SIGNATURE VERIFICATION

Dr. H.B.Kekre, Dr. Dhirendra Mishra, Ms. Shilpa Buddhadev, Ms. Bhagyashree Mall,
Mr. Gaurav Jangid, Ms. Nikita Lakhotia

Computer engineering Department, MPSTME, NMIMS University
Vile Parle (W),Mumbai,India

Abstract—In this paper we present an off-line signature verification and recognition system based on a combination of features extracted such as blob features, average of radon transform, fusion of grid and global features using average and clustering technique. The system is trained using a database of signatures. For each person, a feature vector is obtained from a set of his/her genuine samples using the features that were extracted. The signature is then used as a template which is used to verify a claimed signature. We use the Euclidean distance in the feature space to obtain measure of similarity between template signature and claimed signature. We have discussed four methods and combined the results as per observations based on far, frr and gar.

Keywords— Thinning, Region of interest(ROI), skeletonization, clustering techniques, Gaussian Noise.

I. INTRODUCTION

Signature has always been one of the methods by which the recognition and verification of human beings can be done. Signature recognition and verification is a technique which helps in identification of an individual, through the use of signature. Signature recognition is a behavioural biometric.

It can be operated in two different ways:

Static mode: In this mode, the signature is written on paper. It is then digitize, through an optical scanner or a camera. The signature is analysed by its shape through the biometric system. This mode is also known as "offline" signature verification mode.

Dynamic mode: In this mode, the signature is written in a digitizing tablet, which needs a signature in a real time. Dynamic recognition is also known as "online" signature verification mode. Some areas where online signature verification is required is protection of small personal devices (e.g. laptop), authorization of computer users for accessing sensitive data or programs and authentication of individuals for accessing physical devices.

In this paper, four different techniques are used for the offline verification of signature. Signature is read and is converted from colour to grayscale. Noises are removed from the signature using appropriate filtering techniques and therefore signature free from noises is extracted. Applying pre-processing techniques on the image brings the signature to a basic format so that we can compare them properly. We apply pre-processing technique on all the images in the database and store them. Then we apply the four techniques as discussed in later sections of paper. The results are observed on the basis of far, frr, and gar which provides a way as how much the template signature is matching the claimed signature.

II. RELATED WORK

Several steps need to be performed in order to verify or identify a signature. All signatures from the database are first pre-processed by converting them to a portable greyscale format; their boundaries are extracted to facilitate the extraction of features[5-8]. Experiments have been performed with the signature database. The signature database used is shown in Figure.1. The boundary of each signature must be extracted prior to the feature extraction process. The features extracted must be appropriate for both the application and the classifier used.

The approach that [1] has been used to extract features for the signature verification problem employs BLOB features like centroid, area, perimeter, mean intensity and diameter. The signature is transformed to binary format and the BLOB properties act as the features of the signature. The experiments have shown promising results in the task of discriminating random and simple forgeries. The test signature is compared with all other signatures in database using Euclidean distance using the formula (1) :

$$d^2(p, q) = (p_1 - q_1)^2 + (p_2 - q_2)^2 + ... + (p_i - q_i)^2 + ... + (p_n - q_n)^2 \quad (1)$$

The next approach is [2] based on Signature Verification Using average of radon transform. Radon transform at various angles such as 30, 60, 90, 180, 270 is applied. The column wise average act as feature vector. The experiments have shown promising results in the task of discriminating random and simple forgeries.

The next approach for [3] Off-line Signature Verification is based on Fusion of Grid and Global Features Using Average. The global and grid features are fused to generate set of features for the verification of signature. The test signature is compared with data base signatures based on the set of features and match/non

match of signatures is decided with the help of the average of the rows and columns. The performance analysis is conducted on random, unskilled and skilled signature forgeries along with genuine signatures [3].

The next approach [4] is based on Features Extraction And Verification Of Signature Image Using Clustering Technique. It presents a set of geometric signature features for offline automatic signature verification based on the description of the signature envelope like height-width ratio, distance ratio and occupancy ratio. ; It is a novel robust technique for the off-line signature verification problem in practical real conditions is presented [4].

Signature Verification is a system which requires to maintain a database of the signatures. Signature database is required for comparing the query image signature with the signature from the database image and the finding the result. We have downloaded a few signature database from the net[6]. We have downloaded around four different databases which consists of around 30-35 signatures and combined them to form a single collection of 130-140 signatures. We have also added our signatures to the database. A view of signature database is shown in Figure 1.

