper [26], the trace transform based affine invariant features are applied for signature verification. The diametric and trace functions are appropriately chosen to compute a set of circus functions from each signature image. Recognition rate of 76% is obtained. Low accuracy, more invariant functional will be designed for usefulness in signature verification.

This paper [27], deals with the analysis of discriminative powers of the features that can be extracted from an on-line signature, how it's possible to increase those discriminative powers by Dynamic Time Warping as a step in the pre-processing of the signal coming from the tablet. The accuracy obtained is 99.7%. Pre-processing is done using Filtering, equi-



**Figure 9:** Flow Diagram for Paper [23]

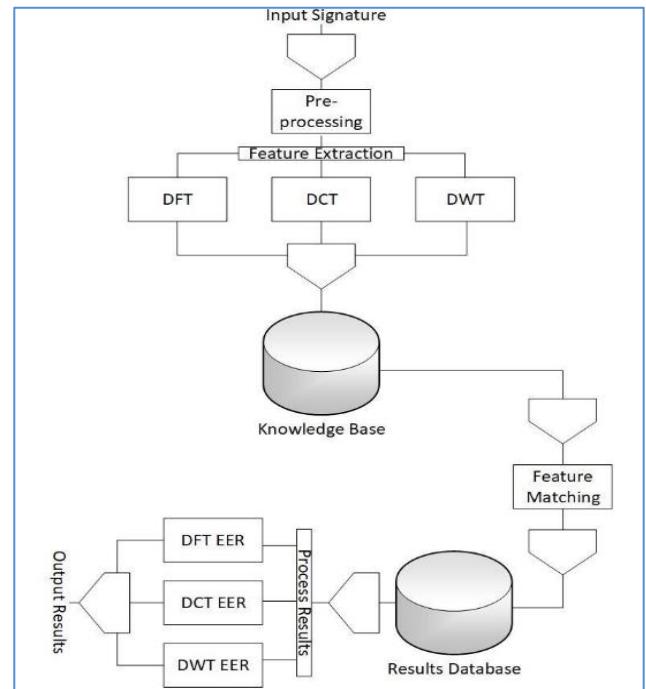
spacing by Linear Interpolation, Normalization, DTW Alignment, Derived Signals: Speed and Acceleration The main processing includes init minus min End minus min Average Root Square Average Time over 0 Crossing 0 Mean over 0 Standard deviation Number of traces, Time of signature, Writing Time of signature / Time of Signature, Height / Width, Area, Length.

Paper [28] uses a texture base approach called the Local binary Pattern algorithm along with SVM, The signature models are trained with genuine signatures on white background and tested with other genuine and forgeries mixed with different backgrounds. Results depict that a basic version of local binary patterns (LBP) or local directional and derivative patterns are more robust than others like GLCM features to the grey level distortion with SVM with histogram oriented kernels as a classifier or rotation invariant uniform LBP. The proposed configurations are checked and evaluated under different situations and conditions: changing the number of training signature images, database with different inks, multiple signing sessions, increasing the number of signers and combining different features. Results have also been provided when looking for the signature in the check and segmenting it automatically. In all these cases, the best results were obtained with the LDerivP feature set, which improve the results obtained in the predefined baseline, showing quite significant improvements with fictitious signature images.

Paper [29] uses Conic section function neural network (CSFNN) circuitry was designed for offline signature recognition. CSFNN is a unified framework for multilayer perceptron (MLP) and radial basis function (RBF) networks and the size of feature vectors was not suitable for designed CSFNN chip structure owing to the input limitations of the circuit. Pre-processing is done using noise reduction algorithm, skeletonization. The few main disadvantages of analog systems include its sensitivity to ambient noise and to temperature. Accuracy shown is 95.5%.

This paper [30] explores the usefulness of local binary pattern (LBP) and local directional pattern (LDP) texture measures to discriminate off-line signatures. Comparison between these several texture normalizations is generated in order to look for reducing pen dependence. The recognition rate is 91.92%. The pre-processing techniques include binarized, cropped, or-exclusive operation, Texture histogram normalization. Least Squares Support Vector Machine (LS-SVM) is applied for classification.

The goal of this study [31] is to investigate the effect of combining transform features to authenticate signatures. Due to genuine human error and lack of consistency, comparing signatures requires pre-processing to assist with standardization. An EER of



**Figure 10:** Flowchart of system in paper [31]

2.46% which means a recognition rate of 99.40% is shown by the system. The features extracted include x coordinate, y coordinate, pen pressure, azimuth, altitude, DFT, DCT and DWT. Classification is done with Fast Dynamic Time Warping (FastDTW) algorithm

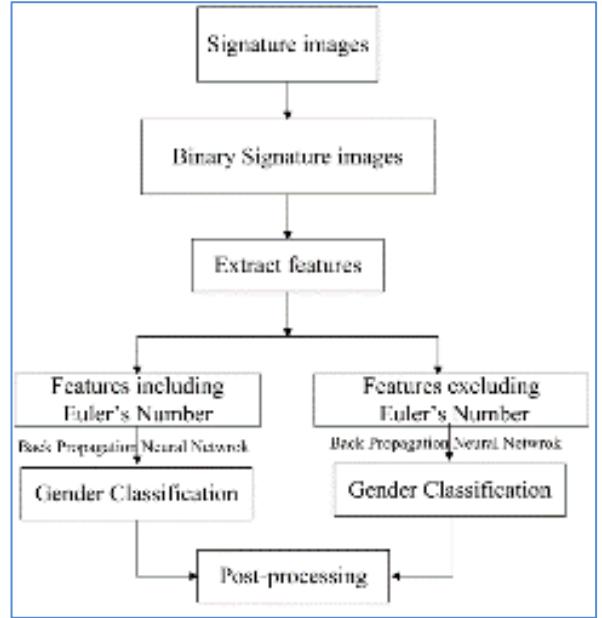
In this paper [32], gender discrimination has been proposed by feature extraction method. The proposed framework considers handwritten Hindi signature of each individuals as an input for gender detection. Recognition rate obtained is 92.90%.

In order to solve the shortcomings of manual identification in technical accuracy and subjectivity, this paper [33] proposed an off-line signature identification method based on Support Vector Machine (SVM). Accuracy shown here is 85.00%. Dataset are stained by useless border. Other pre-processing techniques used in the system include Image binarization, denoising, removing blank margins. Features include global feature like height, width, area and slant angle and sum of black pixels. Identification rates within and between writing systems is prone to swing in some degree under different partitioning strategy.

This paper [34] titled presents a set of geometric signature features for offline automatic Signature verification based on the description of the signature envelope and the interior stroke distribution in polar and Cartesian coordinates. Feature extraction method includes Outline Detection and Representation, Feature Vector Based on Polar Coordinates, Feature Vector Based on Cartesian Coordinates. Classification is performed using The HMM Signature Model, Support Vector Machine Signature Model and Euclidean Distance-Based Signature Model.

The proposed system [35] segments each signature curve based on pen's velocity value. The signature curve, would be decomposed in low or high partition according to velocity's value. For each partition, hand movement direction between two consequent point Extracted. 95.10%. Pre-processing technique here are removing noise, translation invariance, rotation 7 scale invariance. Signature features extracted and used shape of signature would be partitioned based on dynamic feature such as velocity or pressure. Classification is done using Hidden Markov Model.

Optical flow is used to define a stability model of the genuine signatures for each signer in paper [36]. Stability between the unknown signature and reference signatures is estimated and consistency with the stability model of the signer is evaluated. Accuracy obtained is 96.00%. In pre-processing, signature image size was adjusted to a fixed area. Optical flow vectors were used for the analysis of the local stability of a signer to detect the stable regions in the signature. Optical flow vectors are for the analysis of the local stability of a signer to detect the stable regions in the signature.



**Figure 11:** Flow chart of paper [32]

In this paper [37] an efficient off-line signature verification method based on an interval symbolic representation and a fuzzy similarity measure is proposed. 88.26% Local Binary Pattern, interval-valued symbolic model. A histogram-based threshold technique, mean filter for noise removal, minimum bounding boxes. Classification of the signature image is done based on the similarity value, an adaptive writer-dependent acceptance threshold

A new approach of showing online signatures by interval-valued symbolic features. The online signature also gives global features that are to be extracted and used to form an interval-valued feature vectors. Methods for signature verification and recognition based on the symbolic representation are also proposed in paper [38] Recognition rate is 95.40%.

This paper [39] explores the utility of information derived from the dynamic time warping (DTW) cost matrix for the problem of online signature verification. The prior research and experimentations in literature primarily utilize only the DTW scores to authenticate a test signature. Accuracy measured is 97.24%. As the paper itself suggests local features & histogram representation shall be an interesting extension.

This paper [40] presents a new approach for online signature verification that exploits the potential of local stability information in handwritten signatures. Different from previous models, this approach classifies a signature using a multi domain strategy. Accuracy obtained is 97.90%. Both variable and stable regions of a signature image object could be considered for supporting the advanced personalized techniques in signature verification and recognition, since probably, from a behavioural point of view, a variability model of a signer/author could also be very complementary and informative to a stability model.

## 5. Proposed work (algorithm/ techniques/ experimental setup)

### 5.1 Algorithm to be used

The proposed work intends to stretch and extend one of the papers discussed in the above section of literature review which includes the features extraction of Local Binary Pattern from the signature images and to generate an efficient offline signature recognition and verification system. This algorithm is also to be combined with some simple features of the signature image that can have global features that define features of a part or parts of the signature as well as the global features which requires signature as a whole.

At architectural level the basic structure and flow of the system is very much similar to how most of the research finds out. The flowchart block diagram would start with image acquisition where the image would be taken in as input. Then the images would go through series of pre-processing stages such as RGB to Grey, thresholding, Boundary Box cropping and noise removal filters. In feature extraction stage different set of shape and size based are to be extracted. The images are then converted to LBP images and all the texture based LBP features are extracted again but this time from the LBP images. The generated feature set of all the images along with their respective classes would be given to a classification algorithm. This currently has K-nearest neighbors using Euclidian distance based approach and can be combined with another to increase accuracy. Finally this stage would give out the class to which the input test image belongs to as output decision class.

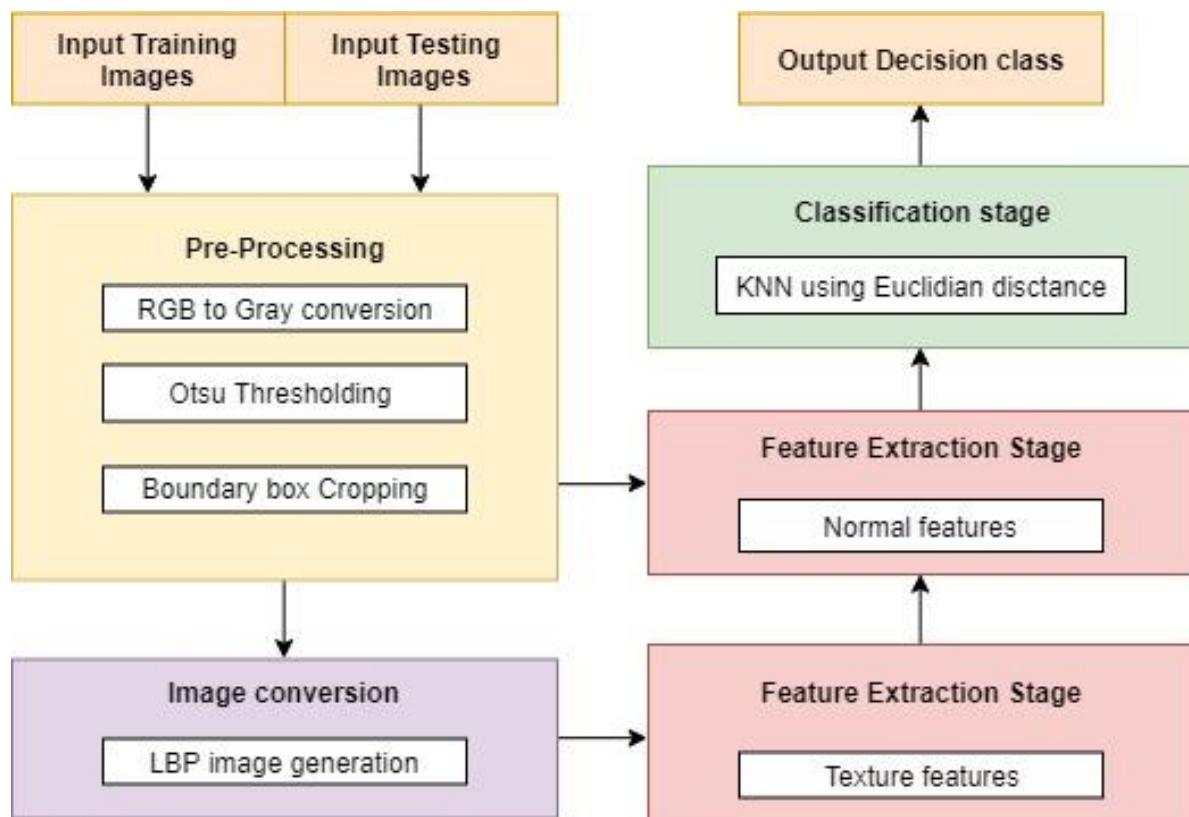


Figure 12: Block diagram of the proposed approach

## 5.2 Otsu thresholding

In global thresholding, we used an arbitrary value for threshold value, right? So, how can we know a value we selected is good or not? Answer is, trial and error method. But consider a **bimodal image** (*In simple words, bimodal image is an image whose histogram has two peaks*). For that image, we can approximately take a value in the middle of those peaks as threshold value, right? That is what Otsu binarization does. So in simple words, it automatically calculates a threshold value from image histogram for a bimodal image. (For images which are not bimodal, binarization won't be accurate.)

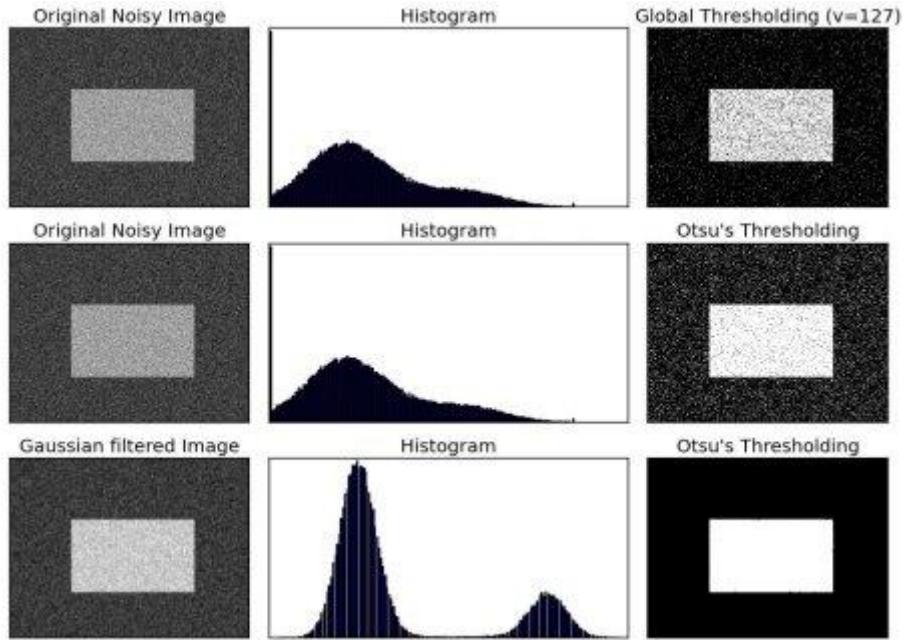
For this, our **`cv.threshold()`** function is used, but pass an extra flag, **`cv.THRESH OTSU`**. **For threshold value, simply pass zero.** Then the algorithm finds the optimal threshold value and returns you as the second output, `retVal`. If Otsu thresholding is not used, `retVal` is same as the threshold value you used.

Check out below example. Input image is a noisy image. In first case, I applied global thresholding for a value of 127. In second case, I applied Otsu's thresholding directly. In third case, I filtered image with a 5x5 gaussian kernel to remove the noise, then applied Otsu thresholding. See how noise filtering improves the result.

