A Grid based Offline Signature Verification System

Suraj Kumar Dubey[1] A.K.Shukla[2]
[1]M.Tech. Student [2]Assistant Professor
[1,2]Department of Computer Science & Information Technology
[1,2]Sam Higginbottom Institute of Agriculture, Technology & Sciences, Allahabad

Abstract— Signatures is an important biometric because it is still widely used as a means of personal verification and hence an automatic signature verification system is needed. In this paper we present an off-line signature verification and recognition system based on tree and grid based features extracted such as pixels in tree, eccentricity, center etc. The main advantage of this system is it does not require already trained dataset.. Verification is perform on runtime with only one genuine and test signature. Finally decision making is done on the majority basis. Since three feature are used hence authenticity is decided on the favor of two or more that two features. Experimental results show the effectiveness of proposed approach.

Key words: Offline Signature Verification System, Automatic Signature Verification System

I. INTRODUCTION

Signature verification is one of the most widely used biometrics for authentication. 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: Behavioural and Physiological. Handwriting, speech etc. come under behavioural biometrics. Iris pattern, fingerprint etc. are part of physiological biometrics. In signature verification, system knows the owner of the input signature and system has to match the input signature with the stored signature of the owner to find the authenticity of the input signature. Signature has been a distinguishing feature for person identification. The purpose of signature verification is to decide if a particular input signature is authentic or a forgery. In other words, we can say that 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.

II. NEED FOR SIGNATURE VERIFICATION

Today an increasing number of transactions, especially related to financial and business are being authorized via signatures. Hence the need to have methods of automatic signature verification must be developed if authenticity is to be verified. Approaches to signature verification fall into two categories according to the acquisition of the data: Online and Offline.

III. VERIFICATION APPROACHES

A. Online Signature Verification

Online data records the motion of the stylus while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time. Online systems use this information captured during acquisition. These dynamic characteristics are specific to each individual and sufficiently stable as well as repetitive. Due to the involvement of the dynamic features, it is difficult to intimate the signature.

B. Offline Signature Verification

Offline data is a 2-D image of the signature. In offline signature verification, after having complete signature on the paper, it can be acquired from scanners or cameras. Processing offline signature is complex due to the absence of stable dynamic characteristics. Difficulty also lies in the fact that it is hard to segment signature strokes due to highly stylish and unconventional writing styles. The nature and the variety of the writing pen may also affect the nature of the signature obtained. The non-repetitive nature of variation of the signatures, because of age, illness, geographic location and perhaps to some extent the emotional state of the person, accentuates the problem. All these coupled together cause large intra-personal variation.

Kisku, D. R., et al. (2010) presented score level fusion of multiple matchers for offline signature identification The proposed system has used global and local features to the classifiers, namely, Euclidean, Mahalanobis distances and Gaussian empirical rule. Matching score was obtained by fusing these classifiers along with SVM.

Malekar, M.D., et al. , (2013) , proposed the off-line signature verification and recognition using a new approach that depends on a artificial neural network which discriminate between two classes (i) forgery and (ii) original signature. They proposed scheme which is based on the technique that applies pre-processing on the signature, feature point extraction and neural network training and finally verifies the authenticity of the signature.

Kiani, V., et al., (2011) proposed a new method for signature verification using local Radon Transform. Their proposed method uses Radon Transform locally as feature extractor and Support Vector Machine (SVM) as classifier. The main idea of our method is using Radon Transform locally for line segments detection and feature extraction, against using it globally.

Jena, D., et al., (2008) proposed a novel offline signature verification scheme has been proposed. The scheme is based on selecting 60 feature points from the geometric centre of the signature and compares them with the already trained feature points. The classification of the feature points utilizes statistical parameters like mean and

variance. They suggested that the scheme discriminates between two types of originals and forged signatures. The method takes care of skill, simple and random forgeries.

Mishra, P.K. and Sahoo, M.R., (2009) suggested scheme aims to make the verification of signatures size and angle invariant. The invariance can be achieved by scaling and rotational manipulations on the target image. The shape of a person's signature remains similar in all translational, scaled and rotational alignments of the sign. That is the number of crests, toughs and curves remains the same irrespective of the size and orientation of the image.

