ISSN No. 0976-5697

Volume 4, No. 10, September-October 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Offline Signature Verification based on Pixel Oriented and Component Oriented Feature Extraction

Swati Srivastava*
Computer Science & Engineering
Dr. K.N.Modi Foundation
Modinagar, India
Swati.cs1409@gmail.com

Suneeta Agarwal
Computer Science & Engineering
Motilal Nehru National Institute of Technology
Allahabad, India
Suneeta@mnnit.ac.in

Abstract: Signature verification is one of the most widely used biometrics for authentication. The proposed technique is based on pixel oriented and component oriented features extraction. The aim of the proposed work is to develop an automatic signature verification system which takes the input signature of the known user and either accepts or rejects it after extracting and comparing the different pixel oriented and component oriented features of the input signature with the already trained features of the reference signature.This technique is suitable for various applications such as bank transactions, passports etc. The threshold used in the proposed technique can be dynamically changed according to the target application. Basically, the threshold here is the security level which the user can input as per his requirement. The proposed technique deals with skilled forgeries and has been tested on two databases: Database A and a standard Database B (Set 1 and Set 2). The proposed technique gives FAR of 9.63% and FRR of 8.46% for Database A, FAR of 12.21% and FRR of 10.40% for Database B (Set 1) and FAR of 15.87% and FRR of 13.72% for Database B (Set 2) which is better than many existing verification techniques.

Keywords: Offline Signature Verification, Skilled Forgery, Grid Feature Extraction**,** False Acceptance Rate (FAR), False Rejection Rate (FRR), Pixel oriented features, Component oriented features.

I. INTRODUCTION

Signature verification is a biometric verification which is an important research area targeted at automatic identity verification applications such as legal, banking and other high security environments. Such applications need their own exclusive software for signature verification. Biometrics based authentication systems are better in terms of security than traditional authentication techniques such as passwords etc. It is due to the fact that biometric characteristics of every person are unique and cannot be lost, stolen or broken. There are two types of biometrics: Behavioral and Physiological. Handwriting, speech etc. come under behavioral biometrics. Iris pattern, fingerprint etc. are part of physiological biometrics. There are two methods for signature verification: Offline and Online, which depends on the signature acquisition method. In offline signature verification, after having complete signature on the paper, it can be acquired from scanners or cameras. In online method, during signing process, it can be acquired in parallel with digitizing tablets or any other special hardware. The purpose of signature verification is to classify the input signature as genuine or forge by matching it against the database signature image using some distance measure. Forgery means that an individual is trying to make false signatures of any other individual to become authenticated. There are three types of forgeries[2]:

- ***a. Random Forgery:*** This is also known as simple forgery and is very easy to detect. The signer creates a signature in his own style by just knowing the name of an individual whose sign is to be made.
- ***b. Unskilled Forgery:*** The signer creates a signature after observing the signature once or twice without any prior experience.
- ***c. Skilled Forgery:*** The signer may be a professional in copying signatures. He creates a signature after having a good practice over it. Such signatures are most difficult to detect.

II. PROPOSED METHOD

From previous studies, it has been observed that an offline signature verification process consists of following steps:

(i) Signature Acquisition
(ii) Signature Pre-processing
(iii) Feature Extraction
(iv) Signature Verification

(i) Signature Acquisition: Signature made on A4 paper were acquired by scanner having 300dpi and stored in Portable Network Graphics (PNG) format. “Fig.1” shows some sample signatures from database on which proposed technique have been tested.

Figure.1: Sample Signatures[11]

(ii) Signature Preprocessing: To verify a signature correctly, preprocessing of acquired signature is required. The acquired signature image as shown in “Fig.1” may sometimes contain noise (extra pen dots other than signature). It is necessary to remove these extra pixels from acquired image for correctly verify the signature. This can be done by using median filters.

