Offline Signature Verification using Grid based and Centroid based Approach

Sayantan Roy
Department of Computer Science Engineering
ISM Dhanbad
Jharkhand

Sushila Maheshkar
Department of Computer Science Engineering
ISM Dhanbad
Jharkhand

ABSTRACT
Now a day's Signature verification is one of the most important features for checking the authenticity of a person. There are many security checking parameters like pin code, password, finger print checking but signature recognition is the most popular because it is quite accurate and cost efficient too. On the other hand one doesn't have to remember the authentication key like pin code or password. The signature of a genuine signer stays almost constant. But there may be little difference between well practiced forgeries and the genuine signer. It is required to distinguish these differences. This paper presents grid based, contour based and area based approach for signature verification. Intersecting points and centroids of two equal half of the signature is being calculated and then those centroids are connected with a straight line and the angles of these intersecting points with respect to the centroids connecting lines are calculated.

General Terms
Signature Verification, Grid based approach, Centroid based approach and contour based approach.

Keywords
Signature Verification, Binarization, Normalization, Thinning, Centroid

1. INTRODUCTION
A signature verification system can be divided into two classes Online and Off-line .On-line approach uses an electronic tablet and a stylus connected to a computer to extract information about a signature and takes dynamic information like pressure, velocity, speed of writing etc. for verification purpose. Off-line signature verification involves less electronic control and uses signature images captured by scanner or camera. In off-line signature verification system features are extracted from scanned signature image. The features used for offline signature verification are much simpler. Here only the pixels of the image need to be evaluated. But as in offline signature verification dynamic features like order of stroke, velocity, pressure etc. are not available so it is difficult to achieve that level of accuracy which is provided by the online signature verification. Vigorous research has been pursued in handwriting analysis and pattern matching for a number of years. In this paper some recently used techniques of Offline Handwritten Signature Verification are used and some new feature extraction techniques are used also.

2. TYPES OF FORGERIES
There are lots of forgeries, they can be classified into 3 categories.

A. Random Forgeries
The forger has no information about the signature style and the name of the person.

B. Simple Forgeries
The forger has seen the technique how the signature was done.

C. Skilled Forgeries
The forger knew the signature and practiced well

3. TYPES OF VERIFICATION
There are 2 basic types of signature verification. One is Online Signature Verification and other is Offline Signature Verification.

A. Online Signature Verification
In online Signature Verification, signatures were recorded by digital pen or digitizer. Here we record dynamic features like velocity, pressure, position, inclination of pen etc.[1]

B. Offline Signature Verification
This approach is based on static characteristics of the signature. Signature verification becomes a typical pattern recognition task knowing that variations in signature pattern are inevitable; here main task is to minimize the range of genuine variation. Here images of the signatures written on a paper are obtained using a scanner or a camera. Then feature extraction algorithm was used to find the feature points of the signature.

In this paper offline signature verification is used.

4. RELATED WORK
A lot of research has been done in the field of off-line signature verification. Sabourin used granulometric size distributions for the definition of local shape descriptors then he used a nearest neighbor and threshold-based classifier to detect random forgeries [2]. A total error rate of 0.02% and 1.0% was reported for the respective classifiers. A database of 800 genuine signatures from 20 writers is used. The main approach to this work is to show the feasibility of such implementation, introducing the new scheme for the tasks. Abbas [3] used a back propagation neural network prototype for the offline signature recognition. He used feed forward neural networks and three different training algorithms Vanilla, Enhanced and Batch were used. In his work he reported FAR (False Acceptance Rate) between the ranges of 10-40 % for casual forgeries. A neuron-fuzzy system was proposed by Hanmandlu [4], they compared the angle made by the signature pixels are computed with respect to reference points and the angle distribution, then to train the neural network back propagation algorithm was used. The system reported FRR (False Rejection Rate) in the range of 5-16% with varying threshold.

5. OBJECTIVE
The aim of offline signature verification is to decide that a signature is done by an original signer or a forge signer. First some genuine signatures of a single signer is compared and

the common feature points are extracted and stored in the database corresponding to that genuine signature. After that when someone wants to copy that signature then that signature is compared with those stored feature points of the original signature. Signature is a special case of handwriting which includes special characters and flourishes. Many signs can be unreadable as they are a kind of artistic handwriting objects. However, a signature can be handled as an image, and hence, it can be recognized using computer vision. Signature recognition and verification involves two separate but strongly related tasks:

I) Identification of the owner of signature
II) Whether the signature is original or forged.