### Algorithm

1. Compute histogram and probabilities of each intensity level
2. Set up initial  $\omega_{\{i\}(0)}$  and  $\mu_{\{i\}(0)}$
3. Step through all possible thresholds  $\{t=1, \dots\}$  maximum intensity
4. Update  $\omega_{\{i\}}$  and  $\mu_{\{i\}}$
5. Compute  $\sigma_b^2(t)$
6. Desired threshold corresponds to the maximum  $\sigma_b^2(t)$

Otsu's method exhibits the relatively good performance if the histogram can be assumed to have bimodal distribution and assumed to possess a deep and sharp valley between two peaks. But if the object area is small compared with the background area, the histogram no longer exhibits bimodality.<sup>[4]</sup> And if the variances of the object and the background intensities are large compared to the mean difference, or the image is severely corrupted by additive noise, the sharp valley of the gray level histogram is degraded. Then the possibly incorrect threshold determined by Otsu's method results in the segmentation error.



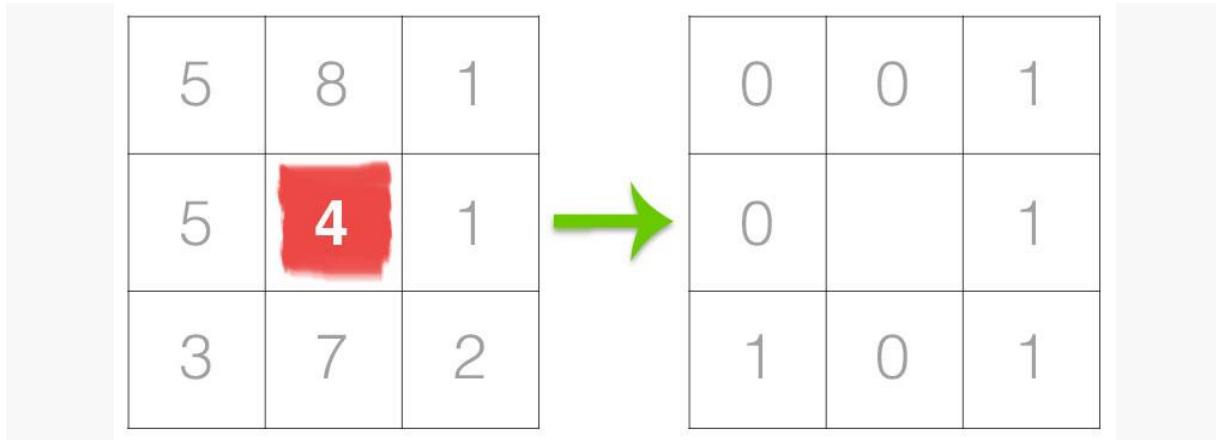
**Figure 13:** Different thresholding methods.

## 5.2 Local Binary Patterns

Local Binary Patterns, or LBPs for short, are a texture descriptor made popular by the work of Ojala et al. in their 2002 paper, [Multiresolution Grayscale and Rotation Invariant Texture Classification with Local Binary Patterns](#) (although the concept of LBPs were introduced as early as 1993).

Unlike [Haralick texture features](#) that compute a global representation of texture based on the [Gray Level Co-occurrence Matrix](#), LBPs instead compute a local representation of texture. This local representation is constructed by comparing each pixel with its surrounding neighborhood of pixels.

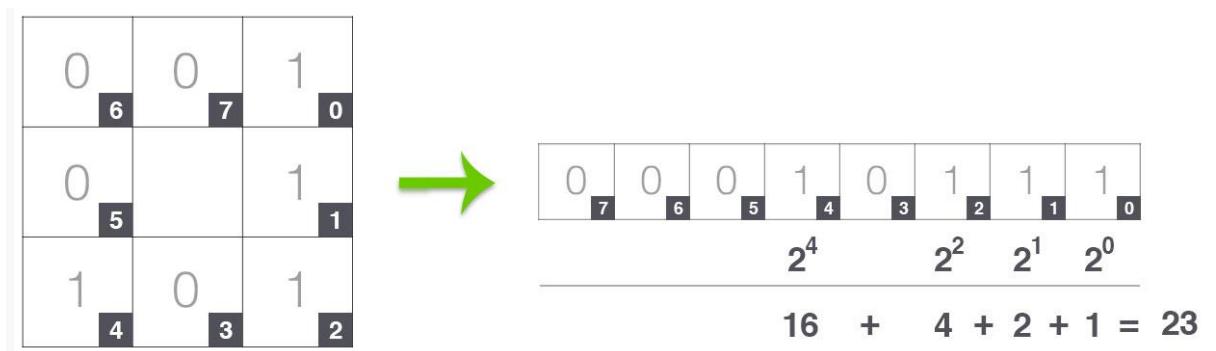
The first step in constructing the LBP texture descriptor is to convert the image to grayscale. For each pixel in the grayscale image, we select a neighborhood of size  $r$  surrounding the center pixel. A LBP value is then calculated for this center pixel and stored in the output 2D array with the same width and height as the input image. For example, let's take a look at the original LBP descriptor which operates on a fixed  $3 \times 3$  neighborhood of pixels just like this:



**Figure 14:** The first step in constructing a LBP.

In the above figure we take the center pixel (highlighted in red) and threshold it against its neighborhood of 8 pixels. If the intensity of the center pixel is greater-than-or-equal to its neighbor, then we set the value to 1; otherwise, we set it to 0. With 8 surrounding pixels, we have a total of  $2^8 = 256$  possible combinations of LBP codes.

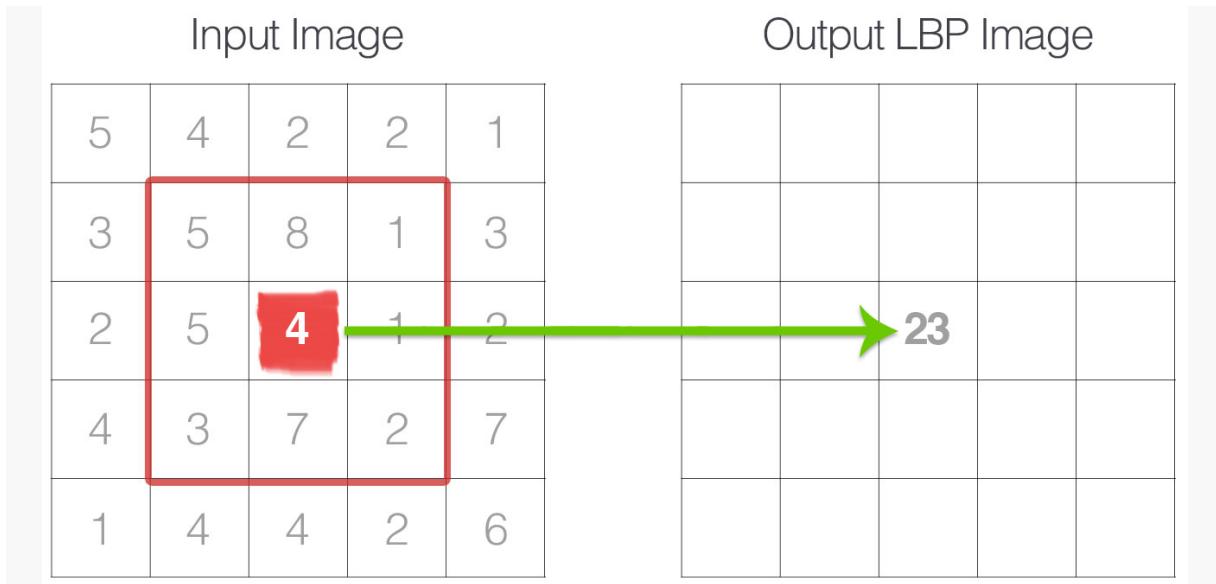
From there, we need to calculate the LBP value for the center pixel. We can start from any neighboring pixel and work our way clockwise or counter-clockwise, but our ordering must be kept consistent for all pixels in our image and all images in our dataset. Given a  $3 \times 3$  neighborhood, we thus have 8 neighbors that we must perform a binary test on. The results of this binary test are stored in an 8-bit array, which we then convert to decimal, like this:



**Figure 15:** The second step in constructing a LBP.

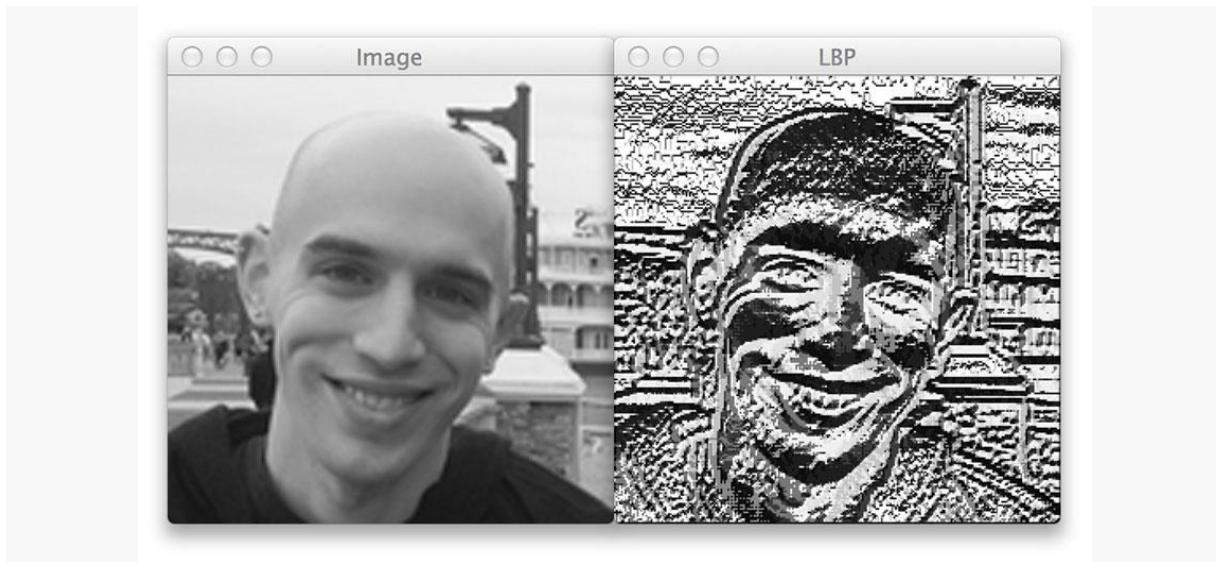
In this example we start at the top-right point and work our way **clockwise** accumulating the binary string as we go along. We can then convert this

binary string to decimal, yielding a value of 23. This value is stored in the output LBP 2D array, which we can then visualize below:



**Figure 16:** The third step in constructing a LBP.

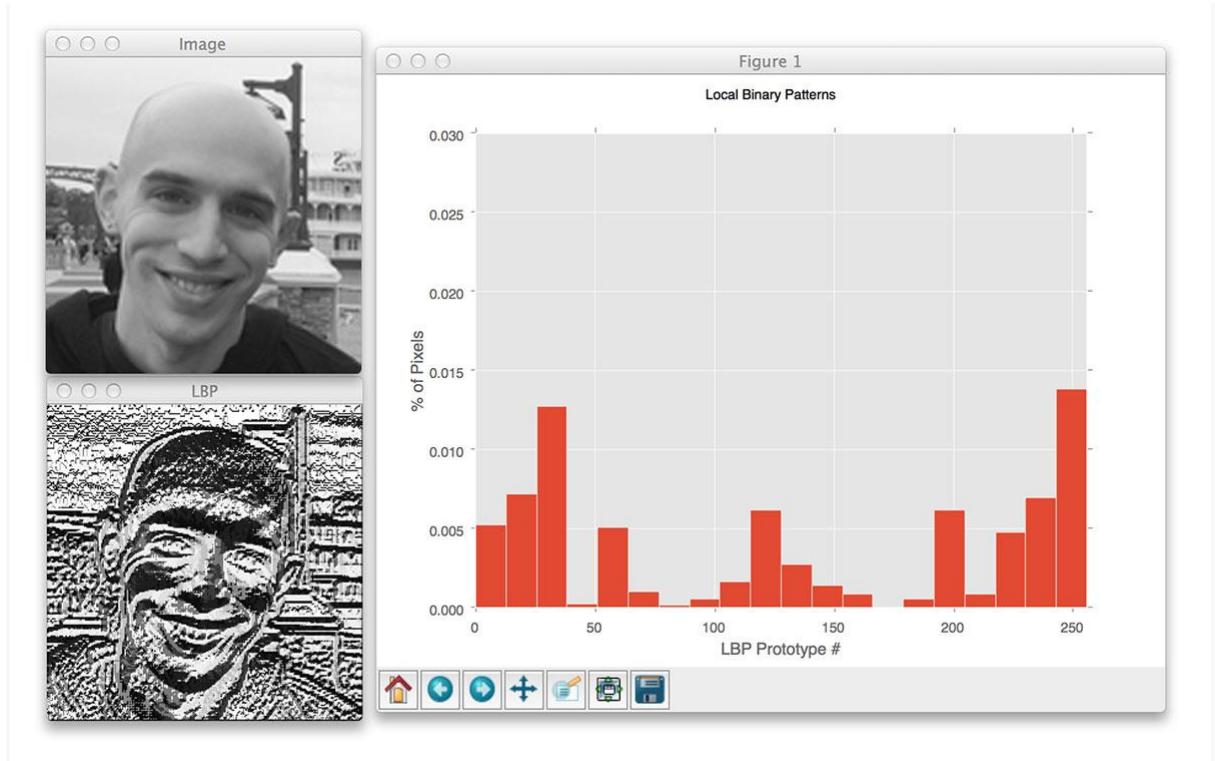
This process of thresholding, accumulating binary strings, and storing the output decimal value in the LBP array is then repeated for each pixel in the input image. Here is an example of computing and visualizing a full LBP 2D array:



**Figure 17:** Computing the LBP representation (right) from the original input image (left).

The last step is to compute a histogram over the output LBP array. Since a  $3 \times 3$  neighborhood has  $2^8 = 256$  possible patterns, our LBP 2D array thus has a minimum

value of 0 and a maximum value of 255, allowing us to construct a 256-bin histogram of LBP codes as our final feature vector:



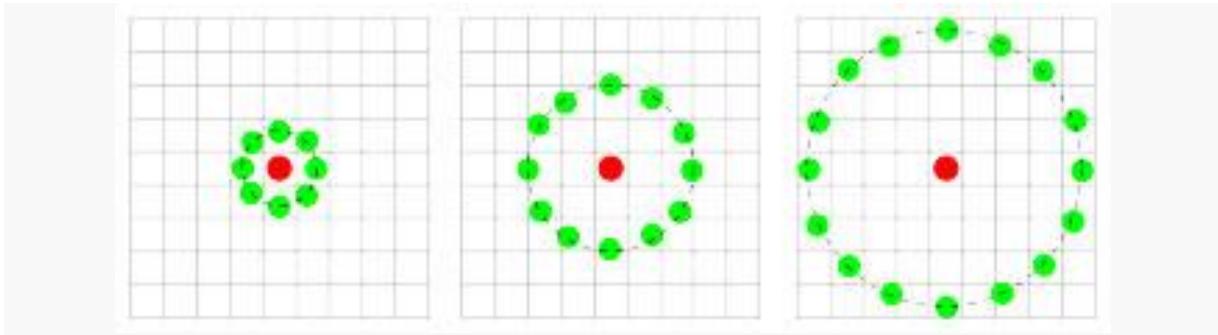
**Figure 18:** Histogram for LBP image

A primary benefit of this original LBP implementation is that we can capture extremely fine-grained details in the image. However, being able to capture details at such a small scale is also the biggest drawback to the algorithm — we cannot capture details at varying scales, only the fixed  $3 \times 3$  scale!

To handle this, an extension to the original LBP implementation was proposed by Ojala et al. to handle variable neighborhood sizes. To account for variable neighborhood sizes, two parameters were introduced:

1. The number of points  $p$  in a circularly symmetric neighborhood to consider (thus removing relying on a square neighborhood).
2. The radius of the circle  $r$ , which allows us to account for different scales.