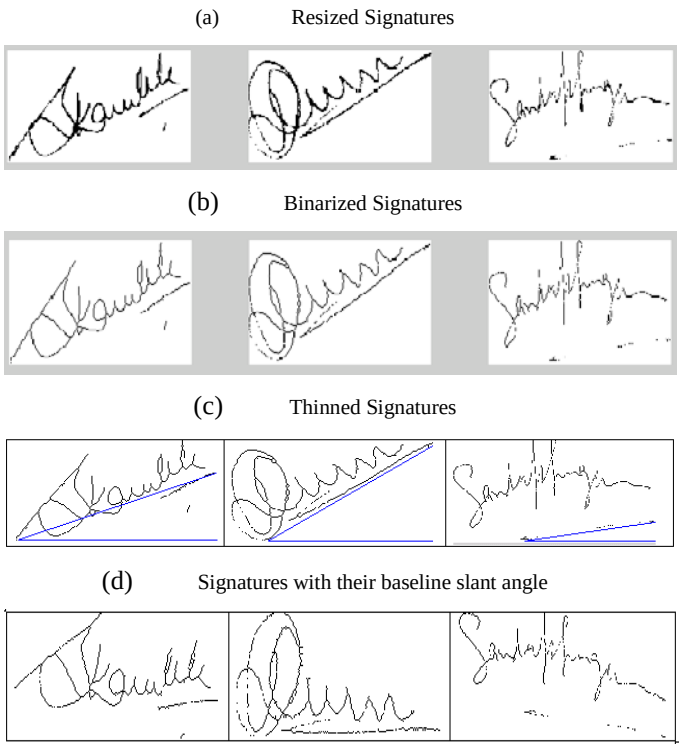

Figure.2: Pre-processing Phase[11]

Pre-processing includes some more operations like resizing, binarization, thinning and rotation normalization. First step in pre-processing is to resize the acquired signature to a standard size (100x200) using resize algorithm shown in "Fig.2 (a)". Binarization means black and white version of the resized (RGB) signature shown in "Fig.2 (b)". Thinning is basically a morphological operation which is applied to binary image to obtain one pixel run of a signature or skeleton of a signature shown in "Fig.2(c)". To obtain rotation invariant image, first baseline slant angle [8] of the image is to be calculated and then the image is rotated by that angle in clock-wise direction as shown in "Fig. 2(d)" and "Fig.2(e)". The result of pre-processing phase is noise free, resized, binarized, thinned and rotation normalized signature image.

(iii) Feature Extraction: The objective of this phase is to extract the features of the test image that will be compared to the features of training image for verification purpose. There are two types of features [5]: (i) Function features and (ii) Parameter features. Function features include position, velocity, pressure etc. and are used in online verification techniques. Parameter features are further divided into global parameters and local parameters. Global parameters include Fourier transform, wavelet transform etc. Local parameters are further divided into component-oriented and pixel-oriented. Component-oriented features include contour based, geometric based, slant based etc. Pixel-oriented features include grid based, intensity based etc. Here we have extracted 9 features from the pre-processed signature image and then used these features in verification phase. The features are as follows:

I. Pixel-Oriented Features(to be Globally Extracted):

a. A m x n matrix corresponding to a m x n grid
b. An array of size m
c. An array of size n

II. Component-Oriented Features(to be Locally Extracted):

a. CGx[8]
b. CGy[8]
c. CG Slope[8]
d. Normalized sum of angles of all points of the signature content
e. Contour Area
f. Aspect Ratio[9]

A. Global Feature Extraction:

a. A m x n matrix corresponding to a m x n grid[11]:

After pre-processing we have a signature of size 100x200(pixels). Then we make a grid of m x n where m < n, m <<100 and n <<200, over a pre-processed signature as shown in "Fig.3". Here we have taken m=10 and n=20. Thus, a signature image is divided into 200 square cells where each cell is having 100 pixels. We have done such segmentation of the signature image so that more efficient and effective comparisons can be done which can easily detect the forgeries. Next we find out the cells of a row of a grid that are containing the signature content. Notice that signature content is calculated in terms of black pixels, therefore only those cells should be considered which are having 3 or more black pixels. Repeat the process for all rows of a grid. Thus we have all those cell positions which are part of the signature image. Now we create a matrix of size m x n corresponding to the grid of size m x n i.e. one cell of a grid corresponds to one element of a matrix. The matrix element is equal to 1 if the cell of same position in the grid is the part of signature, otherwise the matrix element will be 0. Thus, as a result of this step, we have a matrix having elements 0 or 1 accordingly as shown in "Fig. 4".