6. STEPS OF IMPLEMENTATION

There are 4 major steps in achieving signature verification and recognition, and each of these steps consists of many methods to improved results. These steps are follows:

- Data Acquisition/Signature Database
- Image Pre-Processing
- Feature Extraction
- Classification/Verification

6.1. Data acquisition

In offline signature verification individual person's signatures are taken on A4 size paper and then scanned. The database contains data from individuals, including genuine signatures and forgeries. The signatures are collected using either black or blue ink, on a white A4 sheet of a paper within a fixed size box, with 36 signatures per page. In this paper 36 signatures of a genuine signer are taken at different times and 36 signatures from each of the 17 different forgeries are also taken at different times. So here total 36 genuine signatures and 612 forge signatures are analyzed.

6.2. Image pre-processing

Preprocessing is used to improve the quality of signature image. Preprocessor processes the raw signature samples to make them usable by the feature extracting unit. The scanned signature image may contain spurious noise and has to be removed to avoid errors in the further processing steps. The following were the process that was carried out on the signature.

There are 4 steps of image preprocessing:

1. Image Binarization.
2. Finding the bounding box of the image and cropping the image.
3. Thinning.
4. Normalization.

6.2.1. Image Binarization

There is no importance of color in which the signer is signing that's why we convert the image from color image to gray scale image. Then for future calculation we have converted that image to binary image. So to do this conversion we have used OTSU's algorithm. The noise in the boundary region of the signature is also filtered by this OTSU's threshold algorithm.

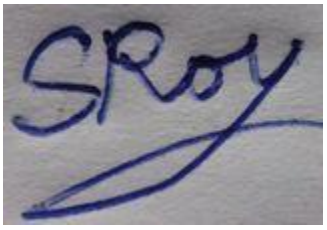

Fig 1: Original Signature

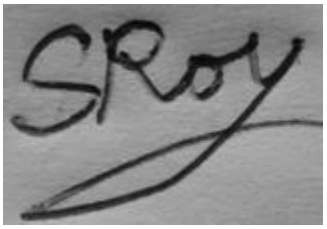

Fig 2: Gray Scale Image

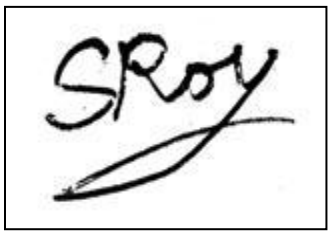

Fig 3: Binarized Signature

6.2.2. Finding the bounding box of the image and cropping the image

After using the OTSU's Threshold algorithm for binarization the image was traversed from all 4 directions means top to bottom, bottom to top, left to right and right to left until a signature part means a pixel with value 0 is fetched. When 0 is fetched then that point is recoded. In this way the bounding box is calculated. Then the image was cropped to separate the unwanted area. Then the ratio between the height and length was calculated.

6.2.3. Thinning

Thinning is used to eliminate the thickness differences of pen by making the image one pixel thick throughout the signature. It is necessary because signer may use different pen at different time and that's why thickness of the signature may vary [5].

6.2.4. Normalization

In Normalization, those points which are parts of the signature are normalized using simple formulas. X_i^{new} and Y_i^{new} are new value corresponding to X_i and Y_i. [6]

$$X_i^{new} = \frac{X_i - X_{min}}{X_{max} - X_{min}} * length \qquad (1)$$

$$Y_i^{new} = \frac{Y_i - Y_{min}}{Y_{max} - Y_{min}} * height \qquad (2)$$

6.3. Feature extraction

Features are of two types:

1. Function features (like velocity, pressure, position).
2. Parameter features
   - (i). Global Parameter
   - (ii). Local Parameter
     - i. Component oriented (like Contour base, geometry based)
     - ii. Pixel oriented (like Grid based, Intensity based)

In this paper the Local Parameter Feature Extraction is used.