Chaurasia, P., (2009) proposed a method and system for improving the accuracy of offline signature verification techniques by analyzing the high pressure regions of an image of the signature. The method and system may analyze global and local features in the high pressure regions of the image for increased verification accuracy. An image is processed to determine the high pressure regions of the image, global features are extracted from the high pressure regions of the image and pattern recognition techniques are applied to the global features to obtain a global static verification of the authenticity of the signature and a global subjective verification of the authenticity of the signature.

IV. PROPOSED MODEL

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

- Signature Acquisition
- Signature Preprocessing
- Feature Extraction
- Signature Verification

A. *Signature Acquisition*

Signature made on A4 paper were acquired by scanner having 300dpi and stored in Portable Network Graphics (PNG) format. Figure 3 shows one sample for each of the writers from the database on which proposed technique have been tested.

1) Database

Proposed technique has been tested on two databases: 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 10 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. In this way the experiments were conducted on database of 1000 signatures having 500 genuine and 500 skilled forgeries collected over a period of time. There is no language restriction with the proposed technique as it is applicable to signatures in any language. The database used here contains signatures in Hindi(writer 47 in Figure 3) and English languages. Figure 4(a) and 4(b) shows 5 genuine and 5 forgery samples of a writer (writer 19 in Figure 3) respectively. Database B contains two sets, Set 1 and Set 2, and is publicly available on http://www.vision.caltech.edu/ mariomu/research/data [].

	A	$B(Set1)$	$B(Set2)$
No. of writers	50	56	50
No. of genuine signatures per writer	10	25	30
No. of forgeries per writer	10	10	10

Table 1: Description of Database 1 and Database 2

B. *Signature Pre-Processing*

To verify a signature correctly, pre-processing of acquired signature is required. The acquired signature image as shown in Figure 5(a) may sometimes contain noise (extra pen dots other than signature). It is necessary to remove these extra pixels from acquired image to correctly verify the signature. This can be done by using filters. Preprocessing includes some more operations like resizing, binarization, thinning and rotation normalization.

1) Resizing

First step in pre-processing phase is to resize the acquired signature to a standard size (100x200) using resize algorithm as shown in Figure 5(b).

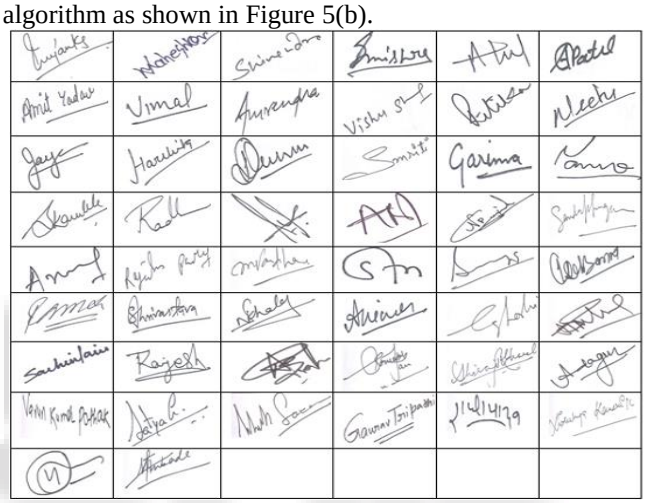


Fig. 3: A sample signature of each writer from Database A

2) Binarization

Binarization means black and white version of the resized (RGB) signature as shown in
Figure 5(c).

3) Thinning

Thinning is required so that a different range of thickness of pen tip does not affect the results. Pen used for database signatures can be of any type. 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 as shown in Figure 5(d).