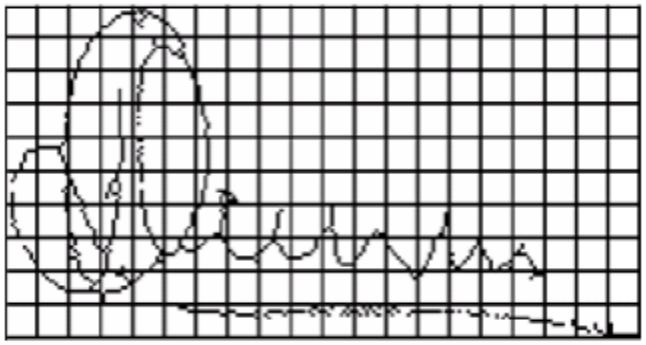

Figure.3: Grid over pre-processed signature image

0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	1	1	1	1	0	1	0	1	1	0	1	0	0	0	0	0	0
1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0
0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Figure.4: Matrix corresponding to the above grid

b. An array of size m[11]:

Calculate the number of black pixels in cells of a row containing signature content and put the value in an array. Repeat the process for all rows.

$A_m = [c_1, c_2, c_3, \ldots\ldots\ldots\ldots\ldots, c_m]$

Where c_m is no.of blackpixels in m^{th} row.

c. An array of size n [11]:

The same process can be applied to columns. Thus we get another array having n elements corresponding to each column.

$A_n = [c_1, c_2, c_3, \ldots\ldots\ldots\ldots\ldots, c_n]$

Where c_n is no.of blackpixels in n^{th} column.

B. ***Local Feature Extraction:*** Features of each cell of a grid are to be extracted.

a. CGx:

It is the center of gravity with respect to x direction. It is defined as the mean of x positions of the black pixels of the signature image.

$$CG_x = \frac{\sum_{i=1}^{n} x_i}{n} \quad (1)$$

Where n=no. of black pixels in the signature image, x_i is the value of x coordinate of i^{th} black pixel.

b. CGy:

It is the center of gravity with respect to y direction. It is defined as the mean of y positions of the black pixels of the signature image. "Fig.5(a)" shows the point which indicates the center of gravity (CG_x,CG_y).

$$CG_y = \frac{\sum_{i=1}^{n} y_i}{n} \quad (2)$$

Where n=no. of black pixels in the signature image, y_i is the value of y coordinate of i^{th} black pixel.

c. CG Slope:

Signature image is partitioned into two equal halves. Find out the center of gravity of the first half and second half separately. Center of gravity of the image is the mean of all black pixels in the image. Then join the two centers of gravity with a line. Now CG Slope can be defined as the angle between this line and the horizontal as shown in "Fig. 5(b)".

d. Normalized sum of angles of all points of the signature content:

Find out the coordinates of all the black pixels of the signature image. From each point draw a line joining the origin as shown in "Fig.5(c)". Then find the angle of each point from horizontal. Find the sum of all the angles and normalize it by dividing with the number of points.

e. Contour Area:

A shape obtained after joining each point of the signature image to the origin has been taken as contour. Filled contour is shown in "Fig.5(d)". Contour area can be defined as total number of black pixels in the contour.

f. Aspect Ratio:

It is the width to height ratio of the image and can be calculated as:

$$\text{Aspect Ratio} = \frac{\text{width}}{\text{height}} \quad (3)$$

Where width [9] is the distance between two points in the horizontal projection and must contain more than 3 pixels in a cell, height [9] is the distance between two points in the vertical projection and must contain more than 3 pixels in a cell.

(iv) Signature Verification:

The purpose of verification phase is to compare the test image with training image using extracted features and to decide whether the test image is original signature of the writer or forgery. In the proposed technique, verification phase includes two parts: Global Verification and Local Verification.

