ISSN:0975-9646

Offline Signature Verification using Euclidian Distance

Ranjan Jana , Rituparna Saha , Debaleena Datta

Department of CA, RCC Institute of Information Technology
Kolkata, West Bengal, India

***Abstract*— Signature authentication is the most widely used method of verifying a person's identity. The texture and topological features are the static features of a signature image. Baseline slant angle, aspect ratio, normalized area, center of gravity of the whole signature image and the slope of the line joining the center of gravities of two halves of a signature image are used as the texture and topological features of the signature. The system is initially trained using a set of original signatures obtained from individuals whose signatures have to be authenticated by the system. The mean values and standard deviations of all the original signature features are computed. This mean signature features acts as the template for verification against a claimed test signature. Euclidian distance in the feature space between the claimed signature and the template serves as a measure of similarity between the two. If this distance is less than a pre-defined threshold, the test signature is verified to be that of the original signature otherwise detected as a forgery. The system gives the result to classify original and forgery signature with accuracy up to 100%.**

***Keywords*— Signature verification, Euclidian distance, Signature recognition, Feature extraction, Biometric.**

I. INTRODUCTION

A handwritten signature is the scripted name or legal mark of a person's identity, executed by hand and it is used for the purpose of authentication. People are familiar with the use of signatures in their daily life. Signature is an age-old distinguishing feature for individual's identification. Even today an increasing number of transactions, especially in financial sectors, are being authorized via signatures. Hence, methods for automatic signature verification must be developed if authenticity is to be verified on a day to day basis. There are several approaches of verifying the authenticity of a signature. Approaches for signature verification fall into two categories according to the acquisition of the data i.e. On-line and Off-line.

On-line data records the motion of the stylus when the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time. These dynamic characteristics are specific to each individual and sufficiently stable as well as repetitive. Off-line data is a 2-D image of the signature obtained physically by means of a digital camera. Processing Off-line 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 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 cause large intrapersonal variation. Signatures are a special case of handwriting subject to intrapersonal variation and interpersonal differences. This variability makes necessary to analyze signatures as complete images and not as collection of letters and words. Any signature verification system built on five stages: data acquisition, pre-processing, feature extraction, comparison process, and performance evaluation. Handwriting is a skill that is highly personal to individuals and consists of graphical marks on the surface in relation to a particular language. Signatures of the same person can vary with time and state of mind.

In this paper, effective offline signature verification using texture and topological features from signature images are proposed. For better performance, the texture and topological features of signature image like baseline slant angle, aspect ratio, center of gravity of the whole signature image and the slope of the line joining the center of gravities of two halves of a signature image are calculated. Based on the texture and topological information, signature verification is done using Euclidian distance in the feature space between the claimed signature and the template serves as a measure of similarity between the two. This paper is organized into the following sections. Section II describes an overview of previous work. Implementation details for offline signature verification are mentioned in section III. Experimented results are mentioned in section IV. Finally, the conclusions are in section V.

II. PREVIOUS WORK

The use of the signature has a long history which goes back to the appearance of writing itself [1]. Utilization of the signature as an authentication method has already become a tradition in the western civilization and is respected among the others. The signature is an accepted proof of identity of the person in a transaction taken on his or her behalf [2]. Unfortunately, a handwritten signature is the result of a complex process depending on the psychophysical state of the signer and the conditions under which the signature apposition process occurs [3], [4]. Signatures are generally recognized as a legal means of verifying an individual's identity by administrative and financial organizations [5]. Many research works on signature verification have been reported. Researchers have applied many technologies, such as neural networks and parallel processing to the problem of signature verification

and they are continually introducing new ideas, concepts, and algorithms.

A systematic comparison between on-line and off-line signature verification are compared based on Hidden Markov Models in [6]. Different methods for signature verification system which extracts certain dynamic features derived from velocity and acceleration of the pen together with other global parameters like total time taken, number of pen-ups is proposed in [7], [8], and [9]. Features are modeled by fitting probability density functions by estimating the mean and variance of the signature features of the same person with respect to time and state of mind. Another signature verification method is proposed using distance statistics of morphological features in [10]. Based on fuzzy modeling using angle features extracted from box approach is proposed to verify signature in [11].

A graph-based approach, compare the outer contour of the signatures based on the Hungarian method is proposed for automatic signature verification in [12]. This approach has two limitations: (1) It works on relatively small window sizes (32*64) and (2) It fails when the test signature is a superset of the original signature. Another graph-matching based automatic signature verification technique is proposed in [13], which is based on geometrical shape of the critical regions of the signature. The comparison of two objects is reduced to the comparison of their respective graph representations. It scales down the complexity of Hungarian matching and precisely models different shapes in the signature to obtain a perfect match. An efficient off-line signature identification method is proposed using Fourier descriptor and Chain codes in [14]. Another signature verification method is proposed using artificial neural network based on morphological features in [15]. 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.

