Offline Signature Verification for Authentication

Ranjan Jana
RCC Institute of Information Technology
Kolkata, India

Saptashwa Mandal
RCC Institute of Information Technology
Kolkata, India

Kunal Chhaya
RCC Institute of Information Technology
Kolkata, India

ABSTRACT
Biometrics verification has become a recent trend to prevent unauthorized accesses to all kinds of e-data. Signature is strongly accepted in legally and socially as identification and authentication of a person's identity. But, it is very difficult to verify the signature physically. So, it is needed to design a system that verifies the signature of a human automatically. A set of actual signatures is collected from individuals whose signatures have to be authenticated by the system. The topological and texture features are extracted from the actual signature set. The system is trained by using these features. The mean feature values of all the actual signature features are calculated. This mean features acts as the model for verification against a test signature. Euclidian distance between template signature features and claimed signature features serves as a measure of similarity between the two. If this distance is greater than a predefined threshold, then the test signature is detected as fake. The system provides the result to classify actual and forgery signature with accuracy up to 100%.

General Terms
Image Processing, Pattern Recognition

Keywords
Authentication, Biometric identification, Euclidian distance, Feature extraction, Signature verification.

1. INTRODUCTION
Signatures are generally used for authentication of an individual. Aim of the signature verification system is to verify the uniqueness of an individual based on the analysis of the signature. Signature consists of graphical symbols on the surface in relation to a language. Signatures of the same person can vary with time. However, Signature is a unique feature for individual's identification. Now a day's massive number of transactions are authorizing via signature, especially in economic sectors. So, automatic signature authentication needs to be developed on a day to day basis. Several algorithms are used for authentication of signature. Two kind of acquisition of signature are generally used for signature verification i.e. offline and online. Offline signature is obtained by camera which is a two-dimensional image. Offline signature processing is very hard due to the absence of dynamic characteristics like signature strokes, pen velocity, unconventional writing styles, and pen pressure. Online signature is obtained when the signature is produced which records pen pressure, velocity, and acceleration as functions of time. Dynamic characteristics are unique to each person those are adequately stable as well as repetitive.

Signature image acquisition, preprocessing of signature image, features extraction from signature image, and feature matching with actual signature and test signature are four common stages of offline signature verification systems. To improve system's performance, the texture features of signature image like aspect ratio, center of gravity, baseline slant angle, slope of the line joining the center of gravities of two halves of a signature image are calculated. Using above texture features, signature verification is done using Euclidian distance between the claimed signature and the template signature. This paper is structured into the following sections. An overview of previous work is described in Section 2. Section 3 gives the implementation details of offline signature verification for authentication. Algorithm is given in section 4. Experimented results are shown in section 5. Finally, the conclusions are in section 6.

2. PREVIOUS WORKS
Signature verification as authentication has already become a tradition and accepted all over the world and is respected among the others. The most important proof of identity of a person in a transaction taken especially in financial sector on his or her behalf is signature [1], and [2]. Unfortunately, a signature is the result of a difficult process which depends upon psychological state of the signer [3], and [4]. Signatures are widely accepted biometric for legal means for verifying an individual's identity in administrative and economic sectors. A lot of research works are being done on signature verification [5]. For the problems of signature verification, researchers are continuously introducing new ideas, concept, and algorithms in order to increase the accuracy up to 100%. A brief and systematic comparison between offline and online signature verification is compared based on Hidden Markov Models in [6], and [7]. Different methods for signature verification which extracts certain dynamic features derived from velocity and acceleration of pen together with global parameters like total time taken, number of pen ups and downs is proposed in [8], and [9]. Dynamic features are modeled by defining probability density functions of signature features of the same person with respect to time. Another signature verification system is proposed using distance statistics of morphological features which is proposed in [10]. Based on fuzzy modeling using angle features extracted from box approach is proposed to verify signature in [11]. A graph-based approach, which compares the outer contour of the signatures based on the Hungarian method, is anticipated for automatic signature verification in [12]. The graph based approach has two limitations: (1) It works on relatively small window sizes (32*64) and (2) It doesn't work when the test signature is a superset of the original signature. Based on geometrical shape of the critical regions of the signature, a graph matching based signature verification technique is introduced in [13]. The comparison of two signatures is reduced to the comparison of their respective graph representations. The graph matching reduces the complexity of Hungarian matching and precisely models different shapes in the signature to obtain a perfect match. Two efficient