Threshold: Here the threshold is taken as the security level which the user wants to achieve in the target application. Threshold range[11] is from 100 to 65 i.e. lowest security level for which results can be obtained in the proposed system, is 65. Since the proposed technique works for a range of security levels, it can be used in various applications in which different level of security is required for different applications.

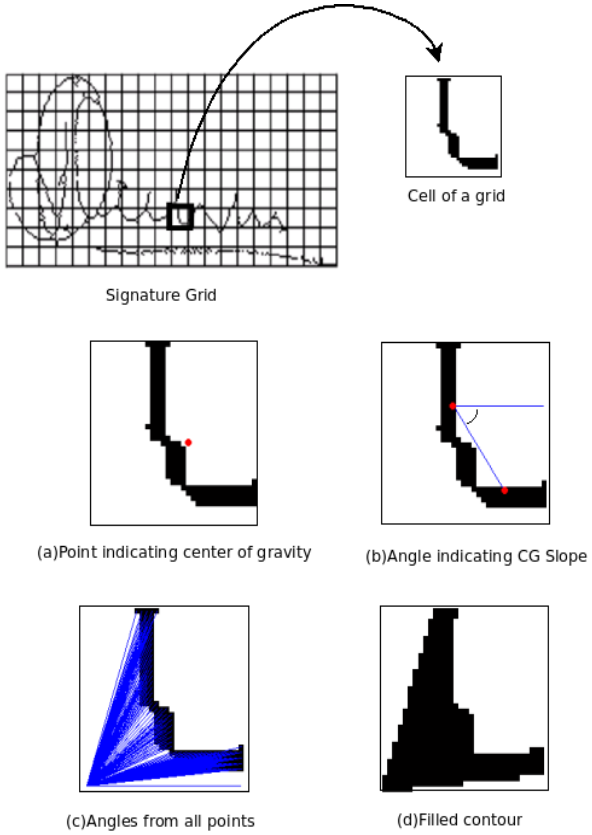

Figure.5: Local Feature Extraction

A. Global Verification:

***(i)* Calculate Column Matching Score (CMS)[11]**

a) Let M_1 and M_2 be the matrices of reference image and test image respectively. Compare the columns of the matrix M_2 with M_1. Each column is having m elements. If at least β, where $\beta \geq 7$, elements are same then that column is said to be matched and increase the column count C_1 (say) by one.

b) Let A_1 and A_2 be the arrays of reference image and test image respectively containing number of black pixels in each column. Compare the corresponding

elements of array A_2 with A_1. Now check the following condition:

$$\sigma_{Ref} - \propto < \sigma_{Test} < \sigma_{Ref} + \propto \quad (4)$$

Where, σ_{Ref} is the element of reference array A_1, σ_{Test} is the corresponding element of the test array A_2 and α is the tolerable factor which is the allowed variation in number of pixels. Tolerable factor is a dynamic value as it varies for different columns depending on the signature content in that column. Tolerable factor can be calculated as:

$$\propto = \frac{p \times \sigma_{Ref}}{100} \quad (5)$$

Where, p is percentage of black pixels in a column of a grid and σ_{Ref} is the number of black pixels in that column, p can be obtained as:

$$p = \frac{\sigma_{Ref}}{N} \times 100 \quad (6)$$

Where, N is total area of the cells having black pixels in that column and can be calculated as:

$$N = (width \times height) \times c \quad (7)$$

Where, c is the number of cells which are part of the signature in that column of a grid, width [9] is the distance between two points in the horizontal projection and must contain more than 3 pixels in a cell, height [9] is the distance between two points in the vertical projection and must contain more than 3 pixels in a cell. If condition (4) satisfies then that column is acceptable and increase the counter C_2 (say) by one.

c) If $C_1 = n$ and $C_2 = n$, then CMS is said to be 100% . Similarly for $C_1 = n - i$ and $C_2 \geq n - i$ where i= 1,....,8, CMS will be $\left[\frac{n-i}{n} \times 100\right]$ % i.e. signatures upto 60% CMS are considered for further processing. If CMS is below 60% then the test signature will be classified as forgery at this step itself.

