OFFLINE SIGNATURE VERIFICATION USING CONTOUR FEATURES

Md Arif & Nayanmoni Baishya
Indian Institute of Technology Guwahati, Assam

ABSTRACT

- An offline signature verification system based on contour features is presented. The total process was divided into two parts feature selection and matching strategies. For features we used Turning Angle Scale Space(TASS) along rows and columns, Equimass Segmentation (Grid approach), Contour-hinge PDF, Contour-direction PDF, Local Binary Pattern(LBP),Fusion of different features and for classifiers we used Dynamic Time Warping(DTW), Histogram Matching, Gaussian Mixture Model(GMM), Vector-Quantization(VQ). Performance of these methods were based on the equal error rate(EER). Verification was done on a sub-corpus of the MCYT signature database. Results were comparable to existing approaches based on different features. It is also observed that combination of the proposed features does not provide improvements in performance , maybe to some existing correlation among them.

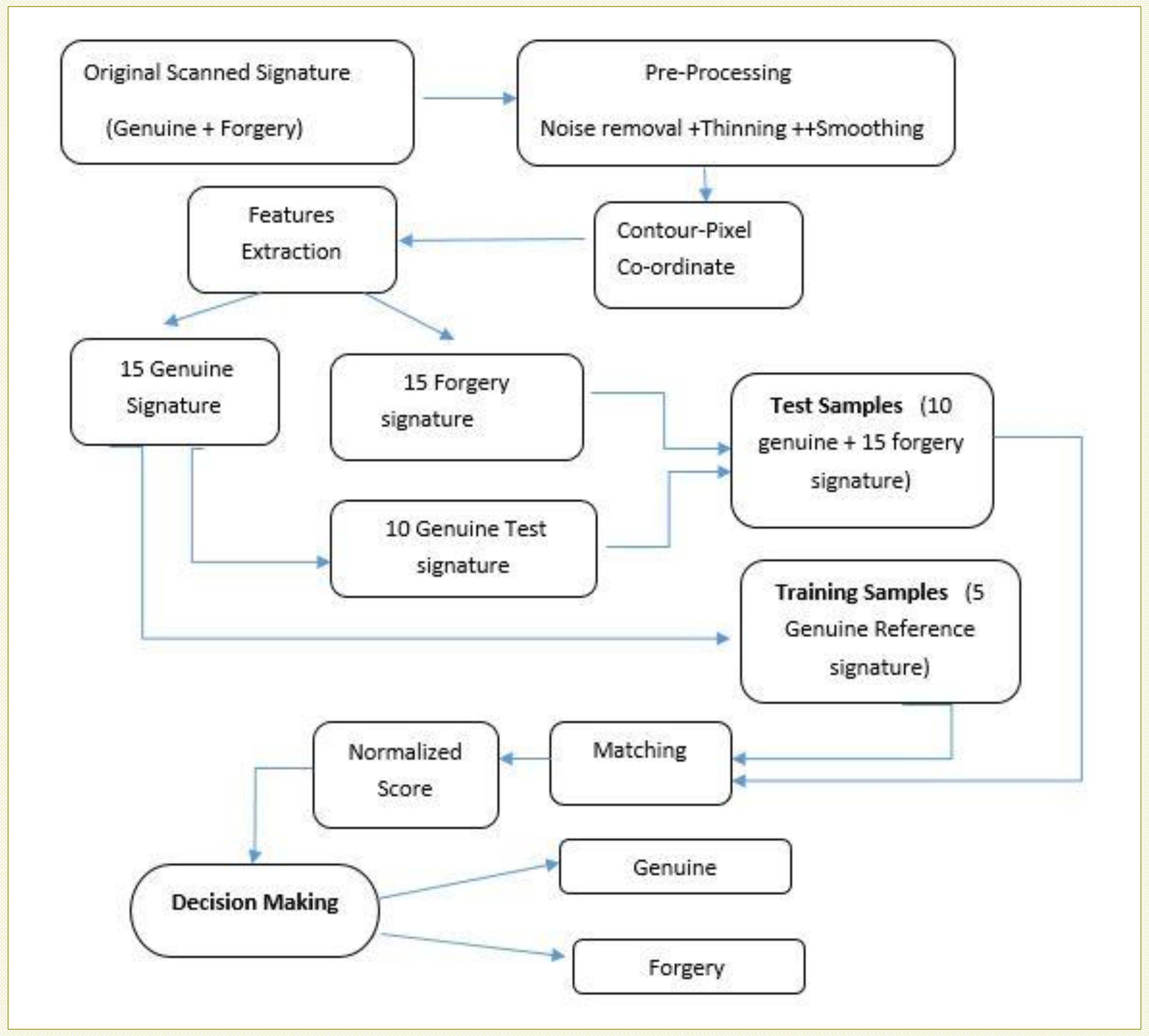
BACKGROUND

- Off-line approach are much more difficult than online because the only available information is a static two-dimensional image obtained by scanning pre-written signatures on a paper; the dynamic information of the pen-tip (stylus) movement such as pen-tip coordinates, pressure, velocity etc. cannot be captured by an image scanner. The off-line method, therefore, needs to apply complex image processing techniques to segments and analyse signature shape for feature extraction.
- The problem of signature verification becomes more and more difficult when passing from **random** to **simple** and **skilled** forgeries, the latter being so difficult a task that even human beings make errors in several cases.

OBJECTIVES

- **Feature Selection** : To extract a minimal feature set that maximizes technique interpersonal distance between signature examples of various persons while minimizing intrapersonal distance for those belonging to the same person.
- **Matching Strategies**: The performance of the signature verification system also depends on the matching strategy. To come up with an efficient matching strategy in order to achieve better results.

SCHEMATIC



Original Scanned Signature (Genuine + Forgery)

Pre-Processing
Noise removal +Thinning ++Smoothing

Contour-Pixel Co-ordinate

Features Extraction

15 Genuine Signature

15 Forgery signature

10 Genuine Test signature

Test Samples (10 genuine + 15 forgery signature)

Training Samples (5 Genuine Reference signature)