offline signature verification methods are proposed using Fourier descriptor and Chained Codes and another is using Multi Scale Fourier descriptor and Wavelet Transform in [14], and [15]. A signature verification method is proposed using artificial neural network in [16], and [17]. Signature verification using Euclidian Distance between the mean signatures of training dataset and test data using maximum, average and minimum threshold is proposed in [18]. Signature verification still remains an open challenge since a signature is judged to be genuine or a forgery only on the basis of a few reference specimens.

3. IMPLEMENTATION

The signature verification system takes a query signature as input. Then it is compared with the genuine signatures those are stored in the database to see if a particular query signature belongs to a particular person. The proposed signature verification system primarily involves four steps: image acquisition, pre-processing, features extraction, and feature matching.

3.1 Image Acquisition

Signature images are captured by any type of digital camera for pre-processing the image as shown in figure 1.

Fig 1: Color Signature Image

3.2 Preprocessing

Captured color image is converted into binary image as shown in figure 2. Then, binary signature image is cropped to keep only the signature as the content as shown in figure 3.

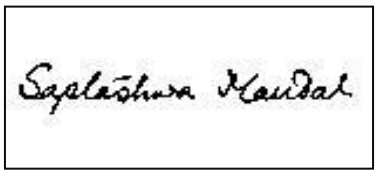

Fig 2: Binary Signature Image

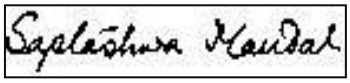

Fig 3: Cropped signature Image

3.3 Feature Extraction

The following features are extracted from the cropped signature image.

3.3.1 Height to Width Ratio (F1)

The height and width may change however the height to width ratio of the signature area would remain nearly constant.

F1= (number of rows in cropped image / number of column in cropped image)

3.3.2 Signature Occupancy Ratio (F2)

The density of the image or the occupancy ratio of the image is the amount of space occupied by the signature within the whole image. Hence, it can be defined as the ratio of the number of pixels in the signature to the total Number of pixels in the cropped image.

F2 = (number of pixels fall on signature / number of pixels in cropped image)

3.3.3 Adjacency Ratio (F3)

Find the position of the first white pixel in each column from the top and store in the 1D Array (LT). Then, find the position of the first white pixel in each column from the bottom and store in the 1D Array (LB).

F3= (sum of all elements of LT/ sum of all elements of LB) * signature occupancy ratio

3.3.4 White Pixel Ratio (F4 and F5)

The image in then divided virtually into two halves, left and right and then the ratio of the number of white pixels in one half to the total image is calculated. Hence,

F4= (number of white pixels in the 1st half of negative image / number of white pixels in the whole negative image)

F5 = (number of white pixels in the 2nd half of negative image / number of white pixels in the whole negative image)

3.3.5 Corner ratio using Harris Corner Method (F6 and F7)

The ratio of the Number of corners detected in one half of the image to the number of corners in the whole negative image is detected and extracted as a feature.

F6= (number of corners in the 1st half of negative image / number of white pixels in the whole negative image)

F7 = (number of corners in the 2nd half of negative image / number of white pixels in the whole negative image)

3.3.6 Coordinates of the Centre of mass of the image (F8 and F9)

The center of mass is a 2-tuple(X, Y).

F8= average x coordinate values of all signature pixels

F9= average y coordinate values of all signature pixels

3.3.7 Slope of the line joining the Centre of masses of the two halves of the signature image (F10)

The slope of the line joining the centre of masses of the two halves of the signature image is calculated and extracted as a feature. The two centre of masses being (x_1, y_1) and (x_2, y_2).

$$F10 = (y_2 - y_1)/(x_2 - x_1)$$

3.3.8 Distance of the line joining the centre of masses of the two halves of the signature (F11)

The distance of the line joining the two centers of masses of the two halves of the signature image is calculated and extracted as a feature.