III. IMPLEMENTATION

The signature verification system takes a query signature as input. Then it is compared with the genuine signatures contained in the database to see if a particular query signature belongs to a particular person. This signature verification system primarily involves three steps: Pre-processing, Feature extraction, and Verification.

A. Pre-processing

Signature pre-processing is a necessary step to improve the accuracy of feature extraction. The pre-processing stage primarily involves of the following steps. First, Color signature image is converted into gray image and binary image as shown in Fig. 1, Fig. 2, and Fig. 3. Dust on camera lens, imperfection in the scanner lighting might introduces the noise in the image. For that reason, Median filter is used to remove the noise like “salt and pepper” noise before processing. Signature image may be inclined with respect to horizontal axis as shown in Fig. 4. Both gray image and binary image are rotated to make the signature parallel to the horizontal axis as shown in Fig. 5, and Fig. 6. The region where the signature is exactly situated is cropped as shown in Fig. 7, and Fig. 8. Cropping is done with respect to bounding box of image by calculating first foreground row, first foreground column, last foreground row and last foreground column to obtain region of interest.

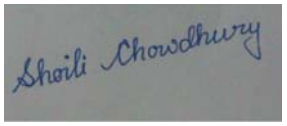

Fig. 1: Color Image

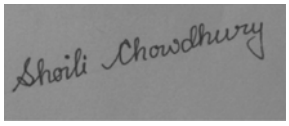

Fig. 2: Gray Image

Fig. 3: Binary Image

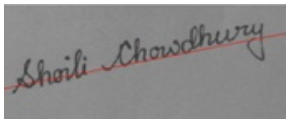

Fig. 4: Inclined Image

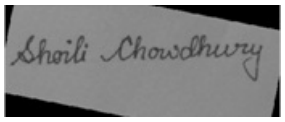

Fig. 5: Rotated Gray Image

Fig. 6: Rotated Binary Image

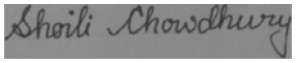

Fig. 7: Cropped Gray Image

Fig. 8: Cropped Binary Image

B. Feature Extraction

Feature extraction is the most important task to improve the accuracy of signature verification system. The following features are extracted from pre-processed signature image.

1) *Height to Width Ratio (F1):* The feature F1 is the ratio of height to width of the signature. The bounding box coordinates of the cropped signature are determined, and the height and width are computed using these coordinates. Height and width of the Signature can change for a person in different times. But height-to-width ratio of an individual’s signatures is approximately constant.

F1 = (height of the signature / width of the signature)

2) *Occupancy Ratio (F2):* The feature F2 is the ratio of number of pixels which belong to the signature and total number of pixels of the signature image. This feature provides information about the signature density.

F2 = (number of pixels which belong to the signature / total number of pixels in the signature image)

3) *Density Ratio (F3):* Signature image is divided into two halves vertically. The feature F3 is the ratio of number of pixels which belong to the left half of the signature image to number of pixels which belong to the right half of the signature image. It provides information about the signature density ratio of two halves of the signature image.

F3 = (density of the left half of signature / density of the right half of the signature)

4) *Critical points (F4):* Corners are regions in the image with large variation in intensity in all the directions. Here corners points treated as critical points. Numbers of critical

points are counted in the signature image using Harris corner method. The feature F4 is the number of critical points in the signature image.

5) *Center of Gravity (F5):* Number of white pixels which belong to the binary signature image is treated as ON pixel. Center of Gravity is the average coordinate point of all ON pixels of the binary signature image.

6) *Slope of the Center of Gravities (F6):* Signature image is divided into two halves vertically and the center of gravity of the two halves are determined separately. The feature F6 is the slope of the line joining the Center of Gravities calculated.

7) *Center of Masses of Sub-regions (F7):* First, the signature is divided vertically to get two centres of masses. Then, each half of signature image is divided horizontally to get four centers of masses. Again, four regions of signature image are divided vertically to get eight centers of masses. Finally, eight regions of signature image are divided horizontally to get sixteen centers of masses. The feature F7 is the above thirty centers of masses of the signature image.

The above features F1 to F7 are extracted and stored in a feature vector. This feature vector is used to train the system as well as for verification of a sample signature.