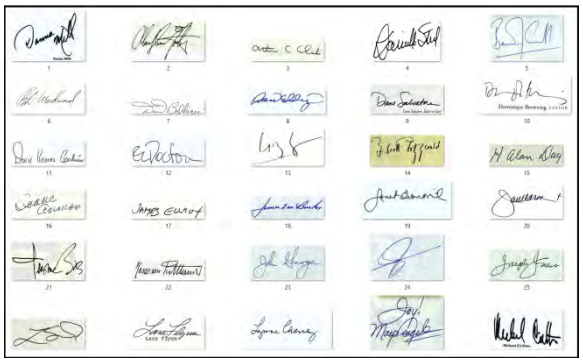

Figure.1. Signature Database

III. PROPOSED METHODOLOGY

The process of Signature verification require many steps for completely verifying the signature. These steps are implemented in a sequential manner.

1. Preprocessing
2. Feature extraction
3. Feature comparison
4. Performance evaluation
5. Results and Discussion

1. <u>Preprocessing :</u> Preprocessing is carried out to extract signature feature to obtain high resolution for smaller normalization box. Thus a transformed image of enhanced quality is obtained. It involves-

1.1. Resizing: The signature is resized to give a standard size**.**

1.2. Conversion of Color image to Grayscale image : It converts the color image of signature to a grayscale image.

1.3. Noise Removal: This noise can be present in the image in the form of salt and pepper noise. A noise free image is required. Thus, median filter is used to remove this noise.

1.4. Smoothing: Additive white Gaussian Noise is removed by smoothing and it preserves high frequency components.

1.5. Thinning: The signature is reduced to a skeleton of unitary thickness and computational time using Zhang-Suen algorithm.

1.6. Canny Edge detector : The edges of the signature image are detected.

2. <u>Feature Extraction :</u>

2.1.Signature Verification Using average of radon transform.[4]

Radon transform at various angles such as 30, 60, 90, 180, 270 is applied. The negative of Radon Transformed images is taken followed by the computation of the column wise average which act as feature vector. The number of columns in the radon transform will be equal to the no of elements in feature vector. Thus we get five feature vector of different sizes as shown in Figure.2. Same procedure is applied for all the signatures in the database.

2.2.Signature Recognition Method Based On The BLOB properties.[3]

In this method we get all blob properties like centroid, Area, Perimeter, mean intensity and diameter. These blob properties are our feature vectors. We compute the same properties for all our other signature images of our database as shown in Figure.3.

2.3.Signature Verification Using Cluster Based Global Features.[1]

In this methods, we initially count the number of pixels having value 0 in a particular row and the do this for all the rows in the image having the signature and then take the average value. Similarly we do the same process for the columns and then take the average. The average of the rows and columns will be the feature vector of comparison of the two images i.e. the image from the database and the query image as shown in Figure.4.

2.4.Features Extraction And Verification Of Signature Image Using Clustering Technique.[2]

In this method the region of interest is found. The region of interest is the area which comprises of only the signature part i.e. from extreme left of the signature to the extreme right and from the highest point of the signature to the lowest point of the signature. This ROI (region of interest) will then be used to generate the feature vector of the signature. Height-width ratio of the signature needs to be calculated. Also the occupancy ratio is calculated later which provides us information about signature density followed by distance ratio calculated at boundary. Also the length and ratio of the adjacency columns is computed as shown in Figure.5. The size of feature vector is 4.

3.Feature Comparison :

Euclidean distance is calculated to verify the signature. If Euclidean distance is equal to zero match is found and signature is verified else it is rejected.

4.Performance Evaluation :

We have implemented the above method and the results that are obtained have been shown below in Table 1. The following are the performance evaluation formulas.

$$FAR = \frac{\text{number of false signatures accepted}}{\text{total number of false attempts}} \quad (2)$$

$$FRR = \frac{\text{number of genuine signatures rejected}}{\text{total number of genuine attempts}} \quad (3)$$

$$GAR = 1 - FRR \quad (4)$$

We see that for method 1, method 3 and method 4 the values obtained of far, frr and grr are the same i.e. 40, 0 and 100 respectively and for methods 2 the values of far, frr and grr is 0, 0 and 100.