Matching

Normalized Score

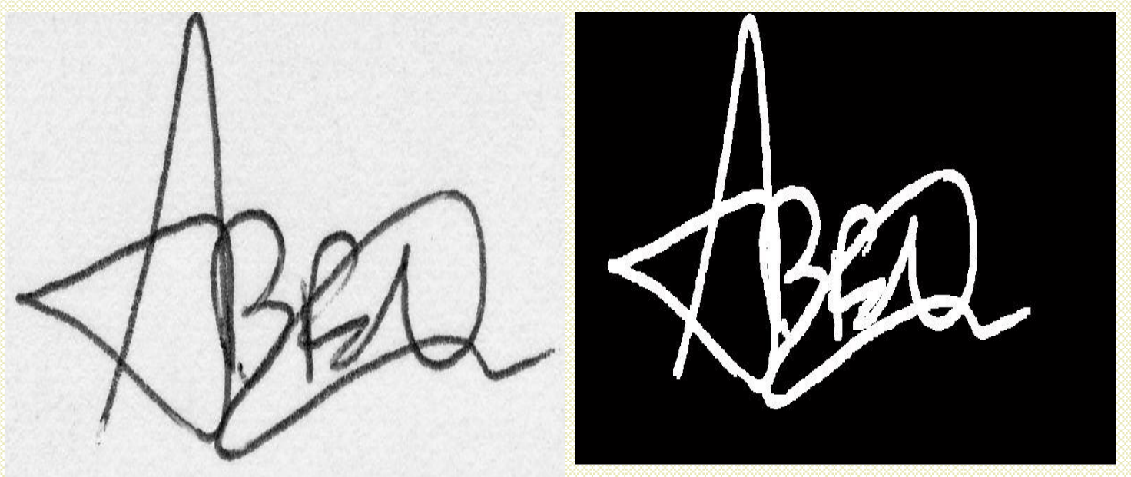
Decision Making

Genuine

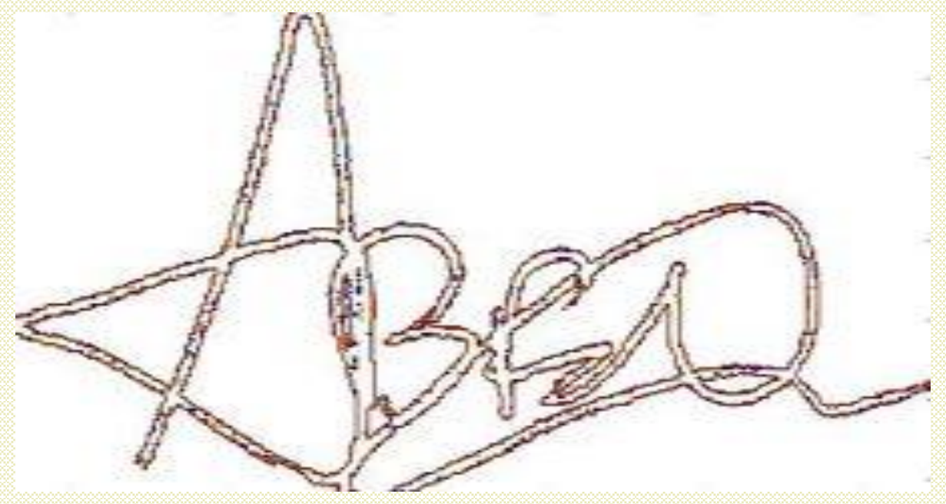
Forgery

Feature Extraction

Image Preprocessing Stage
To obtain a transformed image with enhanced quality ,removing Noise to eliminate the pixels that are not part of the signature, but contained in the image.