C. Verification

The features F1 to F7 are extracted from signature images of different persons. The features extracted from each person's group are used to derive a mean signature features for each person. Then all the features of a query signature is extracted to calculate the Euclidian distance with respect to the mean signature features of the original (training) signature images. The maximum and minimum Euclidian distance values of training signature sample are used to set the acceptance range. If the Euclidean distance of the query signature image with respect to mean signature image is within the acceptance range, the query signature is authenticated otherwise it is detected as a forged one. Three different percentages have been used to measure the performance of the system. These are False Rejection Rate (FRR), False Acceptance Rate (FAR), and Accuracy. FRR is the percentage of original signatures that are incorrectly classified. FAR is the percentage of forgeries that are incorrectly classified. Accuracy is the percentage of signatures those are exactly classified. The threshold must be chosen so that there is an acceptable trade-off between False Acceptance Rate (FAR) and False Rejection Rate (FRR). Choosing a high threshold value will increase FAR and choosing a low threshold value will increase FRR. For the purposes of this work, the value 2.5 is chosen as a threshold.

Algorithm for Signature Verification using Euclidian Distance

STEP 1: Input a set of signatures belonging to a person.
STEP 2: Convert each colored signature image into gray image and binary image.
STEP 3: Perform noise reduction on both binary and gray images.
STEP 4: Perform rotation on binary images to equalize the inclination of all signatures based on the baseline slant.
STEP 5: Find the bounding boxes of the images and crop on the basis of these boxes.
STEP 6: Extract the features F1, F2, F3, F4, F5, F6, and F7 from each signature and store in a feature matrix.
STEP 7: Dataset is created by computing the mean signature feature values.
STEP 8: Calculate the Euclidian distance of query signature features from the mean signature features of the dataset.
STEP 9: If the distance is below a certain threshold then the query signature is verified to be that of the claimed person otherwise it is detected as a forged one.

IV. RESULTS

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:

A. Max Thresold

Max Threshold value 2.5 is reliant on the features used for calculating the Euclidean Distance. It is not recommend for using a threshold greater than this value for these features. It has been found that very few original signatures cross this threshold.

B. Pre-computed Threshold:

This threshold is computed while creating the dataset. It is based on the maximum 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.

C. Average Threshold

The performance has also been tested with the mean of the max threshold and the pre-computed threshold, possibly resulting in an acceptable tradeoff between FAR and FRR. Table 1 shows the result obtained on testing with datasets collected from different people. Skilled forgeries' signature have also been used for testing purpose.

TABLE 1
PERFORMANCE ANALYSIS USING MAX THRESHOLD, PRE-COMPUTED THRESHOLD, AND AVERAGE THRESHOLD

Dataset Name	Training Signature	Test Signature	Max Threshold			Pre-computed Threshold			Average Threshold		
			FRR	FAR	Accuracy	FRR	FAR	Accuracy	FRR	FAR	Accuracy
D1	10 originals	6 originals 10 forgeries	0%	50%	68.75%	50%	0%	81.29%	33.3%	40%	62.5%
D2	10 originals	14 originals 12 forgeries	0%	16%	92.3%	21.4%	0%	92.3%	14.2%	0%	96.15
D3	8 originals	4 originals 12 forgery	0%	0%	100%	25%	0%	93.75%	25%	0%	93.75%
D4	8 originals	4 originals 12 forgeries	25%	16.7 %	81.25%	25%	0%	93.75%	25%	0%	93.75%
D5	8 originals	4 originals 13 forgeries	25%	23%	76.47%	50%	0%	88.23%	25%	7.7%	88.23%
Total		32 originals 59 forgeries	6.2%	22%	84.61%	31.2%	0%	90.1%	21.9%	8.5%	87.91%

V. CONCLUSIONS

A number of methods have been proposed by several authors for clustering data. Hierarchical clustering, self-organizing maps, K-means, and Fuzzy c-means have all been successful in particular applications. A new method to extract features from handwritten signature and verification of it is presented here. The proposed method promises a very simple but reliable solution to the problem of signature verification. Achieved results are encouraging and suggest the adequacy of the selected features. Experimental results clearly show that this method can indeed differentiate forgery with actual ones with accuracy up to 100%. The proposed algorithm will help community in the field of signature verification, signature analysis and signature recognition. This work studies an image clustering process based on Euclidian distance approach enabling to handle clusters of different sizes and shapes of signatures. The proposed image clustering technique can also be used in the field of Face recognition and Thumb impression recognition.

ACKNOWLEDGMENT

The authors are grateful to all the faculty members of MCA department, RCC Institute of Information Technology, Kolkata for their help and support to improve this paper. The authors are also grateful to all persons who have given the permission to use their signature images.

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] 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.

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

[9] S. Nanavati, M. Thieme, and R. Nanavati, "Biometrics: Identity Verifica-tion in a Networked World", New York: Wiley, pp. 123–131, 2002.

[10] M. K. Kalera, S. Srihari, and A. Xu, "Off-line signature verification and identification using distance statistics", International Journal of Patern 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 38, pp. 341-356, 2005.

[12] Ibrahim S. I. ABUHAIBA, " Offline Signature Verification Using Graph Matching", Turk J Elec Engin, 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] 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.