$$F11 = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

3.4 Feature Matching

After extracting all the features F1 to F11, for each training dataset on an individual, the mean signature dataset is created. Then the features of a query signature are also extracted. Now the Euclidian distance between the mean signature dataset and the query signature dataset is computed. The maximum and minimum value of the Euclidian distance between training signature samples are used to set the acceptance range, the

maximum threshold and minimum threshold respectively, for dataset of each individual. If the Euclidean distance of the query signature image with respect to mean signature image is above the threshold range, the query signature is detected as forged otherwise it is detected as an original one. There are three different percentages that have been used to measure the performance. These are False Acceptance Rate (FAR), False Rejection Rate (FRR), and Accuracy. FAR is the percentage of forgeries that are incorrectly classified. FRR is the percentage of original signatures that are incorrectly classified. Accuracy is the percentage of signatures which are exactly classified.

4. ALGORITHM

Step 1: A set of signatures of an individual is taken as an input and hence considered as a training data set.

Step 2: The colored signature images are converted into binary images.

Step 3: The bounding boxes of the signature image is detected and thereby cropped to boundary boxes.

Step 4: The features F1 to F11 from each signature image is extracted and stored in a feature matrix.

Step 5: Mean signature feature values are computed.

Step 6: The query signature features are extracted and the Euclidian distance between the query signature features and mean signature features is computed.

Step 7: If the distance is above a certain threshold then the query signature is forgery otherwise it is original.

5. RESULT

This section introduces the experimental results. Above mentioned FAR, FRR, and Accuracy have been tested using different threshold values and the results have been tabulated in table 1. The thresholds are Max, Pre-computed, and Average. Max threshold is computed while dataset is created. It is based on the maximum Euclidean distances from the original signatures to the mean signature. It has been found that very few original signatures cross this threshold. Pre-computed threshold is computed while dataset is created. It is based on the minimum Euclidean distances from the original signatures to the mean signature. This threshold varies according to the signatures used and usually increases the FRR and decreases the FAR. Average Threshold is the average of max threshold and the pre-computed threshold, possibly resulting in an acceptable tradeoff between FAR and FRR.

Table 1. Tested Result for Different Threshold Value

Data set	Training Signature	Test Signature	Max Threshold			Pre-computed Threshold			Average threshold		
			FRR	FAR	Accuracy	FRR	FAR	Accuracy	FRR	FAR	Accuracy
D1	10 originals	5 originals 10 forged	0%	10%	93.33%	20%	10%	86.67%	20%	10%	86.67%
D2	10 originals	5 originals 10 forged	0%	50%	66.67%	0%	30%	80%	0%	40%	73.33%
D3	10 originals	5 originals 10 forged	0%	10%	93.33%	0%	10%	93.33%	0%	10%	93.33%
D4	10 originals	5 originals 10 forged	0%	0%	100%	0%	0%	100%	0%	0%	100%
D5	10 originals	5 originals 10 forged	0%	60%	60%	0%	50%	66.67%	0%	60%	60%
D6	10 originals	5 originals 10 forged	0%	0%	100%	0%	0%	100%	0%	0%	100%
D7	10 originals	5 originals 10 forged	0%	0%	100%	0%	0%	100%	0%	0%	100%
Total		35 originals 70 forged	0%	18.57%	87.61%	2.86%	14.28%	89.52%	2.86%	17.14%	87.61%

6. CONCLUTIONS

Several authors have suggested different methods for signature verification of an individual. Different clustering methods like K-means, fuzzy c-means, hierarchical clustering has been used for features classification. In this paper, a new technique is used to extract features from signature image and classify the signature using Euclidian distance measurement. The experimental results provide a reliable solution with accuracy up to 100% for verification of actual signature with forgery. The proposed algorithm will help the community those who are interested on biometric features like iris, thumb impression, and face features for authentication. The system can detect random, simple and semi-skilled forgeries but the performance deteriorates in case of skilled forgeries. False acceptances as well as false rejections can be reduced by using a larger database. The performance can be improved using dynamic information gathered during the time of signature. The concepts of Fuzzy C-Means and Neural Networks give a lot of assurance to build the systems with high accuracy.

7. ACKNOLODGEMENT

The authors are thankful to all the teachers of the department of Computer Applications, RCC Institute of Information Technology, Kolkata for their support to improve this paper. The authors are also thankful to all persons who have given the permission to use their signature images.