Below follows a visualization of these parameters:



**Figure 19:** Three neighborhood examples with varying  $p$  and  $r$  used to construct Local Binary Patterns.

Lastly, it's important that we consider the concept of LBP **uniformity**. A LBP is considered to be uniform if it has **at most** two 0-1 or 1-0 transitions. For example, the pattern 00001000 (2 transitions) and 10000000 (1 transition) are both considered to be **uniform patterns** since they contain at most two 0-1 and 1-0 transitions. The pattern 01010010 on the other hand is not considered a uniform pattern since it has six 0-1 or 1-0 transitions.

The number of uniform prototypes in a Local Binary Pattern is completely dependent on the number of points  $p$ . As the value of  $p$  increases, so will the dimensionality of your resulting histogram. Please refer to the original Ojala et al. paper for the full explanation on deriving the number of patterns and uniform patterns based on this value. However, for the time being simply keep in mind that given the number of points  $p$  in the LBP there are  $p + 1$  **uniform patterns**. The final dimensionality of the histogram is thus  $p + 2$ , where the added entry tabulates all patterns that are **not uniform**.

So why are uniform LBP patterns so interesting? Simply put: they add an extra level of rotation and grayscale invariance, hence they are commonly used when extracting LBP feature vectors from images.

## 5.2 K-Nearest Neighbours

K-Nearest Neighbors is one of the most basic yet essential classification algorithms in Machine Learning. It belongs to the supervised learning domain and finds intense application in pattern recognition, data mining and intrusion detection.

It is widely disposable in real-life scenarios since it is non-parametric, meaning, it does not make any underlying assumptions about the distribution of data (as opposed to other algorithms such as GMM, which assume a Gaussian distribution of the given data).

We are given some prior data (also called training data), which classifies coordinates into groups identified by an attribute.

As an example, consider the following table of data points containing two features:

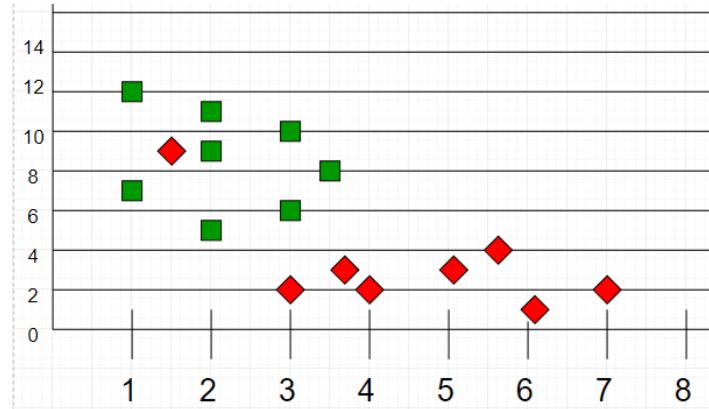


Figure 20: data points set 1

Now, given another set of data points (also called testing data), allocate these points a group by analyzing the training set. Note that the unclassified points are marked as ‘White’.

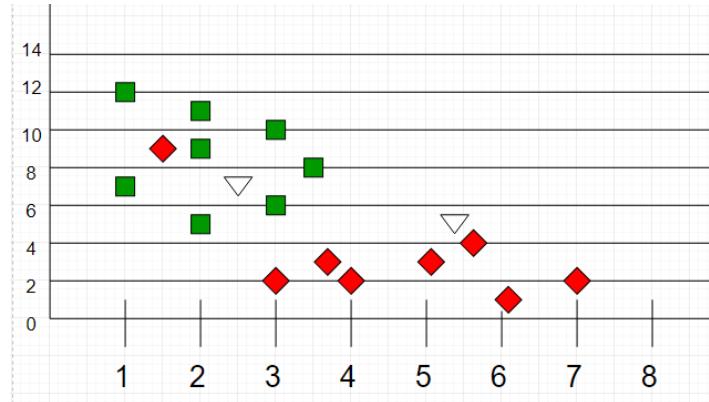


Figure 21: data points set 2

## Intuition

If we plot these points on a graph, we may be able to locate some clusters, or groups. Now, given an unclassified point, we can assign it to a group by observing what group its nearest neighbours belong to. This means, a point close to a cluster of points classified as ‘Red’ has a higher probability of getting classified as ‘Red’.

Intuitively, we can see that the first point (2.5, 7) should be classified as ‘Green’ and the second point (5.5, 4.5) should be classified as ‘Red’.

## Algorithm

Let ‘m’ be the number of training data samples. Let p be an unknown point.

1. Store the training samples in an array of data points arr[]. This means each element of this array represents a tuple (x, y).
2. for i=0 to m:
3.     Calculate Euclidean distance d(arr[i], p).
4. Make set S of K smallest distances obtained. Each of these distances correspond to an already classified data point.
5. Return the majority label among S.

## 5.2 Implementation tools end setup

There are many implementation programming tools that can be used for image Processing and Machine learning projects like MATLAB. This project will also require a database and an interface between the programming tool and the database.

### 5.2.1 Python using PyCharm

Implementation programming tool to be used here is Python. Python is powerful... and fast; plays well with others, runs everywhere, is friendly & easy to learn and is Open. It is a popular programming language used in web development (server-side), software development, mathematics, system scripting.

- Python can be easy to pick up whether you're a first time programmer or you're experienced with other languages. The following pages are a useful first step to get on your way writing programs with Python!
- The Python Package Index (PyPI) hosts thousands of third-party modules for Python. Both Python's standard library and the community-contributed modules allow for endless possibilities.

Contains number of libraries, which are easy to install & import...

- OpenCV : Computer vision and machine learning software library.
- NumPy : Scientific computing & array-processing
- Imutils : Functions to make basic image processing functions easier
- Math : Provides access to the mathematical functions
- Matplotlib : Python 2D plotting library
- Pymysql : A simple database interface for Python
- OS : allows easy file handling
- Scipy : Provides many user-friendly and efficient numerical routines
- PySimpleGUI : User interface renderer

PyCharm is a python editor and compiler. Allow to be more productive by saving time while PyCharm takes care of the routine. Allows to focus on the bigger things and embrace the keyboard-centric approach to get the most of PyCharm's many productivity features.

Get Smart Assistance with PyCharm that knows everything about our code. We can always rely on it for intelligent code completion, on-the-fly error checking and quick-fixes, easy project navigation, and much more.

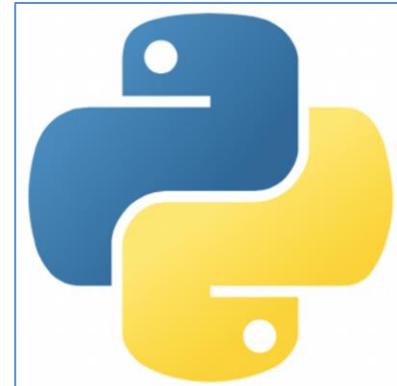


Figure 22: Python logo



Figure 23: PyCharm logo

### 5.2.2 Database using MySQL

A **database** is a collection of information that is organized so that it can be easily accessed, managed and updated. Data is organized into rows, columns and tables, and it is indexed to make it easier to find relevant information. A database is a separate application that stores a collection of data. Each database has one or more distinct APIs for creating, accessing, managing, searching and replicating the data it holds. Other kinds of data stores can also be used, such as files on the file system or large hash tables in memory but data fetching and writing would not be so fast and easy with those type of systems.

So in this project we are going to deal with a lot of data such as training features, testing features and also classes etc. So to store and reuse the data from somewhere, we are going to need a database.

SQL is a standard language for storing, manipulating and retrieving data in databases. It is a database computer language designed for the retrieval and management of data in a relational database. SQL stands for Structured Query Language. SQL is the standard language for Relational Database System. All the Relational Database Management Systems (RDBMS) like MySQL, MS Access, Oracle, Sybase, Informix, Postgres and SQL Server use SQL as their standard database language.

MySQL is the most popular Open Source Relational SQL Database Management System. MySQL is one of the best RDBMS being used for developing various web-based software applications. MySQL is developed, marketed and supported by MySQL AB, which is a Swedish company.

MySQL is a fast, easy-to-use RDBMS being used for many small and big businesses. MySQL is developed, marketed and supported by MySQL AB, which is a Swedish company.



Figure 24: SQL logo



Figure 25: MySQL logo

## 6 Work done

### 6.1 Research

The work done includes further research of the related research papers to explore more and more about in depth knowledge of the existing algorithms that can be used for signature recognition and verification. The research allowed me to read more research papers on one of the algorithm that I have finalized to use, Local Binary Pattern based approach. Along with finalization of the algorithm, I have read and also studied more number of research papers based on Signature Recognition and Verification and an excel sheet of all the Literature Review has been prepared. The literature review contains total of 40 research papers based on the topic Signature Recognition. Most of the papers make use of 3 stages: Preprocessing stage, Feature extraction stage, Classification stage.

### 6.2 Dataset preparation

The work also includes dataset preparation include downloading more and more of the online available datasets that people around the world generate and upload for others to use. I have thus downloaded the dataset from the Web.

The signature verification system would need a set of image dataset having handwritten signatures from different authors. The data set prepared was taken from web uploaded by researchers online on the website [42]. The CEDAR signature dataset is one of the benchmark datasets for signature verification. Since the dataset downloaded is vast and contains a lot of images we have prepared a subset of the vast dataset and kept aside directory of folders of images which contains total 26 Authors, all having genuine as well as forged signatures and thus 52 different classes.

The dataset is divided in an approximate ratio of 4:1 for preparing training and testing data respectively. Therefore 988 training images and 260 testing images kept in two different folders combine to a total of 1248 images.

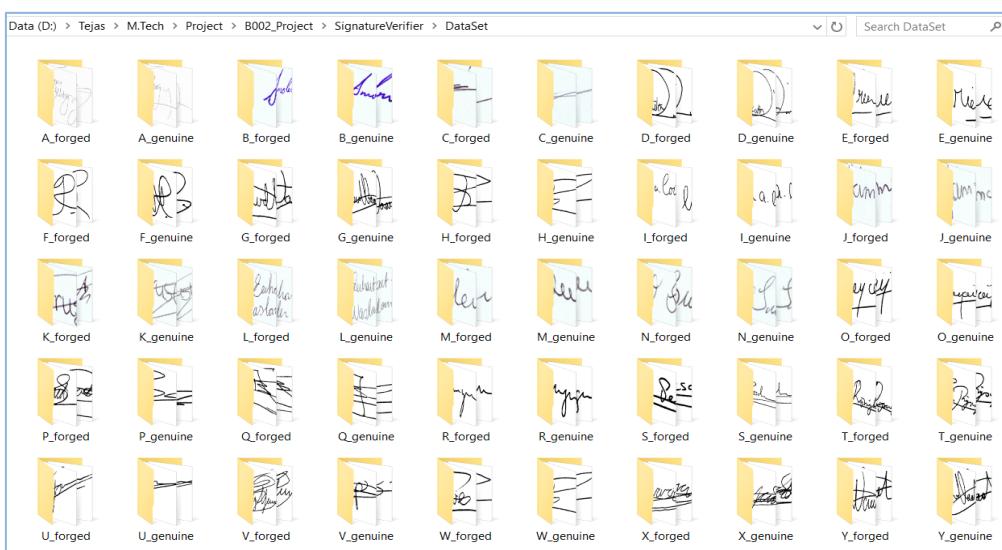
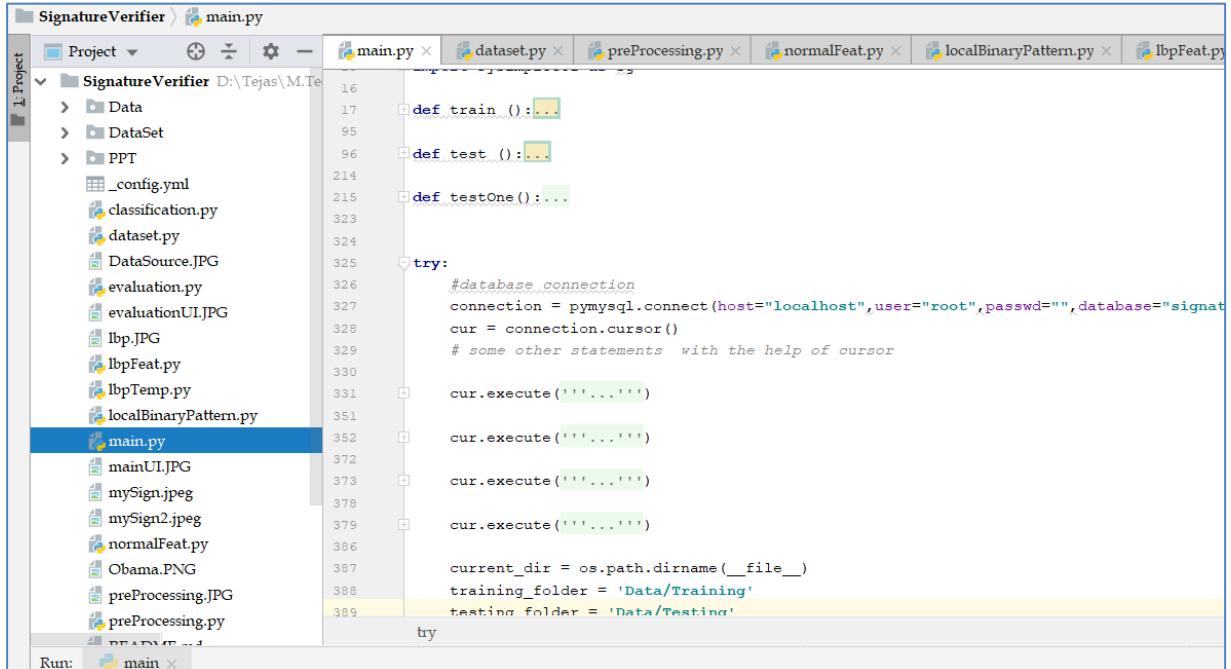


Figure 26: Dataset prepared

### 6.3 Implementation

Implementing with python includes total of 8 python.py files and an SQL file created in PyCharm that can be viewed as below Preprocessing stage that have been implemented include reading the image resizing, grayscale, denoising, threshold based segmentation, boundary box generation displaying the image



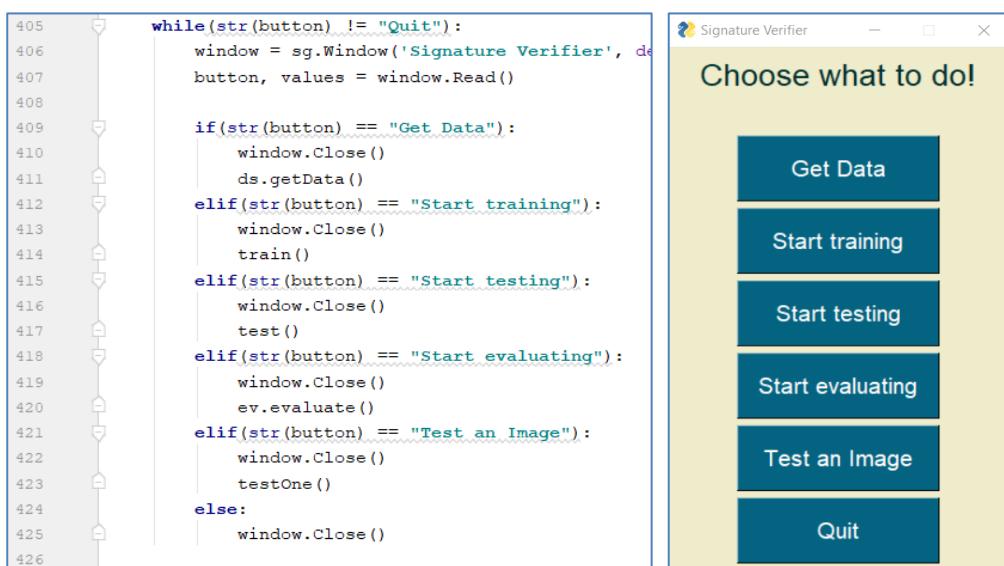
The screenshot shows the PyCharm interface with the project 'SignatureVerifier' open. The left sidebar shows the project structure with files like Data, DataSet, PPT, and several Python files. The main editor window displays the 'main.py' file, which contains Python code for database operations and file paths. The code includes imports for MySQL and os, and defines functions for training, testing, and testOne. The code is color-coded for syntax.

```
16
17     def train():
18
19     def test():
20
21     def testOne():
22
23     try:
24         #database connection
25         connection = pymysql.connect(host="localhost", user="root", passwd="", database="signature")
26         cur = connection.cursor()
27         # some other statements with the help of cursor
28
29         cur.execute(''')
30             ...
31         ''')
32         cur.execute(''')
33             ...
34         ''')
35         cur.execute(''')
36             ...
37         ''')
38         cur.execute(''')
39             ...
40         ''')
41
42         current_dir = os.path.dirname(__file__)
43         training_folder = 'Data/Training'
44         testing_folder = 'Data/Testing'
```

Figure 27: Python program files prepared in PyCharm

#### 6.3.1 Main.py

The entire system is controlled from the main function which is inside the main.py. This is the main python file where the system working starts, calls the other functions, gives the appropriate results and ends.