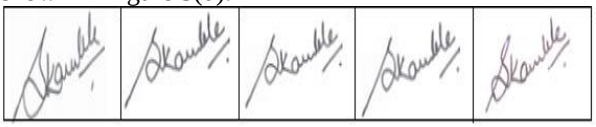


Fig. 4(a): Five genuine signature of a person

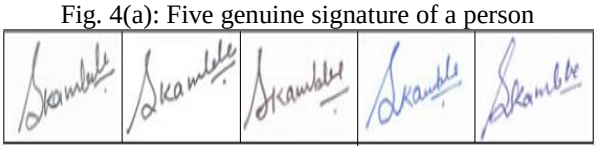


Fig. 4(b): Five skilled forgeries of the same person

Fig. 4: Samples from Database A on which experiments have been performed

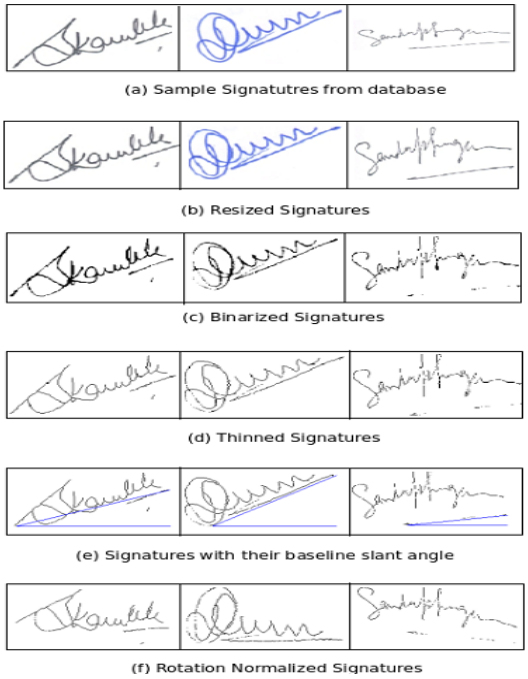


Fig. 5: Pre-Processing Phase

C. *Feature Extraction*

1) Feature Extraction for Proposed Approach:

In proposed approach there are three essential features of tree are used to decide the authenticity of signature. Features are listed below.

- Pixel counting of Tree
- Angle between the slop of local and global center of gravity
- Eccentricity and center of a tree

After calculating these three features we use majority rule. If According to two or more features signature is genuine the output will be yes else no.

2) Pixel counting of Tree

a) Step 1: Divide a matrix of test signature in to grid

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 Figure 6. 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.

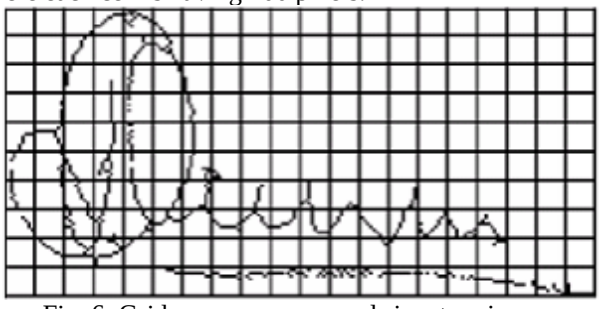


Fig. 6: Grid over pre-processed signature image

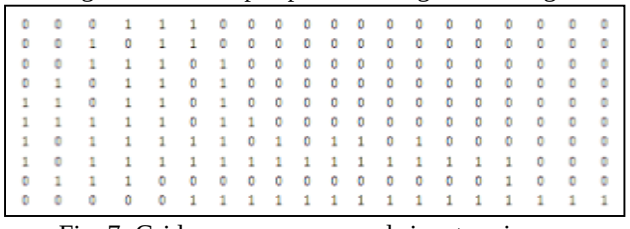


Fig. 7: Grid over pre-processed signature image

b) Step 2: Calculate the center of gravity of each local cell of grid.

1) 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 in cell.

$$\text{CGxlocal} = \frac{\sum_{i=1}^{n} x_i}{n}$$

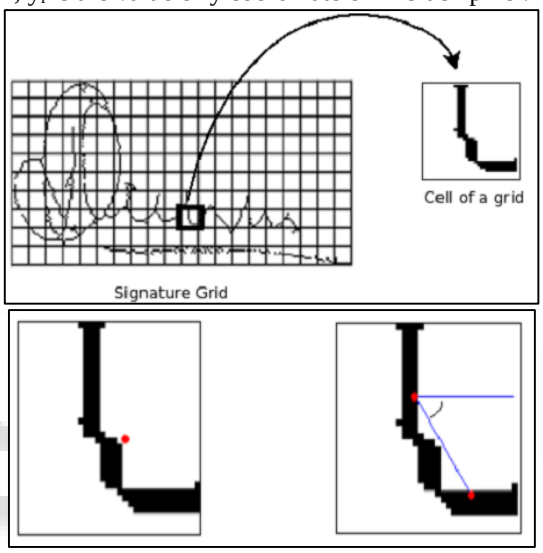
Where n=no. of black pixels in the signature image of cell, x_i is the value of x coordinate of i^{th} black pixel.