8. REFERENCES

[1] R. Plamondon, and G. Lorette, "Automatic signature verification and writer identification: The state of the art", Pattern Recognition, vol. 22, no. 2, pp. 107–131, Jan. 1989.

[2] F. Leclerc and R. Plamondon, "Automatic signature verification: The state of the art 1989–1993", International Journal in Pattern Recognition and Artificial Intelligence (IJPRAI), vol. 8, no. 3, pp. 643–660, Jun. 1994.

[3] R. Plamondon, "The Handwritten Signature as a Biometric Identifier: psychophysical Model & System Design", IEEE Conference Publications, Issue CP408, pp. 23-27, May 1995.

[4] D. S. Doermann and A. Rosenfeld, "Recovery of temporal information from static images of handwriting", International Journal of Computer Vision (IJCV), vol. 15, pp. 143–164, 1995.

[5] M. C. Fairhurst, "Signature verification revisited: Promoting practical exploitation of biometric technology", Electronics & Communication Engineering Journal, vol. 9, no. 6, pp. 273–280, Dec 1997.

[6] G. Rigoli, A. Kosmala, "A Systematic Comparison Between on-line and off-line Methods for Signature Verification with Hidden Markov Models", 14th International Conference on Pattern Recognition - vol. II, pp.1755—1757, Australia, 1998.

[7] Edson J. R. Justino, Abdenaim El Yacoubi, Flavio Bortolozzi, Robert Sabourin, "An Off-Line Signature Verification System Using Hidden Markov Model and Cross-Validation", 13th Brazilian Symposium on Computer Graphics and Image Processing, pp.105-112, ISBN:0-7695-0878-2, 2000.

[8] R. Plamondon and S. N. Srihari, "On-line and off-line handwriting recognition: A comprehensive survey", IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 22, no. 1, pp. 63–84, Jan. 2000.

[9] Jain, F. Griess, and S. Connel, "Online Signature Recognition", Pattern Recognition, vol.35, pp 2963-2972, 2002.

[10] M. K. Kalera, S. Srihari, and A. Xu, "Off-line signature verification and identification using distance statistics", International Journal of Pattern Recognition and Artificial Intelligence, 18(7), pp. 1339-1360, 2004.

[11] M. Hanmandlu, M. H. M. Yusof, and V.K. Madasu, "Off-line Signature Verification using Fuzzy Modeling", Pattern Recognition, vol. 38, pp. 341-356, 2005.

[12] Ibrahim S. I. ABUHAIBA, "Offline Signature Verification Using Graph Matching", Turkish Journal of Electrical Engineering & Computer Sciences, vol.15, no. 1, pp 89-104, 2007.

[13] Bansal B. Gupta, G. Khandelwal, and S. Chakraverty, "Offline Signature Verification Using Critical Region Matching", International Journal of Signal Processing, Image Processing and Pattern, Vol. 2, No.1, March, 2009.

[14] Ismail A. Ismail, Mohamed A. Ramadan, Talaat S. El. Danaf, Ahmed H. Samak, "An Efficient Off-line Signature Identification Method Based On Fourier Descriptor and Chain Codes", International Journal of Computer Science and Network Security (IJCSNS), Vol.10 No.5, May 2010.

[15] Ismail A. Ismail, Mohamed A. Ramadan, Talaat S. El. Danaf, Ahmed H. Samak, "Signature Recognition using Multi Scale Fourier Descriptor And Wavelet Transform", International Journal of Computer Science and Information Security (IJCSIS) Vol. 7, No. 3, pp. 14-19, 2010.

[16] V. Pandey, S. Shantaiya, "Signature Verification Using Morphological Features Based on Artificial Neural Network", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012.

[17] S. Sthapak, M. Khopade, C. Kashid, "Artificial Neural Network Based Signature Recognition & Verification","International Journal of Emerging Technology and Advanced Engineering(IJETAE), Volume 2, Issue 8, pp. 191-197, August 2013.

[18] R. Jana, R. Saha, D. Datta, "Offline Signature Verification using Euclidian Distance", International Journal of Computer Science and Information Technologies (IJCSIT), Volume 5, Issue 1, pp. 707-710, 2014.