6.3.1. Aspect Ratio

Signature may vary from size to size but the ratio between height and length stay always constant [7].

6.3.2. Closed Area

While traversing the signature from left to right until a 0 means black pixel is fetched means a signature part, the value was changed from 1 to 0, doing the same operation from all 4 directions we can calculate the closed area by calculating the area of the remaining white part, shown in Fig 4.[8]

6.3.3. Grid Based Approach

Algorithm for breaking the image in blocks:

Step1: Fetch the preprocessed signature image (Thinned image) of size 140x160(pixels).

Step2: Then form a grid of size m x n, where m<<140 and n<<160. In this paper m is 10 and n is 10. So the signature image is divided into 224 square cells where each cell consists of 100 pixels.

Step3: Then find out the cells of a row of a grid that consist of the content of signature. The content of signature is calculated in terms of black pixels. Therefore consider the cells which consist of 3 or more black pixels. Same process is repeated for all the rows a grid. Thus all those cell positions which are part of the signature image were recorded.

Step4: 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, this produce the fig 6 matrix.

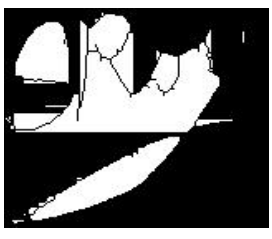

Fig 4: Closed Image

Fig 5: Thinned Image

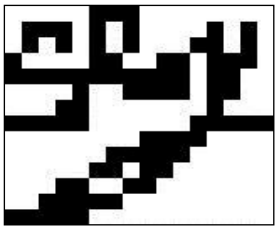

Fig 6: Sectored Image

Then, calculate the number of black pixels in cells of a row containing signature content. Repeat the process for all rows. Then the values of m rows are put in an array. Then same process is applied to columns. We get another array having n elements corresponding to each column.

Step5: Consider a matrix m x n corresponding to a m x n grid.

Step6: An array of size m in which first element is the number of black pixels in first row of a grid, second element is the number of black pixels in second row and so on.

Step7: An array of size n in which the first element is the number of black pixels in first column of the grid, second element is the number of black pixels in second column and so on.

Algorithms for Verification:

Calculate Column Matching Score (CMS).

Step1: Consider M0 and M1 as the matrices of reference image and test image respectively. Compare the columns of the matrix M1 with M0. Each column is having m elements. If at least 7, elements are same then that column is said to be matched and increase the column count C0 by one.

Step2: Consider A0 and A1 be the arrays of reference image and test image respectively containing number of black pixels in each column. Compare the corresponding elements of array A1 with A0.If these are matched then increase the counter C1 by one.

Step3: If C0 and C1 are equal then CMS is 100%.

Step4: Similarly calculate Row Matching Score (RMS). To reduce the complexity we will calculate the RMS only when CMS >60%.

6.3.4. Intersecting points

While traversing the image when a black pixel is fetched whose atleast three neighboring pixels are also black then that pixel is considered as an intersection point of the signature. Then the angles produced by those intersection points with respect to the basement of the signature was calculated and noted as a feature. Basement of the signature was calculated by dividing the signature in 2 equal parts and then finding the centroid of each part and then connecting those 2 centroids the basement line was produced, Fig 9.[9][10]

6.3.5. Finding the Contour

The contour of the signature was calculated by traversing through the image like an array and when the pixel value changes from 0 to 1 or 1 to 0 then those pixels are noted in a new image of the same size of the signature. In this way the level 1 contour was calculated then from that after overlapping level 0(means the actual signature) and level 1 then applying the same algorithm on the overlapped image

level 2 contour was calculated. The testing signature should be fit into totally inside level 0 to maximum level 3 contour if it is genuine.

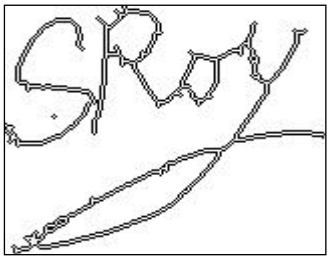

Fig 7: Level 1 Contour Image

In which points the contour curve of the signature bends above the threshold level those points are considered as a feature points of a signature. Those feature points of a genuine signature can be compared to testing signature to detect a forge signature [11][12].