2) 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 in cell. Figure 8(a) shows the point which indicates the center of gravity (CGx, CGy).

$$\text{CGylocal} = \frac{\sum_{i=1}^{n} y_i}{n}$$

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



(a) Point indicating center of gravity (b) Angle indicating CG slope

c) Step 3: Connect all pixels on coordinate center of gravity (CGx, CGy) of each cell. In zig-zag fashion to create a tree on signature.

d) Step 4: Count the pixels of created tree. Let the number of pixels be Ntest.

e) Step 5: Same procedure is repeated with genuine signature and let number of pixels on tree be Ngen.

f) Step 6: Assume a threshold th according to secrecy of application.

$$\text{Signature} = \begin{cases} \text{Genuine} & \text{If } N_{test} = N_{gen} \mp th \\ \text{Fake} & \text{Otherwise} \end{cases}$$

V. Experimental Result and Analysis

Experiments have been performed on various datasets and results show the efficiency of proposed approach. FAR and FRR are the two parameters 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:

FAR = (No of forgeries accepted/No of forgeries tested) x 100

B. FRR (False Rejection Rate):

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

FRR = (No of genuines rejected/No of genuines tested) x 100

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.

C. ROC Curve

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.

D. Results for Database A

From Table 2 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 Figure 12. ROC curve for this database is shown in Figure 13.

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

Table 2: Signature Verification Results of the Proposed System

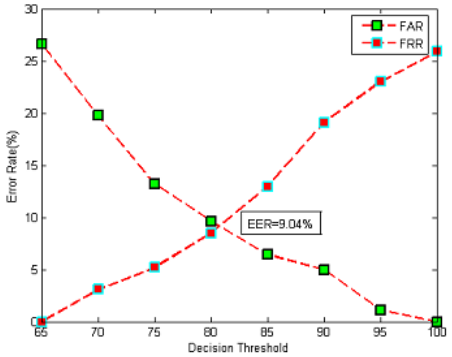


Fig. 10: FAR Vs FRR graph for Database A

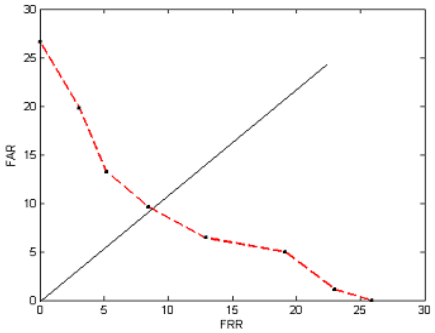


Fig. 11: ROC Curve for Database A

E. Results for Database B

From Table 3 and 4, 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%. Figure 14 and 15 shows the FAR vs FRR graph for Set 1 and Set 2 respectively.

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

Table 3: Signature Verification Result

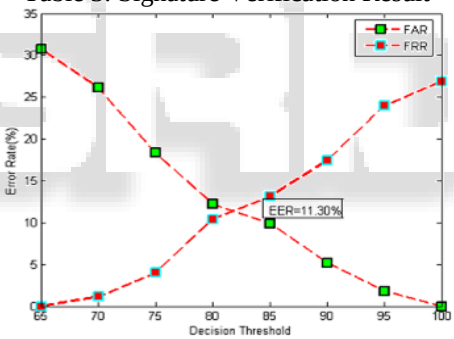


Fig. 12: FAR Vs FRR graph for Database B (set 1)

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

Table 4: Signature Verification Results for Set 2

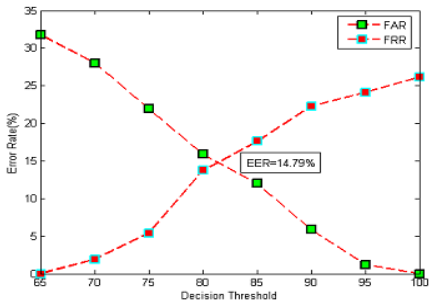


Fig. 13: FAR Vs FRR graph for Database B (set 2)

VI. 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. 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.

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". Priyanka Chaurasia, 2009,"Offline Signature Verification using High Pressure Regions," Patent No. US 7, 599,528 B1.
[8] Dakshina Ranjan Kisku, Phalguni Gupta, Jamuna Kanta Sing, IJSIA 2010, "OfflineSignature Identification by Fusion of Multiple Classifiers using Statistical Learning Theory," Computer Vision and Pattern Recognition.
[9] 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