(ii) **Calculate Row Matching Score (RMS)[11]**

If CMS ≥ 60% then only we are interested in calculating Row Matching Score (RMS). It can be obtained similarly as CMS. All comparisons have to be done row wise. For RMS, $\beta \geq 14$. Calculate C_1 and C_2 for this case.

(iii) **Calculate the Average of CMS and RMS** The values of CMS and RMS obtained in above steps are used to calculate the average.

If the user wants 100% security then input will be 100 and if the average of the CMS and RMS is 100 then the signature will be accepted. If the user wants 95% security then input will be 95 and if the average is greater or equal to 95 then the signature will be accepted and so on. If average is below 65% then that signature will be classified as forge.

B. Local Verification:

For local verification, we use three genuine signatures of a signer as learning images. We treat each cell of a grid as a single image. Now we calculate the all the six features for all cells of the grid. Thus we get the six values for each cell for the three learning images. In other words, we can say that we get three values of each feature for each cell. Now we calculate the values of all six features for the cells of the test image. For verification we compare all six values of a cell of test image with the corresponding values of the learning images. If the value of the feature for a cell of test image is γ where $min_i \leq \gamma \leq max_i$ where min_i is the minimum value of the i^{th} feature, max_i is the maximum value of the i^{th} feature among the three learning images, then the feature value is said to be accepted. If all the six features are accepted, then increase the counter C_3 (say) by one. For 100% security, the input threshold will be 100, and if C_3=100% of m x n then it is said to be accepted. If the user wants 95% security then input will be 95 and if $C_3 \geq$ 95% of m x n then the test image is said to be accepted and so on. If C3 < 65% of m x n then that signature will be classified as forge.

The verification phase may be concluded by performing an AND logic test upon the global and local verifications i.e. if the test image is accepted for both global and local verifications then the signature is said to be accepted. “Fig. 6” shows the proposed verification technique.

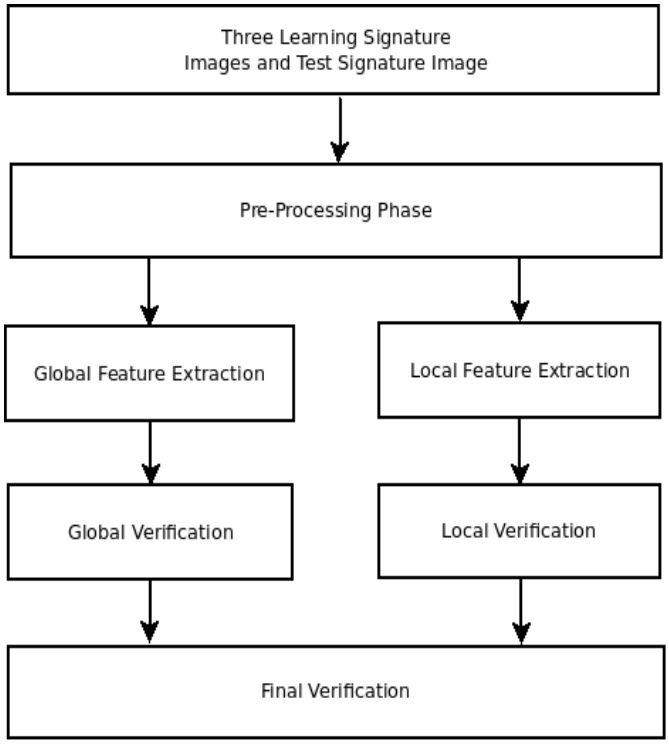

Figure.6: Block Diagram of the Proposed Signature Verification Technique

III. EXPERIMENTAL RESULTS

Two signature databases have been used to perform experiments: Database A and Database B. For database A, 50 persons were asked to contribute 10 signatures each i.e. 500 genuine signatures. 10 forge signatures per person were needed for which 5 volunteers were asked to make skilled forgeries. For practice photocopies have been given to them so that they can make fair skilled forgeries. Thus 500 skilled forge signatures were also collected. Thus Database A consists of 1000 signatures having 500 genuine and 500 skilled forgeries collected over a period of time. Database B is publicly available on http://www.vision.caltech.edu/ mariomu/research/data [1]. Database B has two sets. In Set 1, there are 56 writers with 25 genuine signatures per writer and 10 forgeries per writer. In set 2, there are 50 writers with 30 genuine signatures per writer and 10 forgeries per writer. Proposed technique has been tested on the above databases. FAR and FRR are the two parameters [3] used for

measuring the performance of any signature verification method.