The screenshot shows the 'Main.py' code on the left and its corresponding graphical user interface (GUI) on the right. The code is a part of a larger script, likely a Tkinter application. It initializes a window titled 'Signature Verifier' and enters a loop to handle button events. The GUI window is titled 'Choose what to do!' and contains seven buttons: 'Get Data', 'Start training', 'Start testing', 'Start evaluating', 'Test an Image', and 'Quit'. Each button is represented by a blue rectangular button with white text.

```
405     while(str(button) != "Quit"):
406         window = sg.Window('Signature Verifier', [...])
407         button, values = window.Read()
408
409         if(str(button) == "Get Data"):
410             window.Close()
411             ds.getData()
412         elif(str(button) == "Start training"):
413             window.Close()
414             train()
415         elif(str(button) == "Start testing"):
416             window.Close()
417             test()
418         elif(str(button) == "Start evaluating"):
419             window.Close()
420             ev.evaluate()
421         elif(str(button) == "Test an Image"):
422             window.Close()
423             testOne()
424         else:
425             window.Close()
```

Figure 28: Main.py and GUI

Following buttons are displayed on the main menu screen:

- Get data: This button will call the ‘getData’ function from Dataset.py which is used for analyzing and organizing our image dataset.
- Start Training: This function goes through all other functions of pre-processing, feature extraction of all the training images and also inserts the feature vector and class data in to our database.
- Start Testing: This function goes through all other functions of pre-processing, feature extraction and also classification of all the testing images and also inserts the feature vector and class data in to our database.
- Start Evaluation: This button will evaluate our system and find the accuracy.
- Test an Image: Clicking on this button will display a popup form and allow user to browse through his computer and perform testing over a single image.



Figure 29: Test An image UI

- Quit: This will exit the system and end execution

### 6.3.2 Dataset.py

This file has a ‘getData()’ function that writes a ‘dataAnalysis.txt’ where it gives an analysis of all the data and the count of all the dataset.

26 Authors, 1248 Images  
988 Training images (79.17%)  
260 Testing images (20.83%)

Figure 30: dataAnalysis.txt

The images of our dataset are renamed in the correct naming convention, copied and organized to a different folder, from where our system will use. For instance: ‘xyz.png’ is renamed to ‘A\_orig\_7.png’. Here ‘A’ is the Author, ‘orig’ means that the image is genuine signed by author, ‘A’ and 7 is just a number appended to keep the image name unique within the folder. This name is also used as a primary key of all the tables in our database.

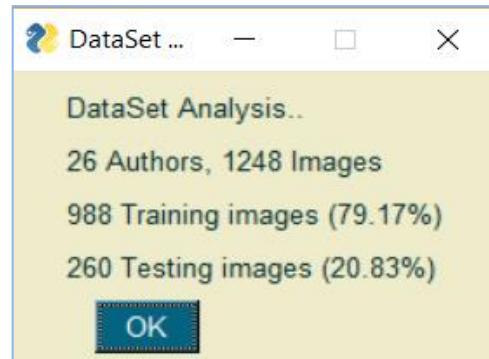


Figure 31: DataSet analysis popup UI

```

imagestry=1
exists = os.path.isfile("DataSet/" + folder + "/" + folder + "_" + str(j) + ".png")
if not exists:
    os.rename("DataSet/" + folder + "/" + file, "DataSet/" + folder + "/" + folder + "_" + str(j) + ".png")

dataFolder = training_folder if (j < (4*total/5)) else testing_folder
dataexists = os.path.isfile(dataFolder + "/" + folder + "_" + str(j) + ".png")
if not dataexists:
    shutil.copy("DataSet/" + folder + "/" + folder + "_" + str(j) + ".png", dataFolder)

```

Figure 32: Dataset.py

### 6.3.3 PreProcessing.py

This function takes the image in the raw format and converts it into a pre-processed format. This will make the image ready for processing. Preprocessing stage that have been implemented include reading the image resizing, RGB to Grey conversion, de-noising, threshold based segmentation, boundary box generation.

The binarization or also called as thresholding is method which converts a grey image into a black and white image. This is done using a threshold and hence the name Thresholding. But a problem in thresholding is finding the correct threshold and thus we use an advanced thresholding technique called the Otsu's thresholding. The Otsu's thresholding method involves iterating through all the possible threshold values and calculating a measure of spread for the pixel levels each side of the threshold, i.e. the pixels that either fall in foreground or background. The aim is to find the threshold value where the sum of foreground and background spreads is at its minimum. We can see from the adjoining image how the threshold must vary for different images having different histograms.

The boundary box cropping is one of the preprocessing stages that was not a predefined function so I got the liberty to create it myself. Its general idea is to remove the white spaces from all four sides of the image and make the problem a little smaller. The idea here was to simply keep cropping out all the rows until we find the first black pixel from top and bottom and do the same for columns from both the sides.

After few of the preprocessing stages the signature image would become a lot cleaner without noise and ready to be used for further processing. Following image shows the same.

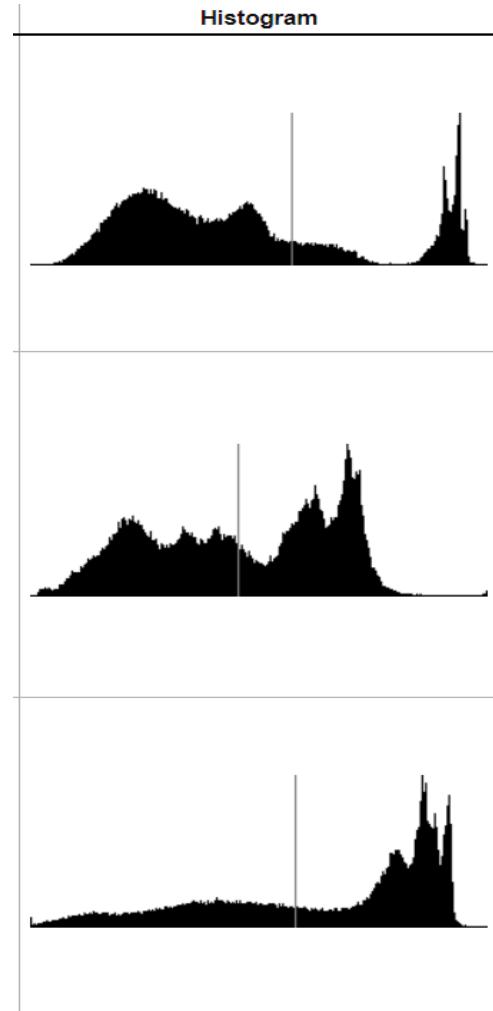


Figure 33: Varying thresholds

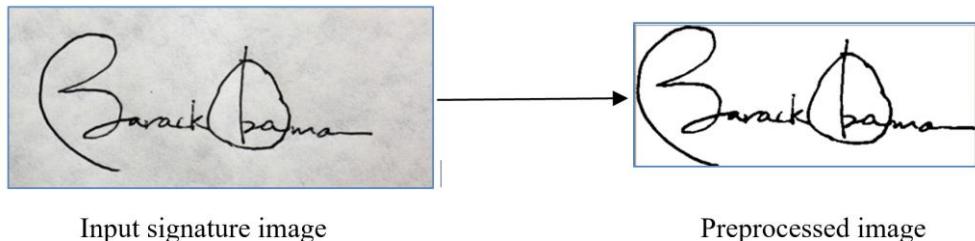


Figure 34: Preprocessing signature image

### 6.3.4 NormalFeat.py

Feature extraction stage means to take out numeric values out of the image so that an algorithmic process can compare them and in turn compare the image. We can use a feature set having a huge number of features but that will not do any good if their impact is not much over their image. Thus we narrow down to a feature vector set having 16 features which includes 8 normal features and 8 texture features. The pre-processed image is used for taking out normal features and LBP image is given to extract texture features.

The following image shows the PySimpleGui progress bar for our training period for over 1000 images.

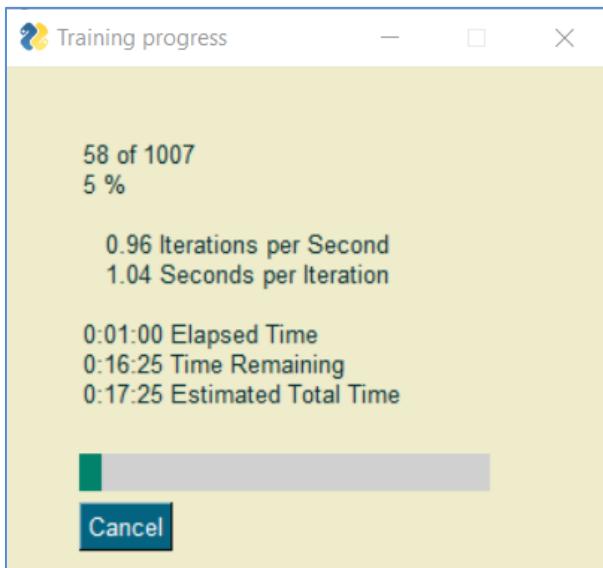


Figure 35: Progress meter bar GUI while training and testing

The normal shape based features that are extracted from the pre-processed image are given below and are also shown on the above image:

1. Aspect Ratio: The ratio of the width to the height of an image or screen.
2. Center of Gravity - X: The Center of Gravity or Center of Mass statistic calculates where the COG of the image lies. The COG of X is calculated by:  

$$\text{COG\_X} = \text{COG\_X} + (I*x)$$
3. Center of Gravity - Y: The Y- Center of Gravity :  

$$\text{COG\_Y} = \text{COG\_Y} + (I*y)$$

4. Baseline Shift: This depicts which side (left or right) is the signature waited more and by how much. Calculated difference of left and right COG\_Y.
5. Energy: the sum of square elements in GLCM
6. Dissimilarity: the weights with which GLCM probabilities are multiplied increase linearly away from the diagonal
7. Haralick: describe the overall texture of the image using measures
8. Kurtosis: Kurtosis is a measure of the combined weight of a distribution's tails relative to the center of the distribution

```

~~~ Normal features ~~~
Aspect Ratio : 2.402135231316726
X_COG: 338.5539421701799
Y_COG: 140.53258886252678
Baseline shift: 0.7266805826126017
Energy: 0.958966395847317
Dissimilarity: 1.9347761808716222
Haralick: 950.8804485905165
Kurtosis: 28.81512693799091

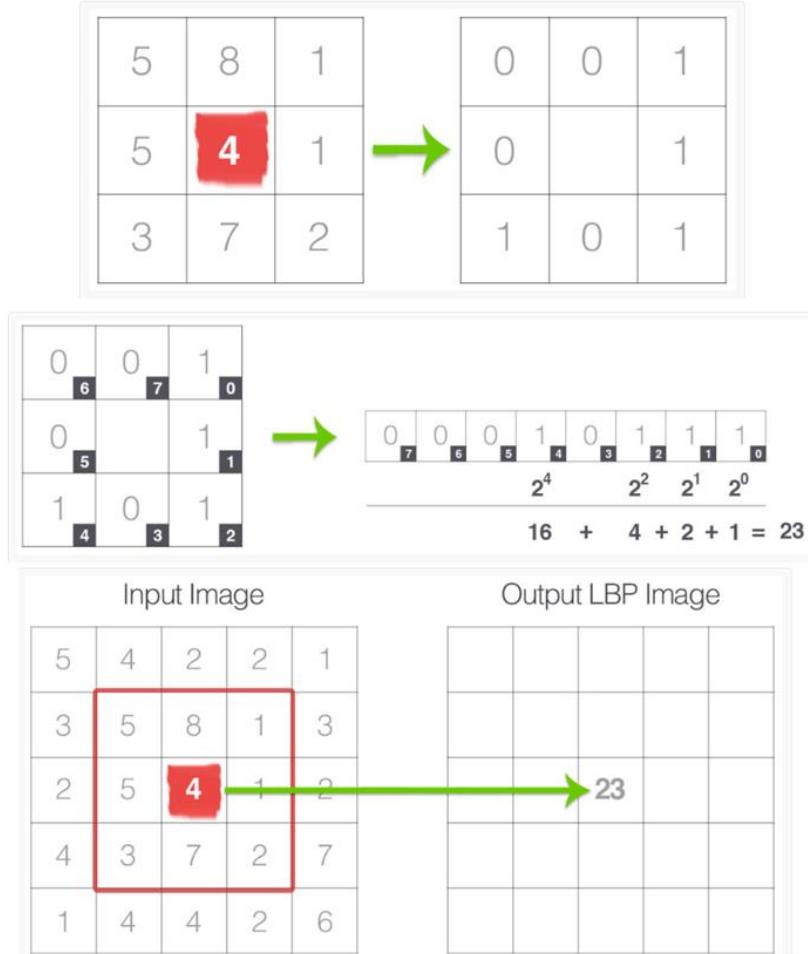
```

Figure 36: Normal features printed on console

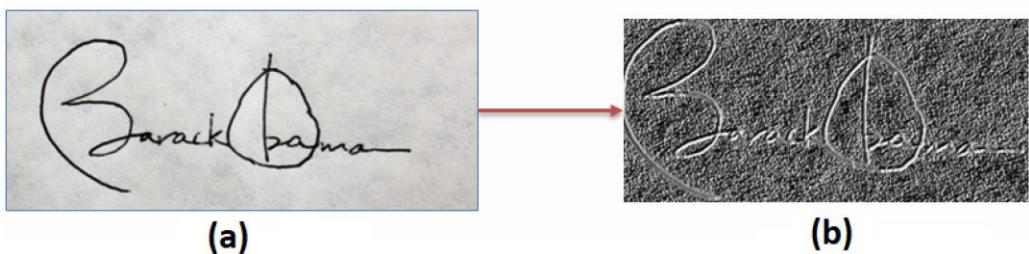
### 6.3.5 LocalBinaryPattern.py

This python file contains function that converts the image to an LBP image which stands for Local Binary Pattern. The code in the image convert the image into LBP image which is darker and shows off the textures of the image to help us extract them. LBP stands for Local Binary Pattern. The grey image is converted to a LBP image in this stage. This LBP image is dark in colour and is very much useful to extract texture based features out of the image.

The first step in constructing a LBP is to take a 3x3 mask the 8 pixel neighbourhood surrounding a centre pixel. We start from upper left corner, and threshold the surrounding 8 pixel with the centre pixel. The one pixel having higher intensity than the centre pixel is set to 0 and one lesser than the centre pixel is set to 1. This mask is then read in a clockwise manner to construct a set of 8 binary digits. Taking the 8 bit binary number, we convert it into a decimal representation. This decimal number is nothing but our LBP value which is set in our LBP image with the same width and height as the original image for the same (x,y) pixel. The mask is then moved ahead in the image and the process repeats. We can refer the above image which shows the steps with an example. The below image shows an original image and its LBP image form.



**Figure 37:** LBP image conversion algorithm



**Figure 38:** LBP image conversion:  
(a) Grey image; (b) LBP image

To obtain better results in this, we perform variations in the LBP algorithm. We can keep the starting pixel as any of the 8 neighbor pixels for both clockwise and anti-clockwise reading of the binarized number. This gives us 16 different variants of LBP conversion that can be tested in our system later for which the accuracy is highest.

Thus we will have following 16 different variants for our LBP implementation based on the starting point or the leftmost pixel as starting for reading

- TL – Top Left : x-1, y-1
- T – Top : x, y-1
- TR – Top Right : x+1, y-1
- R – Right : x+1, y
- BR – Bottom Right : x+1, y+1
- B – Bottom : x, y+1
- BL – Bottom Left : x-1, y+1
- L – Left : x-1, y

x-1, y-1	x, y-1	x+1, y-1
x-1, y	x, y	x+1, y
x-1, y+1	x, y+1	x+1, y+1

Figure 39: 8-neighbour pixels

### 6.3.6 LbpFeat.py

The LBP texture based features that are extracted from the LBP image are given below:

9. Contrast: measure of the intensity contrast between a pixel and its neighbor over the whole image
10. Normalized Area: The amount of darker pixels that constitute the object in the image divided by the total size (no of pixels) in the image.
11. Homogeneity: value that calculates the tightness of distribution of the elements in the GLCM to the GLCM diagonal
12. Energy: the sum of square elements in GLCM
13. Dissimilarity: Dissimilarity measure of LBP image
14. Haralick: Haralick feature of LBP image
15. Skewness: asymmetry in a statistical distribution, in which the curve appears distorted or skewed either to the left or to the right
16. Kurtosis: Kurtosis measure of LBP image

```
~~~ LBP features ~~~
Contrast: 17.679818216493544
Normalized area: 4.2712653288740245
Homogeneity: 0.8302425919185281
Energy: 0.6608064821892133
Dissimilarity: 1.0182713821221416
Haralick: 157.50156224641563
Skewness: -5.43953922460237
Kurtosis: 33.18020199220615
```

Figure 40: LBP texture features printed on console

### 6.3.7 Classification.py

The learning of the system would be dependent heavily on a supervised base learning, which means that the training set images must have the class information in some form. Here I have renamed the training set images in such a way that the name will define the class it belongs to. The python code will first read all the images in the given directory and get the class of each based on its name. Since we have 25 authors each having forged and genuine signatures, we currently have a total of 50 classes.