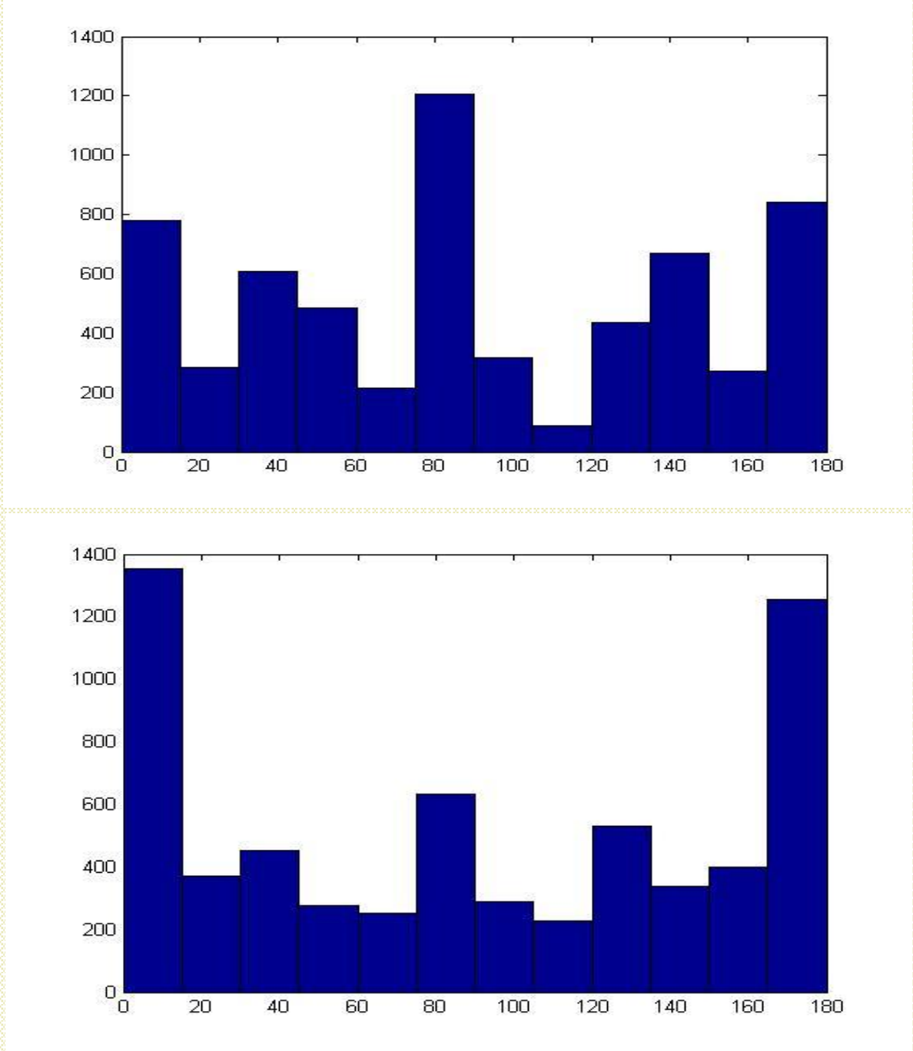


Contour Extraction
Contour pixel co-ordinates , are extracted by scanning the image from left to right and top to bottom.

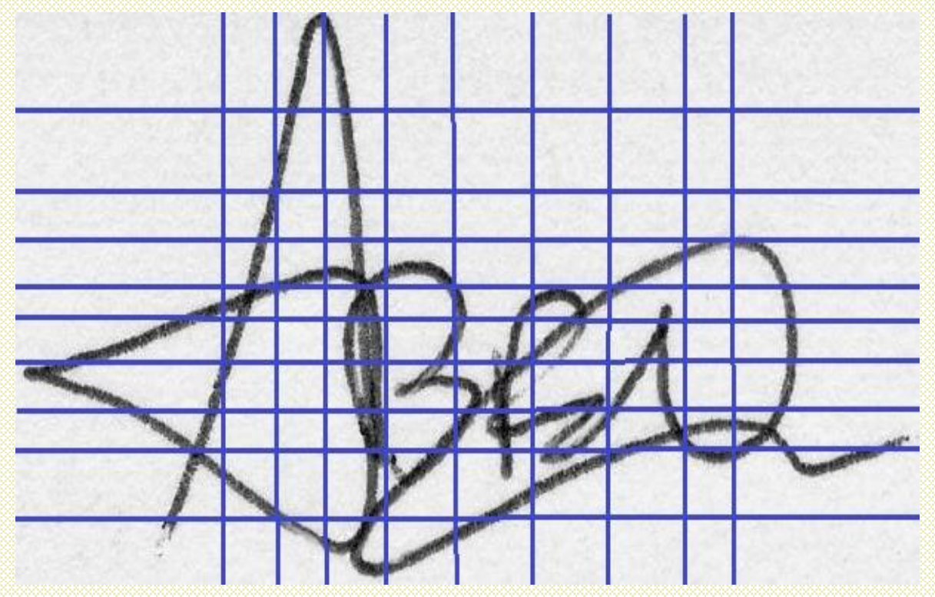


Methods opted for Turning Angle Sequence(TAS)

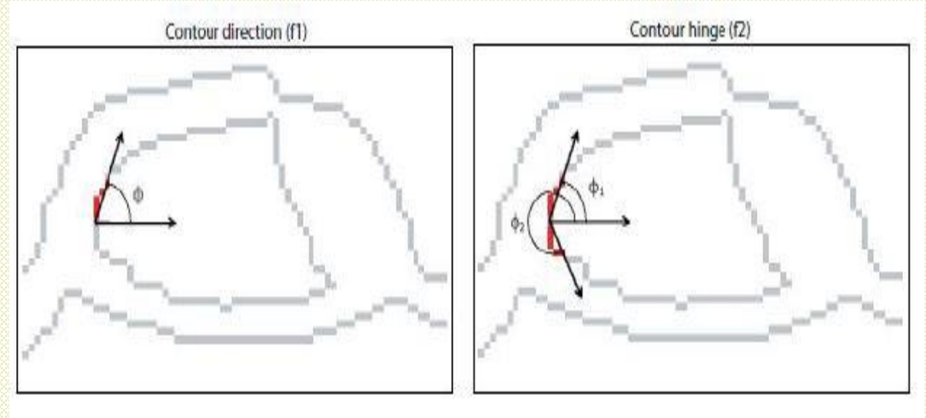
- **Global Approach**
The Turning Angle (TA) between two consecutive segments connecting three points along contour, is found along all rows and columns . The TA at a point (xk, yk) is calculated by using two points , one at (xk-r, yk-r) and the other at (xk+r, yk+r) . The variation in Turning angle description between genuine and forged signature can be seen from the histograms.