a. FAR (False Acceptance Rate): The percentage of falsely accepted forgeries is called the False Acceptance Rate (FAR) and is given by:

$$\text{FAR} = \frac{\text{No.of forgeries accepted}}{\text{No.of forgeries tested}} \text{ x } 100 \quad (8)$$

b. FRR (False Rejection Rate): The percentage of original signatures that are falsely rejected by the system is called the False Rejection Rate (FRR) and is given by:

$$\text{FRR} = \frac{\text{No.of originals rejected}}{\text{No.of originals tested}} \text{ x } 100 \quad (9)$$

The purpose of verification system is to reduce FAR and FRR. FAR and FRR have been calculated to evaluate the performance of the proposed system. Different values of threshold are needed to plot FAR versus FRR graph. Here threshold is the security level which can be set according to the target application. This graph, sometimes called the Equal Error Graph, is one of the most often used by researchers trying to understand the performance of their verification system. It shows the False Accept and False Reject Rates at all thresholds. Minimizing the crossover of the two plots is generally the goal of the verification system.

A. ROC Curve[11]:

The ROC (Receiver Operating Characteristic) plot is a visual characterization of the tradeoff between the FAR and the FRR. In FAR vs FRR plot, the EER is defined as the crossover point on a graph. Also from ROC curve, which plots FAR against FRR, to determine a particular system's accuracy, the EER can be calculated. To calculate the ROC of a biometric system, each corresponding FAR and FRR point is plotted, the EER is then obtained by extending a 45-degree line from the point of origin (0, 0). The point where this 45-degree line crosses the ROC curve gives the EER.

B. Results for Database A:

From Table 1 it can be seen that as threshold increases, FAR decreases while FRR increases. For the database used here, FAR is 9.63% and FRR is 8.46%. FAR vs FRR graph gives the percentage error of the system. Equal Error Rate (EER) that is the point where FAR and FRR becomes equal is 9.04% as shown in Fig.7. ROC curve for this database is shown in Fig.8.

C. Results for Database B:

From Table 2 and 3, it can be seen that for Set 1 FAR is 12.21% and FRR is 10.40% and for Set 2 FAR is 15.87% and FRR is 13.72% . EER for Set 1 is 11.30% and EER for Set 2 is 14.79% . "Fig.9 and 10" shows the FAR vs FRR graph for Set 1 and Set 2 respectively.

Table I. Signature Verification Results for Database A

Threshold	*FAR(%)*	*FRR(%)*
65	26.65	0
70	19.78	3.11
75	13.23	5.23
80	9.63	8.46
85	6.41	12.96
90	5	19.12
95	1.12	23
100	0	25.89