For example, an image file has a name A\_forged\_21.png. Its actual class would be ‘A\_forg’. This means that the signature image belongs to author A and is a forged one.

The classifier we have used is KNN which stands for k-nearest neighbours. It is basically a classification algorithm that means it assigns a class to a test image based on its feature values. The k-nearest neighbours’ algorithm uses Euclidian distance method to find the distance between two training points. Thus using Euclidian distance we find k nearest neighbouring training points of our test point based on its features and the class with maximum number of occurrences is taken as the decision class for that test image and is assigned to that image. If the decision class is genuine the image is ‘Accepted’ and otherwise ‘Rejected’.

Our designed KNN classification algorithm code also situated in this file. KNN stands for K-nearest neighbors. This classification gives us the decision class that our projects intended output would be.

```
~~~~~  
Image file : A_forged_21.png  
■  
■  
■  
Actual Class: A_forged  
Decision: Rejected  
~~~~~  
('F_orig_23', 'F_orig', 'A_forg', 'Rejected')  
('F_orig_24', 'F_orig', 'F_orig', 'Accepted')  
('G_forg_20', 'G_forg', 'G_forg', 'Rejected')  
('G_forg_21', 'G_forg', 'G_forg', 'Rejected')  
('G_forg_22', 'G_forg', 'G_forg', 'Rejected')  
('G_forg_23', 'G_forg', 'G_orig', 'Accepted')  
('G_forg_24', 'G_forg', 'G_orig', 'Accepted')  
('G_orig_20', 'G_orig', 'Z_forg', 'Rejected')  
('G_orig_21', 'G_orig', 'G_orig', 'Accepted')  
('G_orig_22', 'G_orig', 'G_orig', 'Accepted')  
('G_orig_23', 'G_orig', 'G_orig', 'Accepted')
```

Figure 41: Classification printed on console

### 6.3.8 Evaluation.py

For system to be useful for the society it needs to be accurate and has to work well. For our signature recognition and verification system, accuracy of the system is basically how correctly does our system recognizes a particular signature by giving us whom does it belongs to and whether it is forged or genuine.

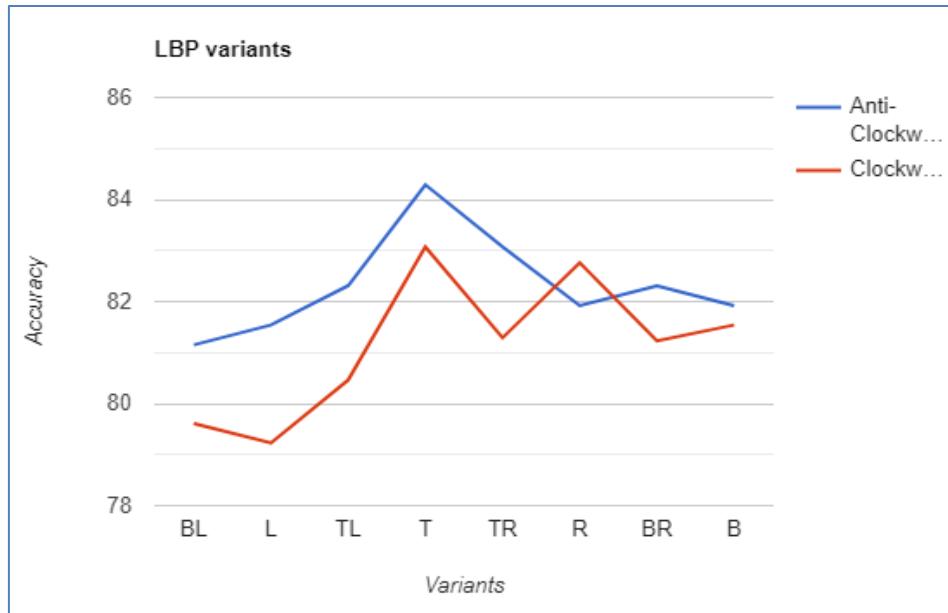
The evaluation parameter used for measuring accuracy of the system is recognition rate. We find the FAR and FRR which stand for False Acceptance Rate and False Rejection Rate. The number of falsely accepted images over the total images is FAR and the number of falsely rejected images over the total images is FRR

We also will have to perform testing and evaluations for the following 16 different variants for our LBP implementation based on the starting point or the leftmost pixel as starting for reading and the results are as shown below.

**Table 2:** Expermintatal Analysis of different LBP Variants

Variant	Clockwise	Anti-Clockwise
TL – Top Left	80.46	82.31
T – Top	83.07	84.29
TR – Top Right	81.29	83.07
R – Right	82.76	81.92
BR – Bottom Right	81.23	82.31
B – Bottom	81.54	81.92
BL – Bottom Left	79.61	81.54
L – Left	79.23	81.15

Thus based on our above data we can make a line graph which is given below. The line graph depicts the variants on horizontal axis and accuracy on the Y-axis, the variants are labelled as above table shows and two different lines are put in the same graph for comparative study of both. We can infer that the anti-clockwise reading shows better results and highest accuracy



**Figure 42:** Line Graph for analysis different LBP Variants

In our experimentation, we find our accuracy to be highest with **84.29 %** at K = 22 in our KNN classifier. The table below shows the different recognition rates for different values for K.

**Table 3:** Expermintatal Analysis with different values of K

K	10	20	22	30	40
<b>FRR</b>	20.77 %	15.2 %	13.79 %	15.38 %	17.69 %
<b>FAR</b>	1.92 %	2.2 %	1.92 %	2.69 %	2.69 %
<b>Accuracy</b>	77.31 %	83.46 %	<b>84.29 %</b>	81.92 %	79.62 %

We can also compare our system with an existing system which we retrieved from the web. This system uses a Convolutional Siamese network along with the constrastive loss function. They chose Euclidian distance as the distance metric for comparing the output feature vectors. The model achieved an accuracy of 73.34%. Deviations of 1-2% are possible as accuracy depends on the threshold. The threshold for the siamese network was computed by taking the average of True positive rate and True negative rate using ROC. The data used is same as the one used in our system described in this paper.

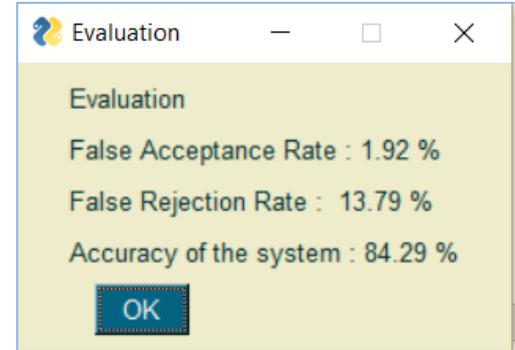


Figure 43: Evaluation popup UI

### 6.3.9 Signature\_verifier.sql

The features extracted are to be stored in 2 dimensional variable here in the system named as ‘trainingFeatures’ and ‘testingFeatures’ where each row has features for each image. Now all the features are then collected in this 2 dimensional array to be later used during classification of the test images. The Feature Vector output is generated for some images and is shown in the figure 25.

```
4.475, 360.11835331181805, 79.94261948670662, 0.9087988826815643, 0.9360953304115469, 1100.423076923077,  
4.315384615384615, 0.9830771833278523, 0.9041345437612739, 0.8979947873264885, 0.817459273222407,  
1.1265560165975104, 272.689094785744, 236.7716856191929, 0.8816548604265529, 6.252597772662824, 951.0669  
144554516, 3.7296741743351043, 0.9853740516953918, 0.8812566819699875, 0.930009741005473, 0.776613339516  
7517,
```

Figure 42: Feature vectors in python console

This data doesn’t really help us understand which is what and also cannot be reused after the execution of code. They might want to be recalculated when the system is run again. To avoid that and to take the system directly to the testing stage, we make use of database. Here we use MySQL database to be run using Apache through the XAMPP control panel. Following image shows how the database

Table	Action	Rows	Type	Collation	Size
testing_classes	★ Browse Structure Search Insert Empty Drop	189	InnoDB	latin1_swedish_ci	16 Kib
testing_features	★ Browse Structure Search Insert Empty Drop	189	InnoDB	latin1_swedish_ci	64 Kib
training_classes	★ Browse Structure Search Insert Empty Drop	637	InnoDB	latin1_swedish_ci	64 Kib
training_features	★ Browse Structure Search Insert Empty Drop	637	InnoDB	latin1_swedish_ci	144 Kib
4 tables	Sum	1,652	InnoDB	latin1_swedish_ci	288 Kib

Figure 43: Tables in MySQL database

## 7 Comparative study

We can also compare our system with an existing system which we retrieved from the web [45]. This system was found on Github, a software hosting website which has brought millions of developers together to discover, share, and build better software

### 7.1 Dataset

The data we have used is a subset of the same dataset as the one used in this system described in this paper and thus we could compare our systems. The CEDAR signature dataset is one of the benchmark datasets for signature verification. The naming conventions of this system is obviously different from our system. The dataset can also be downloaded from the link provided by the designer on his github project page [45]. This dataset is read and used for training and testing within this system.

### 7.2 Preprocessing

For preprocessing, the images from the dataset were converted to grayscale first, which means the 3 dimensional image are first converted to a 2 dimensional image. The image is then inverted and scaled down to 0 or up to 255 depending on whether the pixel value was below or above 50(this was done to remove any background specks and proved to simple yet effective technique for this task). Image tensor sizes of 225x155 were fed into the model. Images were grouped in pairs of genuine and forged images, where the label was 1 if both were genuine and of the same writer and 0 otherwise. 13500 image pairs of each label were chosen, 15% of which were used for testing.

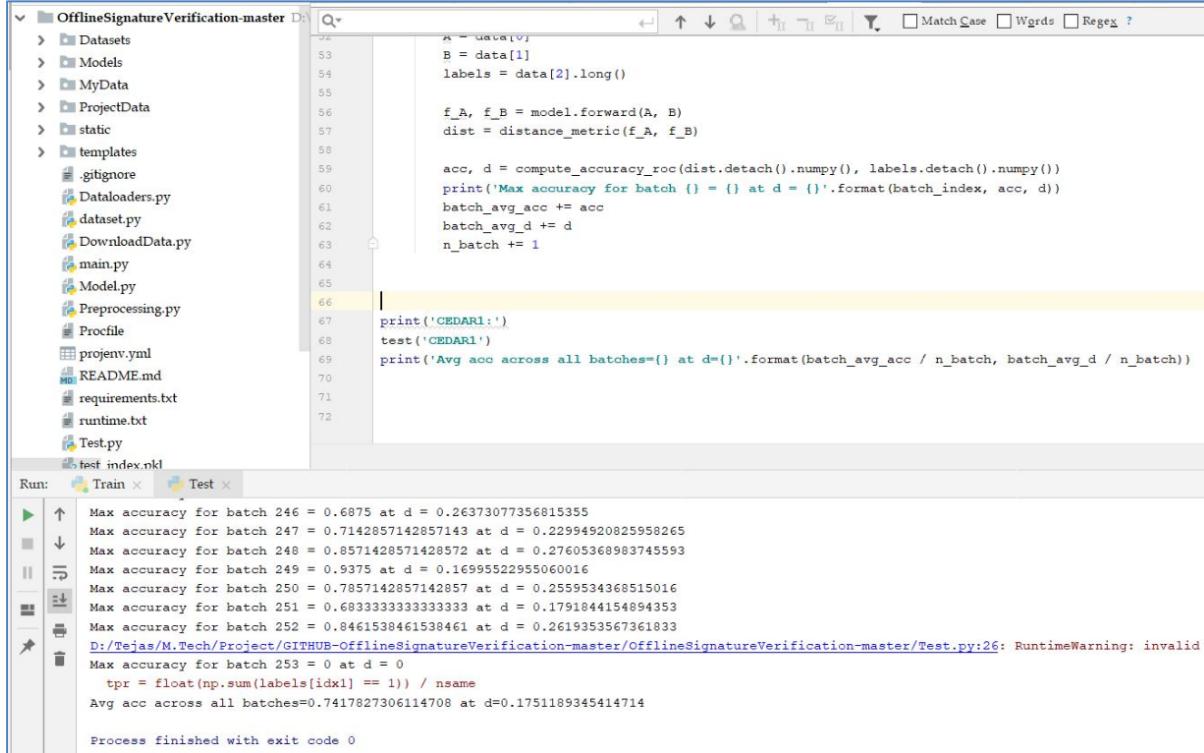
### 7.3 Model used

The model used by the designer is a Convolutional Siamese network. Siamese neural network is a class of neural network architectures that contain two or more *identical* subnetworks. *identical* here means they have the same configuration with the same parameters and weights. Parameter updating is mirrored across both subnetworks.

Along with the Siamese neural network, the system makes use of a Contrastive loss function. This network uses Euclidian distance as the distance metric for comparing the output feature vectors, similar to how we used it in our K nearest neighbor classification algorithm.

## 7.4 Evaluation

The model achieved an accuracy of 73.34% on the CEDAR signature dataset(test set size was around 4100 samples). Deviations of 1-2% are possible as accuracy depends on the threshold. The threshold for the siamese network was computed by taking the average of True positive rate and True negative rate using ROC.