The values obtained for FAR is obtained when a sample genuine database is tested upon by false signatures. The lower the value of FAR the better it is, ideally it should be 0. The lower value in FAR means that a particular method has a very low acceptance of false signature and over here method 2 has a value of 0. Thus this means that the method 2 is better in terms of not accepting false image. We see that few of the false signatures are being accepted as genuine (approx 40 %) in methods 1, 2 and 4.

The values obtained for FRR is obtained when a sample false database is tested upon by genuine signatures. The lower the value of FRR the better it is, ideally it should be 0. We see that all the genuine signatures are being rejected when tested upon false database.

The higher the value of GAR the better it is and over here we see that all the methods have a GAR value of 100.

5.Results and Discussion :

Method 1 : Signature Verification Using average of radon transform.
Method 2 : Signature Recognition Method Based On The BLOB properties
Method 3 : Signature Verification Using Cluster Based Global Features.
Method 4 : Features Extraction And Verification Of Signature Image Using Clustering Technique.

	FAR	FRR	GAR
Method 1	40	0	100
Method 2	0	0	100
Method 3	40	0	100
Method 4	40	0	100
Combined	0	0	100

Table.1. Results obtained from false as well as genuine image database (all values in the above table are in %).

Here the meaning of: FAR is False Acceptance Ratio

FRR is False Rejection Ratio

GAR is Genuine Rejection Ratio

We see that for method 1, method 3 and method 4 the FAR value comes out to be 40 where as for method 2 FAR comes out to be 0. The lesser the value of FAR the better the method it is. Thus method 2 is better in terms of FAR.

For FRR, the lower the value of FRR the better it is. When you go on to look for the value of FRR all the methods have the same FRR value i.e. 0.

Conclusion

This paper is focused on signature verification methods. Signatures are verified based on parameters extracted from the signature using various image processing techniques. This paper will be completed when the utility of signature verification is shown i.e. it helps in detecting the exact person and helps in detecting the exact person by comparing the results based on far, frr and gar for all the four methods being implemented in this paper. The methods were tested using genuine and forgery signatures produced by five subjects. Two types of tests were conducted:(1) genuine test, where genuine signatures were verified, (2) random forgery test, where for every subject, all genuine signatures of all other subjects are considered random forgeries of signature

of the subject under consideration. An error rate of % for random forgeries is achieved. The results as per can be seen from the observations of gar shows that %of verifications of claimed signature is made.

REFERENCES

[1] V A Bharadi , H B Kekre, 'Off-Line Signature Recognition Systems', International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 2, 2010.

[2] Samit Biswas1, Tai-hoon Kim2.*, Debnath Bhattacharyya, 'Features Extraction and Verification of Signature Image using Clustering Technique', International Journal of Smart Home Vol.4, No.3, 2010.

[3] Buddhika Jayasekara, Awantha Jayasiri, Lanka Udawatta, 'An Evolving Signature Recognition System', First International Conference on Industrial and Information Systems, ICIIS, 2006.

[4] Ramachandra A C1, Ravi J2, K B Raja3, Venugopal K R3 and L M Patnaik4 , 'Signature Verification using Graph Matching and Cross-Validation Principle', International Journal of Recent Trends in Engineering, Vol 1, No. 1, 2009.

[5] H.B.Kekre and Dhirendra Mishra, "Content based image retrieval using Full Haar wavelet sectorization", International Journal of Image Processing (IJIP-334), Malaysia, Vol.5, No.1, March 2011

[6] H.B.Kekre and Dhirendra Mishra, "Sectorization of Full Kekre's Wavelet Transform for Feature extraction of Color Images", International Journal of advanced computer science and Applications (IJACSA),USA, Vol.2,No.2, Feb 2011,pp.69-74

[7] H.B.Kekre and Dhirendra Mishra, "Feature extraction of color images using discrete sine transform", International Journal of Computer Application (IJCA),USA, Special Issue for ICWET 2011 Proceedings ISBN is : 978-93-80747-67-2

[8] H.B.Kekre , Dhirendra Mishra and Anirudh Kariwala, "A survey of CBIR Techniques and semantics", International journal of Engineering science and Technology (IJEST), Vol.3, No.5, May, 2011

Preprocessing and Output :