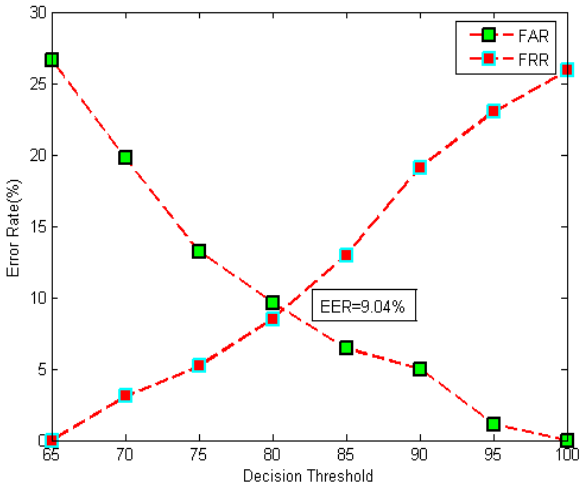

Figure.7.FAR vs FRR graph for Database A

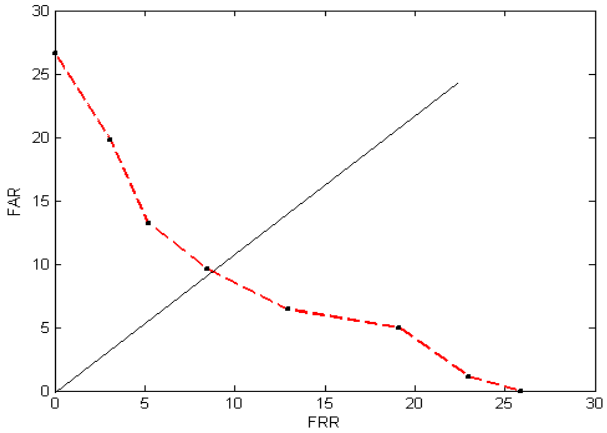

Figure.8: ROC Curve for Database A

Table II. Signature Verification Results for Database B (Set 1)

Threshold	*FAR(%)*	*FRR(%)*
65	30.77	0
70	26.13	1.16
75	18.32	4
80	12.21	10.40
85	9.92	13.12
90	5.17	17.42
95	1.83	23.97
100	0	26.89

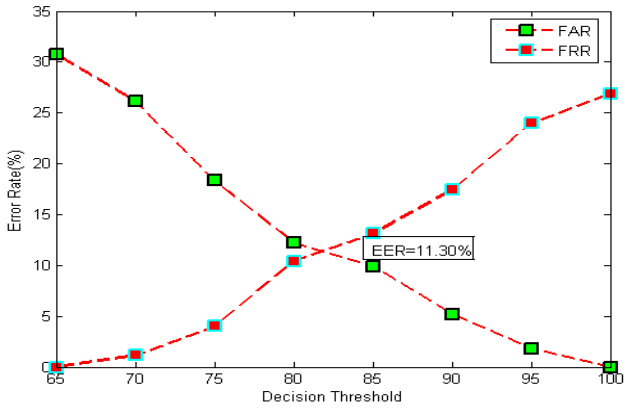

Figure.9: FAR vs FRR graph for Database B (Set 1)

Table III. Signature Verification Results for Database B (Set 2)

Threshold	*FAR(%)*	*FRR(%)*
65	31.76	0
70	28	1.93
75	21.91	5.40
80	15.87	13.72
85	11.98	17.61
90	5.84	22.26
95	1.18	24.15
100	0	26.19

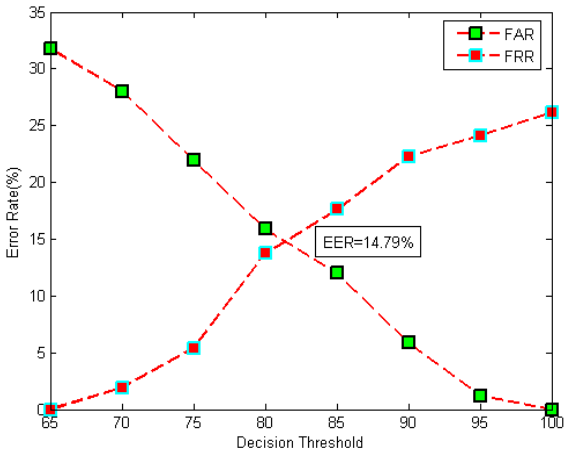

Figure.10. FAR vs FRR graph for Database B (Set 2)

D. Comparative Study:

From experimental results it has been observed that for Database A, the proposed technique gives FAR of 9.63% for skilled forgeries and FRR of 8.46%. The EER for Database A is 9.04%. For Database B (Set 1), FAR is 12.21%, FRR is 10.40% and EER is 11.30%. For Database B (Set 2), FAR is 15.87%, FRR is 13.72% and EER is 14.79%. First comparison used the same standard Database B. From Table 4, it has been observed that proposed technique gives better results than many existing techniques.