The screenshot shows a code editor with a file tree on the left and a code editor window on the right. The file tree shows a directory structure for an 'OfflineSignatureVerification' project, including subfolders like 'Datasets', 'Models', 'MyData', 'ProjectData', 'static', 'templates', and files like 'Dataloaders.py', 'dataset.py', 'DownloadData.py', 'main.py', 'Model.py', 'Preprocessing.py', 'Profile', 'projenv.yml', 'README.md', 'requirements.txt', 'runtime.txt', and 'Test.py'. The code editor window displays Python code for testing a model's accuracy across batches. The code includes imports for PyTorch and custom modules, loops through batches, and prints accuracy metrics for each batch and overall. A terminal window at the bottom shows the execution results, including individual batch accuracies and a final average accuracy of 0.7417827306114708.

```
A = data[0]
B = data[1]
labels = data[2].long()

f_A, f_B = model.forward(A, B)
dist = distance_metric(f_A, f_B)

acc, d = compute_accuracy_roc(dist.detach().numpy(), labels.detach().numpy())
print('Max accuracy for batch {} = {} at d = {}'.format(batch_index, acc, d))
batch_avg_acc += acc
batch_avg_d += d
n_batch += 1

print('CEDAR1:')
test('CEDAR1')
print('Avg acc across all batches={} at d={}'.format(batch_avg_acc / n_batch, batch_avg_d / n_batch))

Run: Train × Test ×
Max accuracy for batch 246 = 0.6875 at d = 0.26373077356815355
Max accuracy for batch 247 = 0.7142857142857143 at d = 0.22994920825958265
Max accuracy for batch 248 = 0.8571428571428572 at d = 0.27605368983745593
Max accuracy for batch 249 = 0.9375 at d = 0.16995522955060016
Max accuracy for batch 250 = 0.7857142857142857 at d = 0.2559534368515016
Max accuracy for batch 251 = 0.6833333333333333 at d = 0.1791844154894353
Max accuracy for batch 252 = 0.8461538461538461 at d = 0.2619353567361833
D:/Tejas/M.Tech/Project/GITHUB-OfflineSignatureVerification-master/OfflineSignatureVerification-master/Test.py:26: RuntimeWarning: invalid
Max accuracy for batch 253 = 0 at d = 0
    tpr = float(np.sum(labels[idx1] == 1)) / nname
Avg acc across all batches=0.7417827306114708 at d=0.1751189345414714

Process finished with exit code 0
```

Figure 44: Existing project

## **8 Conclusion & Future Work**

We can conclude by stating that the remarkable work done by the researchers in over 40 different papers have led and motivated us to design a system which is clearly described in this paper. We provide full credits to all the authors of these papers for sharing their knowledge and their astonishing work they have put forward that led us to our study. By looking at them and comparing, we can say which one is good by merely looking at their recognition rates. But choosing a system does not just depends on the systems efficiency, there are many other aspects that must be considered while designing a system such as application of the system, time requirements, space requirements of the system, complexity of the algorithms and cost of setting up the application and so on.

The research allowed us to learn more and more about the domain and the problem of signature recognition and verification. The research work of over 40 different research work on the problem of signature recognition/verification was done for this paper which allowed to prepare and plan for a signature verification system that was designed and presented in this paper.

The system's accuracy which comes out to be around 85% can still be brought up by adding more amount of research and combining the existing techniques with our work. The system's does take time to train which can also be improvised but testing phase is much quicker. The Local binary Pattern algorithm allows to extract texture based features which has shown great results in similar systems such as face recognition. There are still many approaches out there that may be better than what are listed here and thus the work does not end here.

## 9 References

- [1] S. F. A. Zaidi and S. Mohammed, “Biometric Handwritten Signature Recognition,” 2007.
- [2] D. Morocho, A. Morales, J. Fierrez, and R. Vera-Rodriguez, “Towards human-assisted signature recognition: Improving biometric systems through attribute-based recognition,” *ISBA 2016 - IEEE Int. Conf. Identity, Secur. Behav. Anal.*, 2016.
- [3] S. A. Angadi, S. Gour, and G. Bhajantri, “Offline Signature Recognition System Using Radon Transform,” *2014 Fifth Int. Conf. Signal Image Process.*, pp. 56–61, 2014.
- [4] S. Hangai, S. Yamanaka, and T. Hammamoto, “ON-LINE SIGNATURE VERIFICATION BASED ON ALTITUDE AND DIRECTION OF PEN MOVEMENT,” *Proc. 15th Int. Conf. Pattern Recognition. ICPR-2000*, vol. 3, no. 1, pp. 479–482, 2000.
- [5] I. V Anikin and E. S. Anisimova, “Handwritten signature recognition method based on fuzzy logic,” *2016 Dyn. Syst. Mech. Mach.*, 2016.
- [6] E. Ozgunduz, T. Senturk, and M. E. Karsligil, “Off-line signature verification and recognition by support vector machine,” *13th Eur. Signal Process. Conf.*, no. 90, pp. 1–4, 2005.
- [7] S. A. Angadi and S. Gour, “Euclidean Distance Based Offline Signature Recognition System Using Global and Local Wavelet Features,” *2014 Fifth Int. Conf. Signal Image Process.*, pp. 87–91, 2014.
- [8] Ruangroj Sa-Ardship and K. Woraratpanya, “Offline Handwritten Signature Recognition Using Adaptive Variance Reduction,” *7th Int. Conf. Inf. Technol. Electr. Eng. (ICITEE), Chiang Mai, Thail. Offline*, pp. 258–262, 2015.
- [9] M. A. Djoudjai, Y. Chibani, and N. Abbas, “Offline signature identification using the histogram of symbolic representation,” *5th Int. Conf. Electr. Eng. - Boumerdes*, pp. 1–5, 2017.
- [10] A. B. Jagtap and R. S. Hegadi, “Offline Handwritten Signature Recognition Based on Upper and Lower Envelope Using Eigen Values,” *Proc. - 2nd World Congr. Comput. Commun. Technol. WCCCT 2017*, pp. 223–226, 2017.
- [11] T. Marušić, Ž. Marušić, and Ž. Šeremet, “Identification of authors of documents based on offline signature recognition,” *MIPRO*, no. May, pp. 25–29, 2015.
- [12] S. L. Karanjkar and P. N. Vasambekar, “Signature Recognition on Bank cheques using ANN,” *IEEE Int. WIE Conf. Electr. Comput. Eng.*, no. December, 2016.
- [13] G. S. Prakash and S. Sharma, “Computer Vision & Fuzzy Logic based Offline Signature Verification and Forgery Detection,” *IEEE Int. Conf. Comput. Intell. Comput. Res.*, 2014.
- [14] M. S. Shirdhonkar and M. B. Kokare, “Document image retrieval using signature as

- query,” *2011 2nd Int. Conf. Comput. Commun. Technol. ICCCT-2011*, pp. 66–70, 2011.
- [15] R. Sa-Ardship and K. Woraratpanya, “Offline Handwritten Signature Recognition Using Polar-Scale Normalization,” *8th Int. Conf. Inf. Technol. Electr. Eng. (ICITEE)*, Yogyakarta, Indonesia., pp. 3–7, 2016.
  - [16] A. Piyush Shanker and A. N. Rajagopalan, “Off-line signature verification using DTW,” *Pattern Recognit. Lett.*, vol. 28, no. 12, pp. 1407–1414, 2007.
  - [17] Nancy and P. G. Goyal, “Signature Processing in Handwritten Bank Cheque Images,” *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 2, no. 5, pp. 1239–1243, 2014.
  - [18] A. T. Nasser and N. Dogru, “Signature recognition by using SIFT and SURF with SVM basic on RBF for voting online,” *Proc. 2017 Int. Conf. Eng. Technol. ICET 2017*, vol. 2018–Janua, pp. 1–5, 2017.
  - [19] A. Kumar and K. Bhatia, “A Robust Offline Handwritten Signature Verification System Using Writer Independent Approach,” *3rd Int. Conf. Adv. Comput. Autom.*, 2017.
  - [20] H. Anand, “Enhanced Signature Verification and RECOGNITION USING MATLAB,” *Int. J. Innov. Res. Adv. Eng.*, vol. 1, no. 4, pp. 88–94, 2014.
  - [21] B. H. Shekar and R. K. Bharathi, “Eigen-signature: A robust and an efficient offline signature verification algorithm,” *Int. Conf. Recent Trends Inf. Technol. ICRTIT 2011*, pp. 134–138, 2011.
  - [22] A. R. Rahardika, “Global Features Selection for Dynamic Signature Verification,” *Int. Conf. Inf. Commun. Technol. Glob.*, pp. 348–354, 2018.
  - [23] T. Handhayani, A. R. Yohannis, and Lely Hiryanto, “Hand Signature and Handwriting Recognition as Identification of the Writer using Gray Level Co- Occurrence Matrix and Bootstrap,” *Intell. Syst. Conf.*, no. September, pp. 1103–1110, 2017.
  - [24] A. Beresneva, A. Epishkina, and D. Shingalova, “Handwritten Signature Attributes for its Verification,” pp. 1477–1480, 2018.
  - [25] M. P. Patil, Bryan Almeida, Niketa Chettiar, and Joyal Babu, “Offline Signature Recognition System using Histogram of Oriented Gradients,” *Int. Conf. Adv. Comput. Commun. Control*, 2017.
  - [26] M. M. Kumar and N. B. Puhan, “Offline signature verification using the trace transform,” *2014 IEEE Int. Adv. Comput. Conf.*, pp. 1066–1070, 2014.
  - [27] O. Miguel-Hurtado, L. Mengibar-Pozo, M. G. Lorenz, and J. Liu-Jimenez, “On-Line Signature Verification by Dynamic Time Warping and Gaussian Mixture Models,” *2007 41st Annu. IEEE Int. Carnahan Conf. Secur. Technol.*, pp. 23–29, 2007.
  - [28] M. Ferrer and J. Vargas, “Robustness of offline signature verification based on gray level features,” *IEEE Trans. Inf. FORENSICS Secur.*, vol. 7, no. 3, pp. 966–977, 2012.
  - [29] B. Erkmen, N. Kahraman, R. A. Vural, and T. Yildirim, “Conic section function neural network circuitry for offline signature recognition,” *IEEE Trans. Neural Networks*, vol. 21, no. 4, pp. 667–672, 2010.

- [30] M. A. Ferrer, A. Morales, and J. F. Vargas, “Off-line signature verification using local patterns,” *2nd Natl. Conf. Telecommun.*, pp. 1–6, 2011.
- [31] M. Tahir and M. U. Akram, “Online Signature Verification using Hybrid Features,” *Conf. Inf. Commun. Technol. Soc. Online*, pp. 11–16, 2018.
- [32] M. Pal, S. Bhattacharyya, and T. Sarkar, “Euler number based feature extraction technique for Gender Discrimination from offline Hindi signature using SVM & BPNN classifier,” *2018 Emerg. Trends Electron. Devices Comput. Tech.*, pp. 1–6, 2004.
- [33] W. Pan and G. Chen, “A Method of Off-line Signature Verification for Digital Forensics,” *12th Int. Conf. Nat. Comput. Fuzzy Syst. Knowl. Discov.*, pp. 488–493, 2016.
- [34] M. A. Ferrer, J. B. Alonso, and C. M. Travieso, “Offline geometric parameters for automatic signature verification using fixed-point arithmetic,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 27, no. 6, pp. 993–997, 2005.
- [35] S. A. Farimani and M. V. Jahan, “An HMM for Online Signature Verification Based on Velocity and Hand Movement Directions,” *Iran. Jt. Congr. Fuzzy Intell. Syst.*, pp. 205–209, 2018.
- [36] G. Pirlo and D. Impedovo, “Verification of static signatures by optical flow analysis,” *IEEE Trans. Human-Machine Syst.*, vol. 43, no. 5, pp. 499–505, 2013.
- [37] A. Alaei, S. Pal, U. Pal, and M. Blumenstein, “An Efficient Signature Verification Method Based on an Interval Symbolic Representation and a Fuzzy Similarity Measure,” *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 10, pp. 2360–2372, 2017.
- [38] D. S. Guru and H. N. Prakash, “Online Signature Verification and Recognition: An Approach based on Symbolic Representation.,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 6, pp. 1059–73, 2009.
- [39] A. Sharma and S. Sundaram, “On the Exploration of Information from the DTW Cost Matrix for Online Signature Verification,” *IEEE Trans. Cybern.*, vol. 48, no. 2, pp. 611–624, 2018.
- [40] G. Pirlo, V. Cuccovillo, M. Diaz-Cabrera, D. Impedovo, and P. Mignone, “Multidomain Verification of Dynamic Signatures Using Local Stability Analysis,” *IEEE Trans. Human-Machine Syst.*, vol. 45, no. 6, pp. 805–810, 2015.
- [41] Existing project used for comparison  
<https://github.com/Aftaab99/OfflineSignatureVerification>
- [42] Image Processing TutorialsPoint: <https://www.tutorialspoint.com/dip>
- [43] Machine Learning TutorialsPoint:  
[https://www.tutorialspoint.com/machine\\_learning\\_with\\_python](https://www.tutorialspoint.com/machine_learning_with_python)
- [44] Dataset source:- [http://www.iapr-tc11.org/mediawiki/index.php?title=Datasets\\_List#Handwritten%20Documents](http://www.iapr-tc11.org/mediawiki/index.php?title=Datasets_List#Handwritten%20Documents)
- [45] Github's existing system used for comparison  
<https://github.com/Aftaab99/OfflineSignatureVerification>

## **Appendix**

### **Paper Published**

Tejas Jadhav, "Handwritten Signature Verification using Local Binary Pattern Features and KNN", International Research Journal of Engineering and Technology (IRJET), Vol.06, Issue.04, pp.579-586, April 2019

### **Indexing**

- An ISO 9001-2008 Certified Journal
- Certificate of indexing 2018
- A UGC Recognized Journal
- Google Scholar
- Academia Database
- INNO SPACE
- Cite Factor
- Research Gate
- SJournals Index
- Electronic Journals Library
- Computer Science Directory

Impact Factor: 7211 as of 2018

E - ISSN: 2395-0056

P - ISSN: 2395-0072

**Published Paper:** <https://www.irjet.net/archives/V6/i4/IRJET-V6I4130.pdf>

# Handwritten Signature Verification using Local Binary Pattern features and KNN

Tejas Jadhav<sup>1</sup>

M. Tech in Computer Science Engg.

Mukesh Patel School of Technology Management & Engineering,

NMIMS University, Mumbai, India

[tjadhav95@gmail.com](mailto:tjadhav95@gmail.com)

\*\*\*

**Abstract** - An offline signature verification method has been described in this paper. Handwritten signature has been critical person identification technique for decades. Whether one signs a petition, work documents, contract, or wants to approve payment of a check, he/she uses personal signature to do all those things. The objective of this paper is to give away an efficient biometric signature recognition and verification techniques. The paper intends to give away information all about the application of biometrics i.e. signature detection and also about the various stages that are necessary to be studied by a designer while creating an application that will use it. The system works in different stages which includes pre-processing, LBP image conversion, feature extraction, and classification. A total of 40 different signature recognition approaches were read and studied before designing the system here that are been taken from different research papers. The output obtained is evaluated in the papers itself by performing experimental analysis and can be compared with another existing system in this paper.

**Key Words:** Signature, biometrics, Otsu thresholding, fuzzy, local binary pattern, texture

## 1 INTRODUCTION

Biometrics is currently perceived as a vital technology for setting up secure access control. It utilizes physiological qualities of humans for recognizing individual, and signature is one of the characteristics usable for biometrics. Singular recognizable proof technology utilizing human countenances, more often than not called confront acknowledgment technology, has been concentrated primarily in western nations since 1990s. It has been the most widespread tool for paper documents verification for many decades. In real life the human-expert can verify handwritten signatures easily, but it is a complicated task for doing by machines today.

In this research paper, there are a total of 40 different approaches used in 40 different research papers that were studied before the design of the system. These use not just image processing tools but also some level of machine learning. The approaches listed use feature extraction and classification techniques such as radon transforms, altitude and direction of pen movement, fuzzy logic, adaptive variance reduction, artificial neural network, support

vector machine, Euclidian distances. The system we propose is developed in python 3.6 and used MySQL for storing data related features and classes in database. The development was done in PyCharm python IDE which allows intelligent code completion, on-the-fly error checking and quick-fixes, easy project navigation and much more.

### 1.1 Real life applications [1]

- Finance:** IT-Processing centres of German savings banks are offering their customers solutions to embed dynamic signatures securely into electronic documents
- Insurance:** Signing an insurance contract and documenting the consulting process that is required by EU legislation
- Real Estate:** Increasingly popular among real estate agents in USA are options of paperless contracting through signing on Tablet PCs.
- Health:** The Ingolstadt hospital is capturing and verifying the doctor's signature that fill electronic patient records on tablet PCs.
- Telecom:** Signing phone and DSL contracts in the telecom shops is another emerging market.