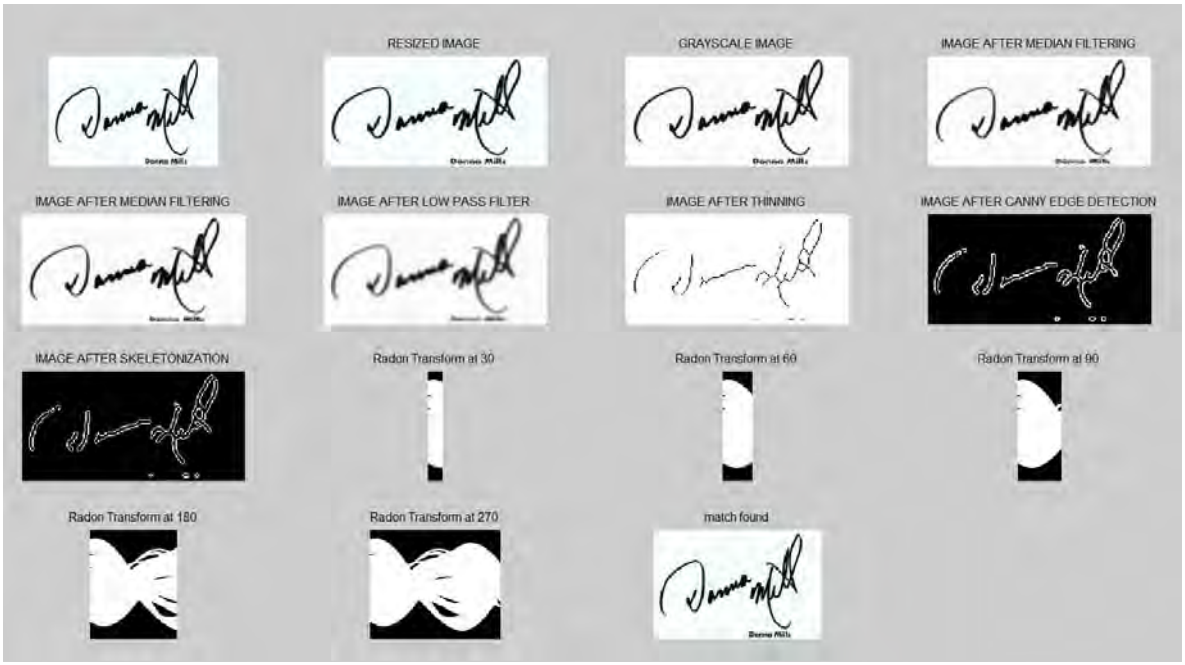

Figure.2. Signature Verification Using average of radon transform.

On applying the algorithm the result was 'match successful' as shown in Figure 2. In above Fig 2,

- The first and second image is the input image.
- Third image is the grayscale image.
- The fourth and fifth image is result after applying median filtering.
- The sixth image is result obtained by low pass filter.
- The seventh image is when thinning is applied.
- The eighth image is on applying canny edge detection.
- The ninth image shows skeletonization .
- The next 5 images shows radon transform at 30,60,90,180,270.
- The last image shows match found as the signature is found in database.

Thus we can observe that the result obtained on applying this algorithm is correct and thus has been implemented correctly.

Preprocessing and Output :

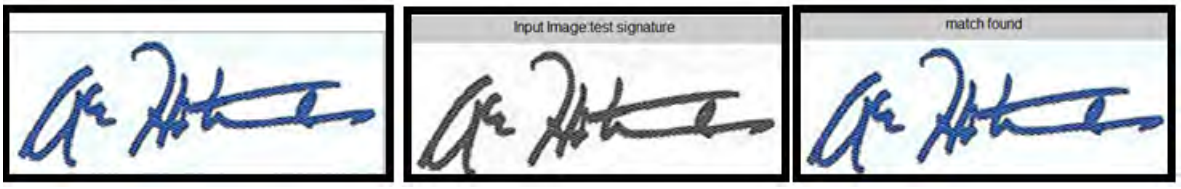

Figure.3.Signature Recognition Method Based On The BLOB properties

In above Figure 3,

- The first image shows the test image.
- Second image shows the grayscale image.
- The next images shows the "match found" as signature is present in database.