6.3.6. Ratio of the distance between centroids

The Signature was broken vertically into 3 equal parts then centroid of each part is calculated. The distance between the 1st parts centroid and middle parts centroid is calculated through x axis then the middle parts centroid and 3rd parts centroid is calculated for the same. Atlast the ratio between them is calculated. Similarly distances between those centroids are also calculated through y axis. For a genuine signer these ratios stay almost constant.[13]

Fig 8: Three centroids of signature

In fig 8 signature is broken into three parts those are shown by two vertical line and white points are the centroids of these parts.

Fig 9: Basement line of signature

Signature is divided into two parts C1 and C2 are two centroids of each part as shown in Fig. 9, by connecting these two points the basement line of the image was produced.

6.3.7. Ratio of the area closed by those centroids and the bounding box

After finding those centroids they were connected to each other. Then the area enclosed by those centroids connecting lines is calculated, in fig 10 it is shown by yellow triangle. Then the ratio between this area and the bounding box area is calculated. The size of the signature may vary but this ratio stay almost constant. [14]

Fig 10: Centroid connecting lines

Flow Chart: 1

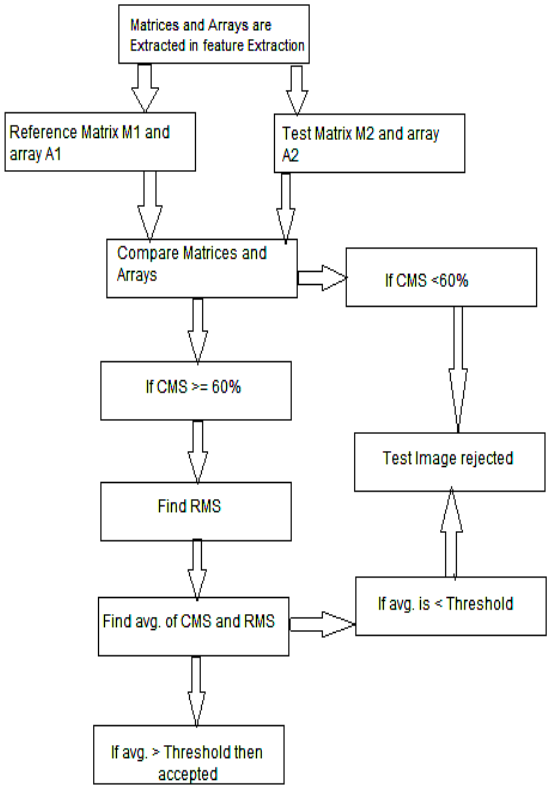

Fig 10: Grid based approach

Flow Chart: 2

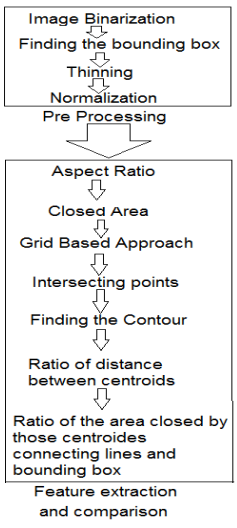

Fig 11: Steps of signature verification

7. RESULT AND DISCUSSION

In this paper total 36 genuine signatures and 612 forge signatures are analyzed. Feature points are extracted from comparing those 36 genuine signatures. Experiment results shows that the False Acceptance Rate (FAR) was reduced to 11-20% on the other hand False Rejection Rate (FRR) was reduced to 7-19%. This FAR and FRR varies between a boundary because we have to maintain the tradeoff of FAR and FRR, because if criteria for acceptance kept high then FAR will decrease but there will be some genuine signature which will be detected as forge so then FRR will increase. Similarly if threshold for acceptance kept low then FRR will reduce but FAR will increase. So after maintaining the tradeoff between FAR and FRR what threshold we have used it gives a FAR of 11-20% and FRR of 7-19%.