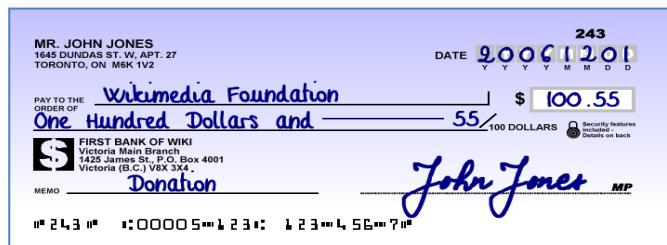


Figure 1: A sample bank cheque with signature

### 1.2 Types & methods of Signature Verification

#### 1. Offline Signature Verification Methods:

In this method, system makes use of a simple scanner or a camera that can take in image having signature & process the image further with whatever features it gets. This method can be seen useful in many applications such as banking cheques, medical certificates & prescriptions etc.

## 2. Online Signature Verification Methods:

Here the system makes use of special acquisition devices like stylus pens and tablets that can take in signature features in real time

## 2 ABOUT THE DOMAIN

To understand the in depth concepts of the different approaches, that are listed and explained in the later part, we might require some basic pre-requisite knowledge of the domain they work under.

### 2.1 Image processing

Image processing [41] is working on images using mathematical operations by form of signal processing for which the input is an image, a series of images, or a video, such as photographs or video frame; the output of image processing could be either an image or a set of characteristics or parameters related to an image. Most image-processing approaches allow treating the image as a two-dimensional array or signal and applying standard signal-processing techniques to it.

### 2.2 Biometrics

Biometrics [42] is the measurement or statistical analysis of people's physical/behavioural characteristics. The approach is mainly used for identification, security and access control, or for investigating individuals that are under surveillance. The basic idea of biometric authentication is that every person is unique and an individual can be identified by his or her intrinsic physical or behavioural traits. The term "biometrics" is taken from the Greek words "bio" and "metric" meaning life and meaning to measure respectively

### 2.3 Machine Learning

Machine learning [44] is a branch of science that deals with programming the systems in such a way that they on their own learn and improve with experience. In ML, learning actually means recognizing and understanding input data and making and giving wise decisions based on that supplied data. It is very hard to cater to all those decisions based on all possible data inputs. To approach this problem, researchers develop algorithms that build knowledge from specific data and past experience with the principles of statistics, logic, probability theory, search, combinatorial optimization, reinforcement learning & control theory.

## 3 LITERATURE REVIEW

This section lists down the various algorithms that we are to study. Most of them work in 3 stages, which are pre-processing, main processing i.e. feature extraction and then post-processing stage which includes decision making or classification. There are a high number of algorithms that

can be implemented for recognition of handwritten signatures these days, but following are the algorithms which give other newly formulated algorithms a backbone.

In paper [1] the researchers are considering some simple parameters like speed, acceleration, pen down time, distance, etc. and based on the literature studies they discuss how these features can be used in the Image processing environment to improve the performance of handwritten signature. The approach provides a PI of 97.5 %.

The paper [2] presents a crowdsourcing experiment to establish the human baseline performance for signature recognition tasks and a novel attribute-based semi-automatic signature verification system inspired in FDE analysis. It combines the DTW algorithm with Attribute based algorithm to obtain better accuracy and increase the recognition rate. With EER of 5%, we can say that recognition rate is 95%.

The proposed system in paper [3] functions in three stages. Pre-processing stage; this consists of gray scale conversion, binarization and fitting boundary box. Feature extraction stage where total 16 radon transform based projection features are extracted which are used to distinguish the different signatures. Finally in the classification stage; an efficient BPNN, Back Propagation Neural Network is prepared and trained with 16 extracted features. The average recognition accuracy of this system ranges from 87% - 97% with the training set of 10–40 persons. Global features include\_Height of the signature, Width of the signature, and Centroid along both X axis, Centroid along both Y axis

In paper [4], researchers propose a new on-line writer authentication system using the pen altitude, pen azimuth, shape of signature, and writing pressure in real time. It is well expected that altitude and the azimuth of gripped pen under signing depends on the shape of writer's hand and the habit of writing. The data set prepared is based on the following Features to be calculated dynamically at every instance of time: X-coordinate:  $x(t)$ , Y-coordinate:  $y(t)$ , Pressure:  $p(t)$ , Azimuth:  $\theta(t)$ , Altitude:  $\phi(t)$ . After individuality in the altitude and the azimuth of gripped pen under signing is explained, the experimental result with writing information by 24 writers is shown. It is found that the authentication rate of 98.2% is obtained.

In this paper [6] researchers present an off-line signature verification and recognition system using the global, directional and grid features of signatures. Support Vector Machine (SVM) was used to classify & verify the signatures and a classification ratio of 0.95 was obtained. Thus 95% accuracy is obtained. As the recognition of signatures represents a multiclass problem SVM's one-against-all method was used.

The proposed system of paper [7] functions in three stages. Pre-processing stage consists of four steps namely grey scale conversion, binarization, thinning and fitting boundary box process in order to make signatures ready

for the important feature extraction. Feature extraction stage consists total 59 global and local wavelet based energy features to be extracted which are used to classify the different signatures. Finally in classification, a simple Euclidean distance classifier is used as decision tool. The average recognition accuracy obtained using this model ranges from 90% to 100% with the training set of images of 10 to 30 persons.

In paper [12], a bank cheque is taken and the signature is collected from the bank cheque by taking it out by cropping the area of interest. The image is then trained and stored into the trained database using an efficient Feed forward artificial neural network. Then signatures to be tested are compared with the signatures that are stored into the test database. The accuracy of the system is tested out to be 85.00%. In pre-processing, Otsu's thresholding or binarization algorithm is used which is one of the finest one, allows image object to be separated from its background and later Gaussian low pass filter is applied to remove unwanted noise.

Fuzzy Logic and Artificial Neural Network Based Off-line Signature Verification and Forgery Detection System is presented in paper [13]. As there are distinct and necessary variations in the feature set of each signature, so in order to match a particular signature image with the database image, the structural features of the signatures and also the local feature variations in the signature characteristics are used. The paper suggests that, variation in personality of signatures, because of age, sickness, geographic location and emotional state of the person actuates the problem.

An offline signature verification using neural network is projected in paper number [20], where the signature is written on a paper are obtained using a scanner or a camera captured and presented in an image format. In pre-processing, colour to grayscale, and finally to black and white, Resizing the image, thinning. Features extracted include Eccentricity, Skewness, Kurtois, Orientation Entropy, Euler number, Solidity, Mean, Standard deviation. The classification is done using a Cascaded feed-forward back-propagation networks and recognition rate of 92.5% is obtained.

The paper [24] examines authentication systems based on handwritten signature and the main informative parameters of signature such as size, shape, velocity, pressure, etc. along with DCT, DFT. System using K-Nearest neighbours' algorithm and Random forest algorithm for classification and the accuracy of 95% is shown.

In this paper [26], the trace transform based affine invariant features are applied for signature verification. The diametric and trace functions are appropriately chosen to compute a set of circus functions from each signature image. Recognition rate of 76% is obtained. Low accuracy, more invariant functional will be designed for usefulness in signature verification.

Paper [28] uses a texture base approach called the Local binary Pattern algorithm along with SVM, The signature models are trained with genuine signatures on white

background and tested with other genuine and forgeries mixed with different backgrounds. Results depict that a basic version of local binary patterns (LBP) or local directional and derivative patterns are more robust than others like GLCM features to the grey level distortion with SVM with histogram oriented kernels as a classifier or rotation invariant uniform LBP. The proposed configurations are checked and evaluated under different situations and conditions: changing the number of training signature images, database with different inks, multiple signing sessions, increasing the number of signers and combining different features. Results have also been provided when looking for the signature in the check and segmenting it automatically. In all these cases, the best results were obtained with the LDervP feature set, which improve the results obtained in the predefined baseline, showing quite significant improvements with fictitious signature images.

Paper [29] uses Conic section function neural network (CSFNN) circuitry was designed for offline signature recognition. CSFNN is a unified framework for multilayer perceptron (MLP) and radial basis function (RBF) networks and the size of feature vectors was not suitable for designed CSFNN chip structure owing to the input limitations of the circuit. Pre-processing is done using noise reduction algorithm, skeletonization. The few main disadvantages of analog systems include its sensitivity to ambient noise and to temperature. Accuracy shown is 95.5%.

This paper [30] explores the usefulness of local binary pattern (LBP) and local directional pattern (LDP) texture measures to discriminate off-line signatures. Comparison between these several texture normalizations is generated in order to look for reducing pen dependence. The recognition rate is 91.92%. The pre-processing techniques include binarized, cropped, or-exclusive operation, Texture histogram normalization. Least Squares Support Vector Machine (LS-SVM) is applied for classification.

This paper [34] titled presents a set of geometric signature features for offline automatic Signature verification based on the description of the signature envelope and the interior stroke distribution in polar and Cartesian coordinates. Feature extraction method includes Outline Detection and Representation, Feature Vector Based on Polar Coordinates, Feature Vector Based on Cartesian Coordinates. Classification is performed using The HMM Signature Model, Support Vector Machine Signature Model and Euclidean Distance-Based Signature Model.

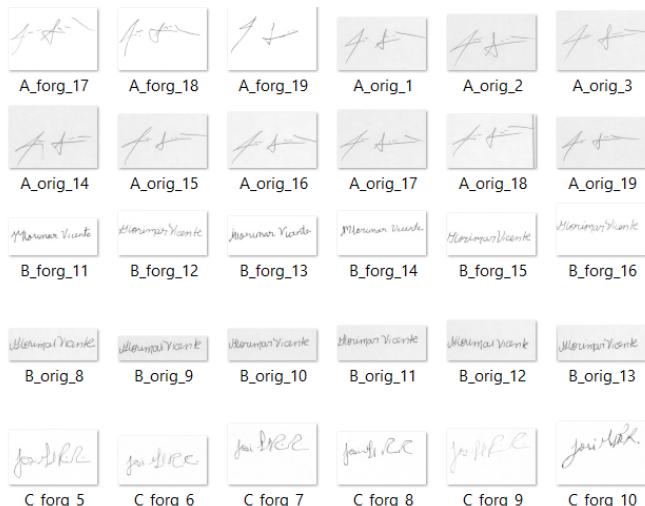
In this paper [37] an efficient off-line signature verification method based on an interval symbolic representation and a fuzzy similarity measure is proposed. 88.26% Local Binary Pattern, interval-valued symbolic model. A histogram-based threshold technique, mean filter for noise removal, minimum bounding boxes. Classification of the signature image is done based on the similarity value, an adaptive writer-dependent acceptance threshold

This paper [40] presents a new approach for online signature verification that exploits the potential of local

stability information in handwritten signatures. Different from previous models, this approach classifies a signature using a multi domain strategy. Accuracy obtained is 97.90%. Both variable and stable regions of a signature image object could be considered for supporting the advanced personalized techniques in signature verification and recognition, since probably, from a behavioural point of view, a variability model of a signer/author could also be very complementary and informative to a stability model.

#### 4 DATASET PREPARED

The signature verification system would need a set of image dataset having handwritten signatures from different authors. The data set prepared was taken from web uploaded by researchers online on the website [42]. The CEDAR signature dataset is one of the benchmark datasets for signature verification. Since the dataset downloaded is vast and contains a lot of images we have prepared a subset of the vast dataset and kept aside directory of folders of images which contains total 26 Authors, all having genuine as well as forged signatures and thus 52 different classes. The dataset is divided in an approximate ratio of 4:1 for preparing training and testing data respectively. Therefore 988 training images and 260 testing images kept in two different folders combine to a total of 1248 images.

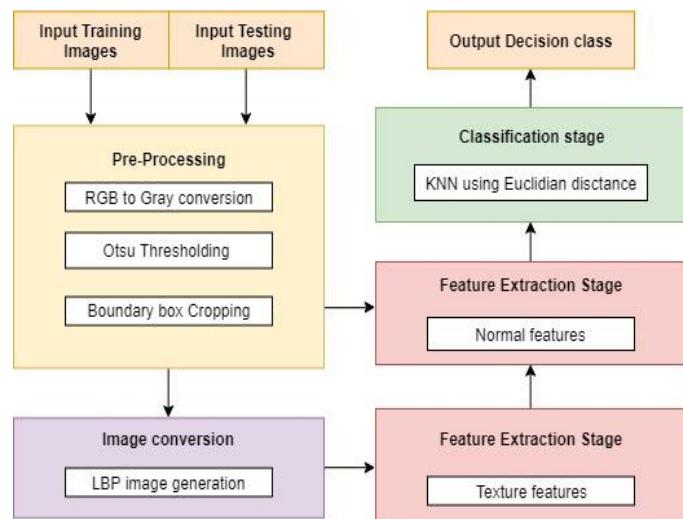


**Figure 2:** Dataset of signature images

The dataset is renamed and kept in a directory in such a manner that the system will be able to retrieve, process and analysed them easily within the system. All the images are kept in '.png' format and are named in format that will depict its class and also will be used as a unique id or a primary key for our database. For instance, G\_orig\_08.png means author G's original image number 8, the class would 'G\_orig' and the unique primary key would be G\_orig\_08.

#### 5 PROPOSED APPROACH

This paper gives a system that works in different stages which includes pre-processing, LBP image conversion, feature extraction and classification. The system like most other systems would give as input set of signature images which would include training set and testing set. The system would give a decision class for all the testing images which we can use to compare with their actual classes to find the accuracy of the system.



**Figure 3:** Block diagram of proposed approach

##### 5.1 Pre-processing

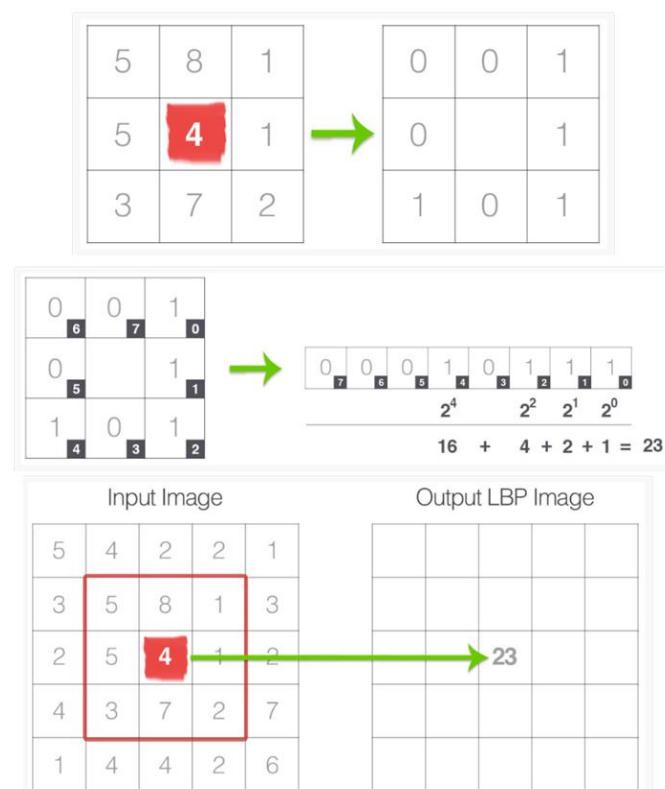
The pre-processing stage is responsible for taking in raw images and convert them into pre-processed form which means the images are ready for processing and feature extraction. The pre-processing stage includes RGB to Grey image conversion which will turns the 3 dimensional colour signature images into a 2 dimensional grey image of having intensity 0 to highest of 255. Then image is turned into a binary image having intensities of 0 or 255 only. To do so we use Otsu thresholding method which dynamically finds the threshold intensity level of image. In the end we crop the image to have only the signature object and no extra white margins.



**Figure 4:** Pre-processing stage: (a) Input signature image; (b) Preprocessed image

## 5.2 LBP image conversion

LBP stands for Local Binary Pattern. The grey image is converted to a LBP image in this stage. This LBP image is dark in colour and is very much useful to extract texture based features out of the image.