Table IV. Comparison with Existing Techniques

Technique	**FAR(%)**	**FRR(%)**
Offline Signature verification using Distance Statics [ ]	34.91(Set1) 33.80(Set 2)	28.33(Set 1) 30.93(Set 2)
Novel Features for Offline Signature verification[ ]	16.36	14.58
Offline Signature Verification using Local Radon Transform & SVM[ ]	22.0	19.0
Proposed Technique (Database A)	9.63	8.46
Proposed Technique (Database B)	12.21(Set 1) 15.87(Set 2)	10.40(Set 1) 13.72(Set 2)

IV. CONCLUSION

Here an offline signature verification technique using pixel oriented and component oriented feature extraction has been discussed. The preprocessed signature i.e. resized, binarized, thinned and rotation normalized signature is segmented into grid of size 10x20 cells where each cell is having 100 pixels. Pixel oriented features such as matrix corresponding to grid and arrays containing number of black pixels in rows and columns are extracted. Also component oriented features such as center of gravity in x direction, center of gravity in y direction, center of gravity slope, normalized sum of angles of all points of the signature content, contour area, aspect ratio are extracted. Pixel oriented features for training and test images are compared for global verification and component oriented features for training and test images are compared for local verification. Apply AND logic test to the results of global and local verifications and the test signature is then classified accordingly. Proposed technique deals with the skilled forgeries and gives better results in terms of FAR and FRR than many existing verification techniques.

V. ACKNOWLEDGMENT

We wish to thank all the people who have helped us by obliging to give sample signatures for testing our technique. We also want to acknowledge the support of our family and friends without which this paper would not have been a reality.

VI. REFERENCES

[1]. Meenakshi K. Kalera, Sargur Srihari and Aihua Xu, 2004,"Offline Signature Verification and Identification using Distance Statistics," International Journal of Pattern Recognition and Artificial Intelligence, Vol.18, No.7, pp.1339-1360.

[2]. Madasu Hanmandlu, Mohd.Hafizuddin Mohd. Yusof, Vamsi Krishna Madasu,2005,"Offline Signature Verification and Forgery Detection using Fuzzy Modeling,"The Journal of the Pattern Recognition Society,Vol.38, pp.341-356.

[3]. Banshider Majhi, Y Santhosh Reddy, D Prasanna Babu, 2006, "Novel Features for Offline Signature Verification,"International Journal of Computers,Communications & Control, Vol. I, No. 1, pp. 17-24.

[4]. Debasish Jena, Banshidhar Majhi, Saroj kumar Panigrahy, Sanjay Kumar Jena, ICCI 2008,"Improved Offline Signature Verification Scheme Using Feature Point Extraction Method," Proc. 7th IEEE Int. Conference on Cognitive Informatics, pp. 475-480.

[5]. Donato Impedovo, Giuseppe Pirlo, 2008,"Automatic Signature Verification: The State of the Art," IEEE Transactions on Systems, Man and Cybernetics-Part C: Applications and Reviews, Vol.38, No.5, pp.609-635.

[6]. Sohail Zafar, Rashid Jalal Qureshi, 2009,"Offline Signature Verification Using Structural Features," Proceedings of the 7th International Conference on Frontiers of Information Technology.

[7]. Mishra, Prabit Kumar and Sahoo, Mukti Ranjan, 2009,"Offline Signature Verification Scheme".

[8]. Priyanka Chaurasia, 2009,"Offline Signature Verification using High Pressure Regions," Patent No. US 7,599,528 B1.

[9]. Dakshina Ranjan Kisku, Phalguni Gupta, Jamuna Kanta Sing, IJSIA 2010,"Offline Signature Identification by Fusion of Multiple Classifiers using Statistical Learning Theory," Computer Vision and Pattern Recognition.

[10]. Vahid Kiani, Reza Pourreza, Hamid Reza Pourezza, 2010,"Offline Signature Verification Using Local Radon Transform and Support Vector Machines," International Journal of Image Processing (IJIP), Vol.3, No.5, pp.184-194.

[11]. Swati Srivastava and Suneeta Agarwal, "Offline Signature Verification using Grid based Feature Extraction," 2nd IEEE International Conference on Computer & Communication Technology (ICCCT-2011), pp.185-190.