8. CONCLUSION AND FUTURE WORK

This paper presents a method of handwritten signature verification using grid based approach and pixel oriented approach. The method uses features extracted from preprocessed signature images. A comparison of extracted features is done between the original signature and other relative signatures. Generally the failure to recognize/verify a signature was due to poor image quality and high similarity between 2 signatures. In this paper simple forgery and skilled forgery both are considered, simple forgery case produce a low FAR but skilled forgery case produces 20% FAR. Recognition and verification ability of the system can be increased by using additional features in the input data set and the Hidden Markov Model or Back Propagation can be used to teach the neural network [11] to compare it and teach the learning system. Gradient Feature and the Modified Direction Feature can also be used here [16][17]. This study aims to reduce the cases of forgery in business transaction.

9. ACKNOWLEDGEMENT

I am really grateful to my guide, my teachers and my friends for this paper. It would not be possible to complete my paper without their help and valuable support. They helped me to generate new ideas; they helped me to understand existing works and their drawbacks. I am also thankful to all the faculty member of the department for providing time to time guidance during this period. I want to thank all the members of the Department who helped me towards the completion of my project. Last of all, I thank to all of my family members and my teachers, without their moral supports it would not be possible.

10. REFERENCES

[1] T.S. enturk. E. O¨ zgunduz. and E. Karshgil,(2005)" Handwritten Signature Verification Using Image Invariants and Dynamic Features," Proceedings of the 13th European Signal Processing Conference EUSIPCO 2005,Antalya Turkey, 4th-8th September, 2005.

[2] Sabourin, R.; Genest, G.; Preteux, F. J., (1997): "Off-line Signature verification local granulometric size distributions", IEEE Trans. Pattern Anal. Mach. Intell. 19 (9).

[3] Abbas, R.; (2003): "Back propagation Neural Network Prototype for off line signature verification", thesis Submitted to RMIT.

[4] M. Hanmandlu, M. H. M. Yusof and V. K. Madasu,(2005) "Offline Signature Verification and forgery detection using fuzzy modeling," Pattern Recognition , vol. 38, pp.341-356.

[5] Plamondon, R. and Srihari, S.N., (Jan.2000): "Online and Offline Handwriting Recognition: A Comprehensive Survey", IEEE Tran. on Pattern Analysis and Machine Intelligence, vol.22 no.1, pp.63-84.

[6] Ramachandra A. C ,Jyoti shrinivas Rao(2009) "Robust Offline signature verification based on global features" IEEE International Advance Computing Conference.

[7] Anu Rathi, Divya Rathi, Parmanand Astya(2012) "Offline handwritten Signature Verification by using Pixel based Method", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 1 Issue 7, September-2012.

[8] Raghuwanshi K. , Dubey N. , Nema R. and Sharma R. (2013) "Signature Verification through MATLAB Using Image Processing" International Journal on Emerging Trends in Electronics and Computer Science, VOL. 2, Issue 4,April 2013.

[9] Srihari, S.; Kalera, K. M. and A. 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.

[10] Ibrahim S.I. Abuhaiba(2007), "Offline Signature Verification Using Graph Matching, Turk J ElecEngin, VOL.15, NO.1.

[11] N. Christofides, (1977): Graph theory: an algorithmic approach (New York, Academic Press Inc.).

[12] Prashanth C. R. and K. B. Raja(2012) "Off-line Signature Verification Based on Angular Features", International Journal of Modeling and Optimization, Vol. 2, No. 4, August 2012.

[13] S. Uchida and M. Liwicki(2010) "Analysis of Local Features for Handwritten Character Recognition." In Proc. ICPR 2010, pp. 1945-1948.

[14] K. Frank,(2009) "Analysis of Authentic Signature and Forgeries" In Proc. IWCF,pp 150-164.

[15] Pradeep Kumar, Shekhar Singh, Ashwani Garg,(2013) "Hand Written Signature Recognition & Verification using Neural Network" , International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 3, March 2013.

[16] V. Nguyen, Y. Kawazoe, T. Wakabayashi, M. Blumenstein and U. Pal,(2010)"Performance Analysis of the Gradient Feature and the Modified Direction Feature for Offline Signature Verification" in proc. ICFHR,2010.pp.303-307.

[17] Armand S., Blumstein M., and Muthukkumarasamy V.(2006)Off-line signature verification based on the Modified Direction Feature. 18th International Conference on Pattern Recognition, Vol. 4, pp. 509-512.