- **Local Approach**
We worked on local approach in which an Image was segmented into grids and an average of all the angles at each contour point of every grid is stacked to generate the feature vector. Signature regimentation is performed using an adaptive grid approach based on the Equimass approach, where the grid lines are found at the Equimass divisions of the horizontal and vertical mass histogram of the signature image (the mass being defined as the number of black pixels).



- **Hinge Feature**
In order to capture the curvature of the contour, as well as its orientation, the “hinge” feature is used. The main idea is to consider two contour fragments attached at a common end pixel and compute the joint probability distribution of the orientations as shown in fig.



- **Local Binary Pattern (LBP)**
A variant of lbp has been used. Around each contour point a mask (of size 7) has been taken consisting of only neighbouring contour points . The Turning Angle of the central pixel is compared with the right and left neighbouring contour points and assigned a bit value either 1 or 0. After obtaining the 6 bit binary number it is converted into its decimal equivalent(hence there were total 2^6 possible numbers).

X_{k-3}	X_{k-2}	X_{k-1}	X_k	X_{k+1}	X_{k+2}	X_{k+3}
30°	120°	10°	45°	60°	40°	150°
1	0	1		0	1	0

A bit value of [101010] and hence its decimal equivalent 42 is assigned to the central pixel Xk.

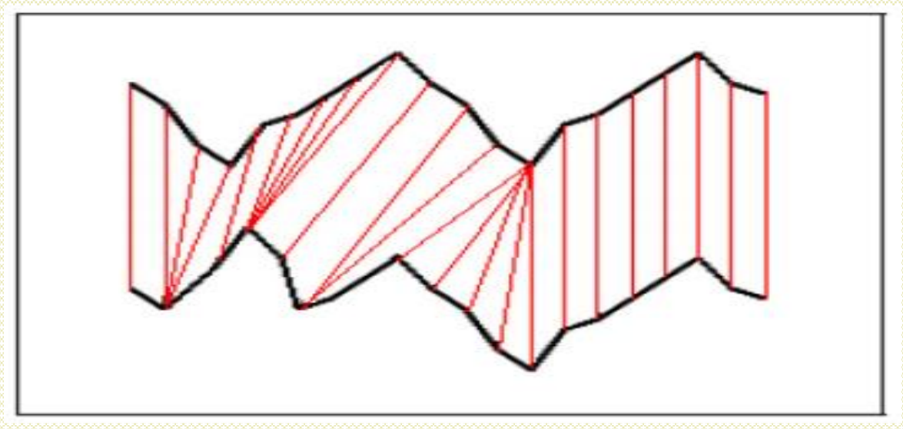
- **Fusion of different features**
Different features like those of LBP, Contour Hinge features were fused using different approaches mainly weighted sum and weighted minimum methods.

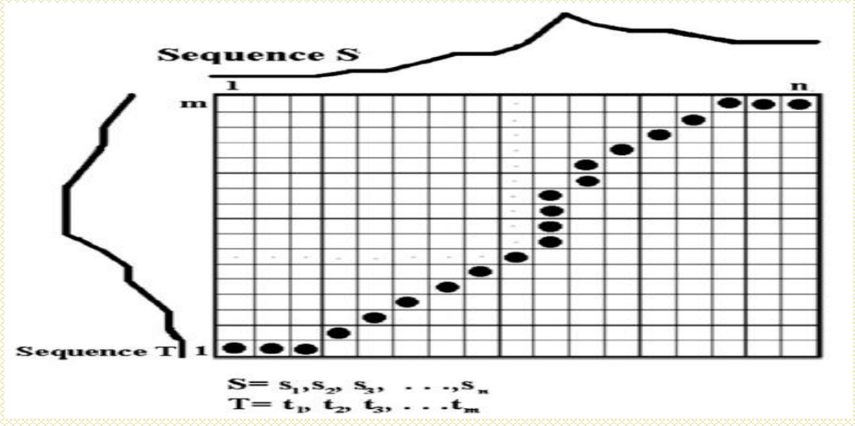
Score=(1-α) *d1 + α*d2 0<=α<=1
Weighted Sum