Preprocessing and Output :

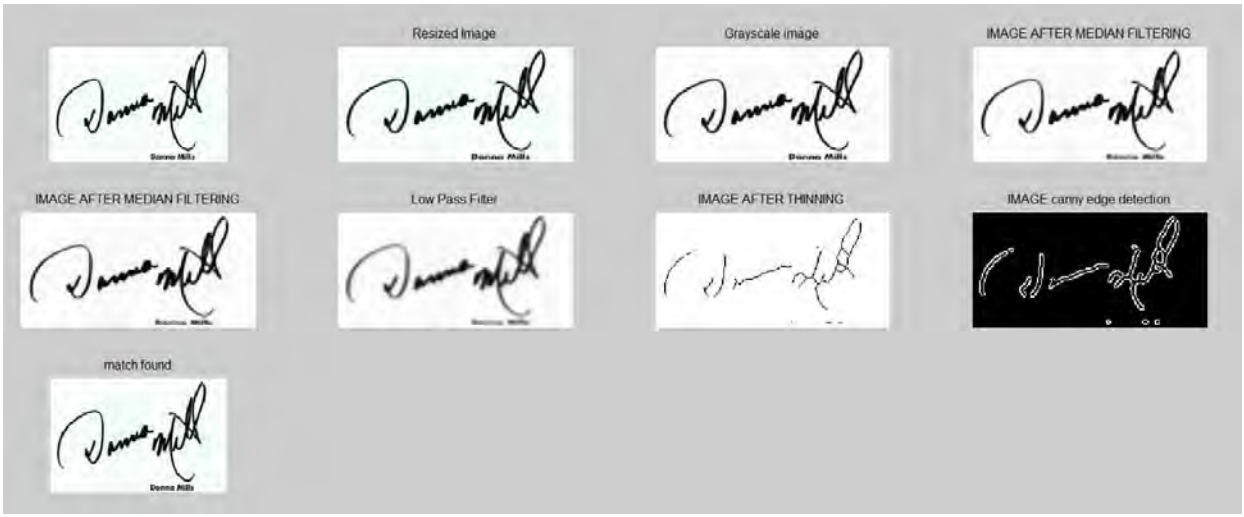

Figure.4.Signature Verification Using Cluster Based Global Features.

On applying this algorithm the result was 'match successful' as shown below in Fig 5.5.

- The first image is the original image.
- It is then resized.
- The next signature is the test signature from the user.
- The 4th image is the median filtered image of the original image
- The 5th image is the median filtered image of the test signature.
- The next image is the image after thinning followed by canny edge detection.
- The last image is the resultant image.

Preprocessing and Output :

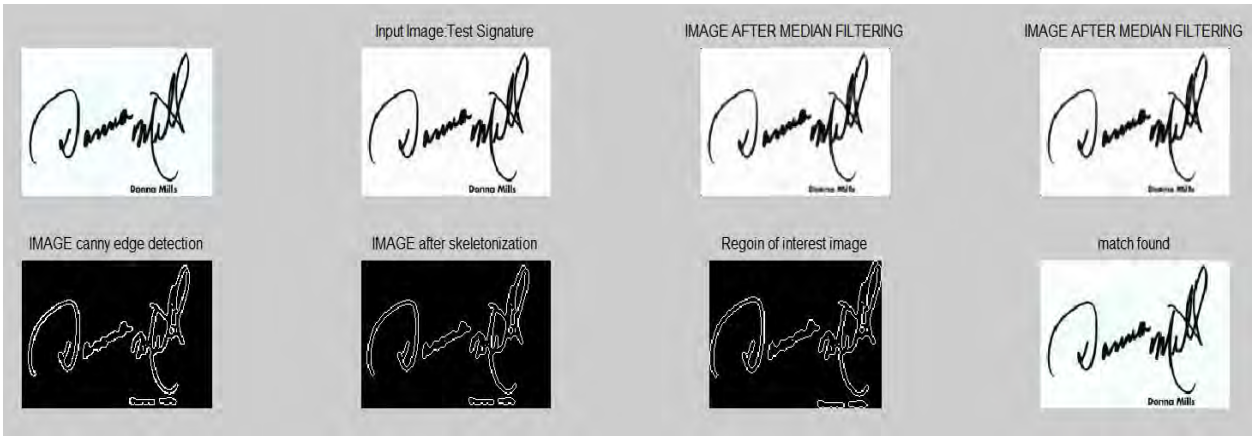

Figure.5. Features Extraction And Verification Of Signature Image Using Clustering Technique.

In above Figure 5

- The first is the colour input image.
- Second image is the input greyscale image.
- The third and fourth is result after applying median filtering,
- The fifth is the image obtained after edge detection.
- The sixth image is result obtained by skeletonization. T
- The seventh image shows the region of interest of our signature.
- The last image shows match found as the signature is found in database.