**Figure 5:** LBP image conversion algorithm

The first step in constructing a LBP is to take the 8 pixel neighbourhood surrounding a center pixel and threshold it to construct a set of 8 binary digits. Taking the 8 bit binary neighborhood of the center pixel and converting it into a decimal representation. The calculated LBP value is then stored in an output array with the same width and height as the original image. The mask is then moved ahead in the image and the process repeats.

## 5.3 Feature extraction

Feature extraction stage means to take out numeric values out of the image so that an algorithmic process can compare them and in turn compare the image. We can use a feature set having a huge number of features but that will not do any good if their impact is not much over their image. Thus we narrow down to a feature vector set having 16 features which includes 8 normal features and 8 texture features. The pre-processed image is used for taking out normal features and LBP image is given to extract texture features.

The normal shape based features that are extracted from the pre-processed image are given below:

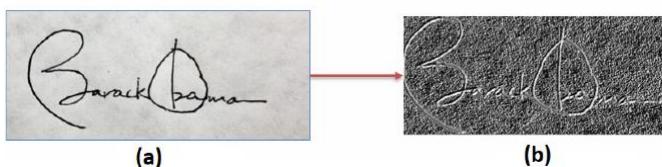
1. Aspect Ratio: The ratio of the width to the height of an image or screen.
2. Center of Gravity - X: The Center of Gravity or Center of Mass statistic calculates where the COG of the image lies. The COG of X is calculated by:  

$$\text{COG}_X = \text{COG}_X + (I^*x)$$
3. Center of Gravity - Y: The Y- Center of Gravity :  

$$\text{COG}_Y = \text{COG}_Y + (I^*y)$$
4. Baseline Shift: This depicts which side (left or right) is the signature waited more and by how much. Calculated difference of left and right COG Y.
5. Energy: the sum of square elements in GLCM
6. Dissimilarity: the weights with which GLCM probabilities are multiplied increase linearly away from the diagonal
7. Haralick: describe the overall texture of the image using measures
8. Kurtosis: Kurtosis is a measure of the combined weight of a distribution's tails relative to the center of the distribution

The LBP texture based features that are extracted from the LBP image are given below:

9. Contrast: measure of the intensity contrast between a pixel and its neighbor over the whole image
10. Normalized Area: The amount of darker pixels that constitute the object in the image divided by the total size (no of pixels) in the image.
11. Homogeneity: value that calculates the tightness of distribution of the elements in the GLCM to the GLCM diagonal
12. Energy: the sum of square elements in GLCM
13. Dissimilarity: Dissimilarity measure of LBP image
14. Haralick: Haralick feature of LBP image
15. Skewness: asymmetry in a statistical distribution, in which the curve appears distorted or skewed either to the left or to the right
16. Kurtosis: Kurtosis measure of LBP image



**Figure 7:** LBP image conversion:  
 (a) Grey image; (b) LBP image

## 5.4 Classification

The classifier we have used is KNN which stands for k-nearest neighbours. It is basically a classification algorithm that means it assigns a class to a test image based on its feature values. The k-nearest neighbours' algorithm uses Euclidian distance method to find the distance between two training points. Thus using Euclidian distance we find k nearest neighbouring training points of our test point based on its features and the class with maximum number of occurrences is taken as the decision class for that test image and is assigned to that image. If the decision class is 'orig' with same signer the image is 'Accepted' and otherwise 'Rejected'.

## 5.5 Evaluation and Analysis

For system to be useful for the society it needs to be accurate and has to work well. For our signature recognition and verification system, accuracy of the system is basically how correctly does our system recognizes a particular signature by giving us whom does it belongs to and whether it is forged or genuine.

The evaluation parameter used for measuring accuracy of the system is recognition rate. We find the FAR and FRR which stand for False Acceptance Rate and False Rejection Rate. The number of falsely accepted images over the total images is FAR and the number of falsely rejected images over the total images is FRR

In our experimentation, we find our accuracy to be highest with 85.66% at K = 22 in our KNN classifier. The table below shows the different recognition rates for different values for K.

**Table 1:** Expermintatal Analysis

K	10	20	22	30	40
FRR	19.7%	15.4%	13.79%	15.3%	17.7%
FAR	2.9%	2.2 %	1.92%	2.7 %	2.7%
Accuracy	77.3%	83.4%	<b>84.29%</b>	81.9%	79.6%

We can also compare our system with an existing system which we retrieved from the web. This system uses a Convolutional Siamese network along with the constrastive loss function. They chose Euclidian distance as the distance metric for comparing the output feature vectors. The model gave an accuracy of 73.34%. Designer explains that the deviations seen 1-2% could be possible as accuracy depends on the threshold. The threshold for the Siamese network is computed by taking the average of True positive rate and True negative rate using ROC. The data used is same as the one used in our system described in this paper and thus we could compare our systems

## 6 CONCLUSION

We can conclude by stating that the remarkable work done by the researchers in over 40 different papers have led and motivated us to design a system which is clearly described in this paper. We provide full credits to all the authors of these papers for sharing their knowledge and their astonishing work they have put forward that led us to our study. By looking at them and comparing, we can say which one is good by merely looking at their recognition rates. But choosing a system does not just depends on the systems efficiency, there are many other aspects that must be considered while designing a system such as application of the system, time requirements, space requirements of the system, complexity of the algorithms and cost of setting up the application and so on.

## 7 FUTURE WORK

The research allowed us to learn more and more about the domain and the problem of signature recognition and verification. The research work of over 40 different research work on the problem of signature recognition/verification was done for this paper which allowed to prepare and plan for a signature verification system that was designed and presented in this paper.

The system's accuracy which comes out to be around 85% can still be brought up by adding more amount of research and combining the existing techniques with our work. The system's does take time to train which can also be improvised but testing phase is much quicker. The Local binary Pattern algorithm allows to extract texture based features which has shown great results in similar systems such as face recognition. There are still many approaches out there that may be better than what are listed here and thus the work does not end here.

## 8 REFERENCES

- [1] S. F. A. Zaidi and S. Mohammed, "Biometric Handwritten Signature Recognition," 2007.
- [2] D. Morocho, A. Morales, J. Fierrez, and R. Vera-Rodriguez, "Towards human-assisted signature recognition: Improving biometric systems through attribute-based recognition," *ISBA 2016 - IEEE Int. Conf. Identity, Secur. Behav. Anal.*, 2016.
- [3] S. A. Angadi, S. Gour, and G. Bhajantri, "Offline Signature Recognition System Using Radon Transform," *2014 Fifth Int. Conf. Signal Image Process.*, pp. 56–61, 2014.
- [4] S. Hangai, S. Yamanaka, and T. Hammamoto, "ON-LINE SIGNATURE VERIFICATION BASED ON ALTITUDE AND DIRECTION OF PEN MOVEMENT," *Proc. 15th Int. Conf. Pattern Recognition. ICPR-2000*, vol. 3, no. I, pp. 479–482, 2000.
- [5] I. V Anikin and E. S. Anisimova, "Handwritten signature recognition method based on fuzzy logic,"

- 2016 *Dyn. Syst. Mech. Mach.*, 2016.
- [6] E. Ozgunduz, T. Senturk, and M. E. Karsligil, "Off-line signature verification and recognition by support vector machine," *13th Eur. Signal Process. Conf.*, no. 90, pp. 1–4, 2005.
- [7] S. A. Angadi and S. Gour, "Euclidean Distance Based Offline Signature Recognition System Using Global and Local Wavelet Features," *2014 Fifth Int. Conf. Signal Image Process.*, pp. 87–91, 2014.
- [8] Ruangroj Sa-Ardship and K. Woraratpanya, "Offline Handwritten Signature Recognition Using Adaptive Variance Reduction," *7th Int. Conf. Inf. Technol. Electr. Eng. (ICITEE), Chiang Mai, Thail. Offline*, pp. 258–262, 2015.
- [9] M. A. Djoudjai, Y. Chibani, and N. Abbas, "Offline signature identification using the histogram of symbolic representation," *5th Int. Conf. Electr. Eng. - Boumerdes*, pp. 1–5, 2017.
- [10] A. B. Jagtap and R. S. Hegadi, "Offline Handwritten Signature Recognition Based on Upper and Lower Envelope Using Eigen Values," *Proc. - 2nd World Congr. Comput. Commun. Technol. WCCCT 2017*, pp. 223–226, 2017.
- [11] T. Marušić, Ž. Marušić, and Ž. Šeremet, "Identification of authors of documents based on offline signature recognition," *MIPRO*, no. May, pp. 25–29, 2015.
- [12] S. L. Karanjkar and P. N. Vasambekar, "Signature Recognition on Bank cheques using ANN," *IEEE Int. WIE Conf. Electr. Comput. Eng.*, no. December, 2016.
- [13] G. S. Prakash and S. Sharma, "Computer Vision & Fuzzy Logic based Offline Signature Verification and Forgery Detection," *IEEE Int. Conf. Comput. Intell. Comput. Res.*, 2014.
- [14] M. S. Shirdhonkar and M. B. Kokare, "Document image retrieval using signature as query," *2011 2nd Int. Conf. Comput. Commun. Technol. ICCCT-2011*, pp. 66–70, 2011.
- [15] R. Sa-Ardship and K. Woraratpanya, "Offline Handwritten Signature Recognition Using Polar-Scale Normalization," *8th Int. Conf. Inf. Technol. Electr. Eng. (ICITEE), Yogyakarta, Indones.*, pp. 3–7, 2016.
- [16] A. Piyush Shanker and A. N. Rajagopalan, "Off-line signature verification using DTW," *Pattern Recognit. Lett.*, vol. 28, no. 12, pp. 1407–1414, 2007.
- [17] Nancy and P. G. Goyal, "Signature Processing in Handwritten Bank Cheque Images," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 2, no. 5, pp. 1239–1243, 2014.
- [18] A. T. Nasser and N. Dogru, "Signature recognition by using SIFT and SURF with SVM basic on RBF for voting online," *Proc. 2017 Int. Conf. Eng. Technol. ICET 2017*, vol. 2018–Janua, pp. 1–5, 2017.
- [19] A. Kumar and K. Bhatia, "A Robust Offline Handwritten Signature Verification System Using Writer Independent Approach," *3rd Int. Conf. Adv. Comput. Autom.*, 2017.
- [20] H. Anand, "Enhanced Signature Verification and RECOGNITION USING MATLAB," *Int. J. Innov. Res. Adv. Eng.*, vol. 1, no. 4, pp. 88–94, 2014.
- [21] B. H. Shekar and R. K. Bharathi, "Eigen-signature: A robust and an efficient offline signature verification algorithm," *Int. Conf. Recent Trends Inf. Technol. ICRTIT 2011*, pp. 134–138, 2011.
- [22] A. R. Rahardika, "Global Features Selection for Dynamic Signature Verification," *Int. Conf. Inf. Commun. Technol. Glob.*, pp. 348–354, 2018.
- [23] T. Handhayani, A. R. Yohannis, and Lely Hiryanto, "Hand Signature and Handwriting Recognition as Identification of the Writer using Gray Level Co-Occurrence Matrix and Bootstrap," *Intell. Syst. Conf.*, no. September, pp. 1103–1110, 2017.
- [24] A. Beresneva, A. Epishkina, and D. Shingalova, "Handwritten Signature Attributes for its Verification," pp. 1477–1480, 2018.
- [25] M. P. Patil, Bryan Almeida, Niketa Chettiar, and Joyal Babu, "Offline Signature Recognition System using Histogram of Oriented Gradients," *Int. Conf. Adv. Comput. Commun. Control*, 2017.
- [26] M. M. Kumar and N. B. Puhan, "Offline signature verification using the trace transform," *2014 IEEE Int. Adv. Comput. Conf.*, pp. 1066–1070, 2014.
- [27] O. Miguel-Hurtado, L. Mengibar-Pozo, M. G. Lorenz, and J. Liu-Jimenez, "On-Line Signature Verification by Dynamic Time Warping and Gaussian Mixture Models," *2007 41st Annu. IEEE Int. Carnahan Conf. Secur. Technol.*, pp. 23–29, 2007.
- [28] M. Ferrer and J. Vargas, "Robustness of offline signature verification based on gray level features," *IEEE Trans. Inf. FORENSICS Secur.*, vol. 7, no. 3, pp. 966–977, 2012.
- [29] B. Erkmen, N. Kahraman, R. A. Vural, and T. Yildirim, "Conic section function neural network circuitry for offline signature recognition," *IEEE Trans. Neural Networks*, vol. 21, no. 4, pp. 667–672, 2010.
- [30] M. A. Ferrer, A. Morales, and J. F. Vargas, "Off-line signature verification using local patterns," *2nd Natl. Conf. Telecommun.*, pp. 1–6, 2011.
- [31] M. Tahir and M. U. Akram, "Online Signature Verification using Hybrid Features," *Conf. Inf. Commun. Technol. Soc. Online*, pp. 11–16, 2018.
- [32] M. Pal, S. Bhattacharyya, and T. Sarkar, "Euler number based feature extraction technique for Gender Discrimination from offline Hindi signature using SVM & BPNN classifier," *2018 Emerg. Trends Electron. Devices Comput. Tech.*, pp. 1–6, 2004.
- [33] W. Pan and G. Chen, "A Method of Off-line Signature Verification for Digital Forensics," *12th Int. Conf. Nat. Comput. Fuzzy Syst. Knowl. Discov.*, pp. 488–493, 2016.

- [34] M. A. Ferrer, J. B. Alonso, and C. M. Travieso, "Offline geometric parameters for automatic signature verification using fixed-point arithmetic," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 27, no. 6, pp. 993–997, 2005.
- [35] S. A. Farimani and M. V. Jahan, "An HMM for Online Signature Verification Based on Velocity and Hand Movement Directions," *Iran. Jt. Congr. Fuzzy Intell. Syst.*, pp. 205–209, 2018.
- [36] G. Pirlo and D. Impedovo, "Verification of static signatures by optical flow analysis," *IEEE Trans. Human-Machine Syst.*, vol. 43, no. 5, pp. 499–505, 2013.
- [37] A. Alaei, S. Pal, U. Pal, and M. Blumenstein, "An Efficient Signature Verification Method Based on an Interval Symbolic Representation and a Fuzzy Similarity Measure," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 10, pp. 2360–2372, 2017.
- [38] D. S. Guru and H. N. Prakash, "Online Signature Verification and Recognition: An Approach based on Symbolic Representation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 6, pp. 1059–73, 2009.
- [39] A. Sharma and S. Sundaram, "On the Exploration of Information from the DTW Cost Matrix for Online Signature Verification," *IEEE Trans. Cybern.*, vol. 48, no. 2, pp. 611–624, 2018.
- [40] G. Pirlo, V. Cuccovillo, M. Diaz-Cabrera, D. Impedovo, and P. Mignone, "Multidomain Verification of Dynamic Signatures Using Local Stability Analysis," *IEEE Trans. Human-Machine Syst.*, vol. 45, no. 6, pp. 805–810, 2015.
- [41] Existing project used for comparison  
<https://github.com/Aftaab99/OfflineSignatureVerification>
- [42] Image Processing TutorialsPoint:  
<https://www.tutorialspoint.com/dip>
- [43] Machine Learning TutorialsPoint:  
[https://www.tutorialspoint.com/machine\\_learning\\_with\\_python](https://www.tutorialspoint.com/machine_learning_with_python)
- [44] Dataset source :- [http://www.iapr-tc11.org/mediawiki/index.php?title=Datasets\\_List#Handwritten%20Documents](http://www.iapr-tc11.org/mediawiki/index.php?title=Datasets_List#Handwritten%20Documents)

## 9 BIOGRAPHIES



Mr. Tejas M. Jadhav pursued Bachelor of Technology in Computer Science and Engineering from NMIMS University, Mumbai, India in 2017. He is currently pursuing Masters of Technology in Computer Science and Engineering from NMIMS University, Mumbai, India. He is currently working as Software Engineer in Diebold Nixdorf LTD, Mumbai, since 2018. His main research work focuses on Image processing, Machine Learning, Game design and development and Computational Intelligence based education. He has 1 year of working experience 3 years of Research Experience