Score=min(α*d1,d2) 1<=α<=2
Weighted minimum

Matching Methods

DTW Algorithm
An Algorithm for measuring similarity between two temporal sequence. It finds an alignment/path which minimizes the distances by “warping” the axis of one or more of the strings to find a better alignment between points . The distance of this path becomes a measurement of similarity between two signatures; the shorter this distance, the more similar two signatures, and for identical signatures this distance will be zero.
Motivation: Used extensively in online signature verification.
Optimum path is constructed dynamically by cumulative distance.
D(i,j) = d(i,j) + min{ D(i,j-1),D(i-1,j-1), D(i-1,j) }
Total cost of matching is normalized with distance of the warping path to maintain the uniformity.





Histogram Matching
Each client of the system is represented by a PDF that is computed using an enrolment set of *5* signatures . For each feature, the histogram of the *5* signatures together is computed and then normalized to a probability distribution.
To compute the similarity between a claimed identity *q* and a given signature i, the ‘chi’ distance is used where *p* are entries in the PDF, *n* is the bin index, and *N* is the number of bins in the PDF (the dimensionality).

$$\chi^2_{qi} = \sum_{n=1}^{N} \frac{(p_q[n] - p_i[n])^2}{p_q[n] + p_i[n]}$$

Gaussian Mixture Model (GMM)
Gaussian Mixture Model (GMM) has been used for training our samples. For this we have taken 5 genuine signatures of each user and extracted the features from all of the samples after proper pre processing steps. The training phase uses Gaussian Mixture Model (GMM) technique to obtain a reference model for each signature sample of a particular user. The number of clusters or Gaussians to be used is provided by the users When the model gets trained, it is used to find the similarity rate between the query data (test set) and the model. By computing Euclidean distance between reference signature and all the training sets of signatures, acceptance range is defined. If the Euclidean distance of a query signature is within the acceptance range then it is detected as an authenticated signature else, a forged signature.

Results

DTW + TAS

Feature Extraction Approach	MEER (in %)
1.TAS only along rows	26
2. TAS only along columns	27
3. TAS along rows and column both	18
4. X and Y co-ord along with TAS	25

DTW + Equimass Segmentation

Grid Size	MEER (in %)
16 partitions of image (r=4)	20
49 partitions of image (r=7)	18

Histogram Matching +Contour-Hinge pdf + Contour- Direction pdf

Hinge Feature	MEER (in %)
Contour-Direction pdf (f1)	13.7
Contour-Hinge pdf(f2)	12.3
Contour-Direction pdf (f1)+ Contour-Hinge pdf(f2)	10.68

Histogram Matching LBP + TAS

Mask Size	MEER (in %)
4 Neighbour (4 bits)	25
6 Neighbour (6 bits)	22.1

GMM +Contour-Direction pdf(f2)

Cluster Size	MEER (in %)
64	28
128	24

Histogram Matching + Hinge + LBP

alpha	MEER (in %)
$\alpha = 0.7$	10.12
$\alpha = 0.5$	12.69
$\alpha = 0.3$	15.45

The lowest MEER obtained for the dataset is **10.12%** for skilled forgeries and **3.4%** for random forgeries using fusion of lbp and hinge features. Experimental results are given using 2250 different signature mages of 75 contributors extracted from the MCYT signature database. The methods achieved satisfactory Mean Equal Error Rate(MEER) of 10.12%(Hinge +LBP), 10.69%(Hinge Features f1 +f2), 22%(GMM).

CONCLUSIONS & FUTURE WORK

- The combination of features does not result in performance improvement, maybe due to the correlation among them. Verification results are comparable to other existing approaches for offline signature verification based on different features using the same experimental framework.