International Association of Scientific Innovation and Research (IASIR)
(An Association Unifying the Sciences, Engineering, and Applied Research)

ISSN (Print): 2279-0047
ISSN (Online): 2279-0055

International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

An Offline Signature Verification System: An Approach Based On Intensity Profile

Charu Jain[1], Priti Singh[2], Aarti Chugh[3]
Department of Computer Science [1, 3], Department of Electronics and Communication [2],
Amity University, Gurgaon, Haryana, India.

Abstract: *Image Intensities have been processed traditionally without much regard to how they arise. Typically they are used only to segment an image into regions or to find edge-fragments. Image intensities do carry a great deal of useful information about three-dimensional aspects of objects and some initial attempts are made here to exploit this. Here we propose an algorithm which uses the inveterate characteristic features to recognize signatures with perceptive accuracy by utilizing the intensity variations in the way in which they may be written.*
Keywords: *Intensity Profile (IP), False Acceptance Rate (FAR), False Rejection Rate (FRR).*

I. Introduction

Signature verification is an important research area in the field of authentication of a person as well as documents. The importance of signature verification arises from the fact that it has long been accepted in government, legal, and commercial transactions as an acceptable method of verification [1] [12]. The problem of offline signature verification [4] has been faced by taking into account three different types of forgeries: random forgeries, Simple forgeries and skilled forgeries [6].

There are two major methods of signature verification systems. One is an on-line method to measure the sequential data such as handwriting speed and pen pressure with a special device. Off-line[7] [8] data is a 2-D image of the signature and processing off-line is complex due to the absence of stable dynamic characteristics of the individual [5]. 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 coupled together cause large intra-personal variation. A robust system [13] [14] [15] has to be designed which should not only be able to consider these factors but also detect various types of forgeries. The system should neither be too sensitive nor too coarse. It should have an acceptable trade-off between a low False Acceptance Rate (FAR) and a low False Rejection Rate (FRR). The false rejection rate (FRR) and the false acceptance rate (FAR) are used as quality performance measures. The FRR is the ratio of the number of genuine test signatures rejected to the total number of genuine test signatures submitted. The FAR is the ratio of the number of forgeries accepted to the total number of forgeries submitted. The offline method, therefore, needs to apply complex image processing techniques to segment and analyze signature shape for feature extraction [2], [3]. Here, we propose an experimental method for the extraction of intensity profiles of offline signatures. The intensity profile of an image is the set of intensity values taken from regularly spaced points along a line segment or multiline path in an image. For points that do not fall on the center of a pixel, the intensity values are interpolated. Our work can be further expanded by merging more quantitative measures to provide better accuracy.

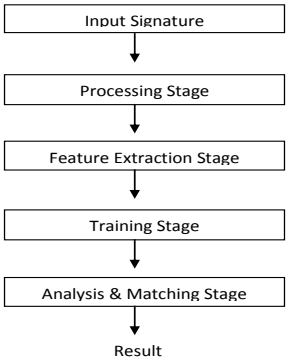
II. Methodology

The overall architecture of our signature recognition system follows: Signature acquisition, Preprocessing, Feature extraction, and Classification. Offline signatures are the signatures made on papers. This requires specifying the resolution, image type and format to be used in scanning each image. In any offline signature verification system, the first step is to extract these signatures from paper using scanner.

A. Data Acquisition and pre-processing

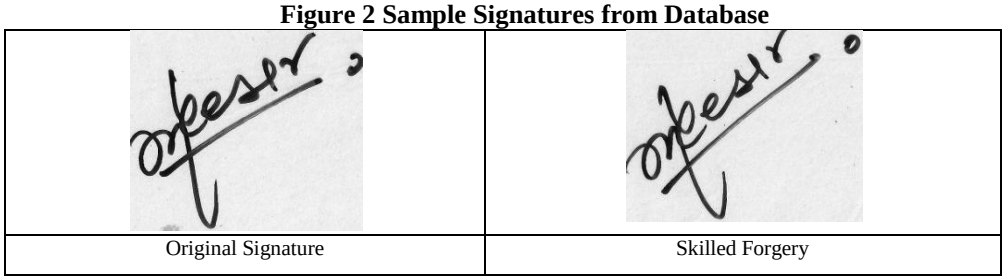
The system has been tested for its accuracy and effectiveness on data from 25 users with 10 specimens of each making up a total of 250 signatures. The proposed verification algorithm is tested on both genuine and forged signature sample counterparts. So we developed a signature database which consists of signatures from all the age groups. Our database is also language independent and also it consists of signatures done with different pens with different colors. 10 users were asked to provide genuine signatures, 5 were asked to do skilled forgeries, 5 provide casual forgeries and 5 did random forgeries. A scanner is set to 300-dpi resolution in 256 grey levels and then signatures are digitized.

Figure 1 Methodology of Signature Verification System



For further working we cut and pasted scanned images to rectangular area of 3 x 10 cm or 400 x 1,000 pixels and were each saved separately in files. The signature samples from the data base are shown in Figure 2.

Figure 2 Sample Signatures from Database



Original Signature	Skilled Forgery

The scanned signature may contain spurious noise. Hence we started with preprocessing. In preprocessing stage, the RGB image of the signature is converted into grayscale and then to binary image. Thinning is applied to make the signature lines as single thickness lines and any noise present in scanned images are removed thus making the signature image ready to extract features.

B. Feature Extraction

Feature extraction process [9] [10] [11] is an important step in developing any signature verification system since it is the key to identifying and differentiating a user's signature from another.

Features available to extract in offline signatures can be either global features i.e. features extracted from whole images or local features i.e. features extracted from local region or part of the signature. In this system, the features extracted are intensity and intensity profile. An 'intensity profile' gives a one-dimensional view of a single cross-section of the data. It is a popular technique in photographic analysis as well, where a 'density profile' is constructed. These are used to train the system. The mean value of these profiles is obtained. In order to keep the problem under control, we use only pairs of points (defining line segments) and keep only interest points that show very high stability with respect to scale and rotation change of the image [16].

Figure 2 (a) Intensity Profile of Trained Sample for genuine signature

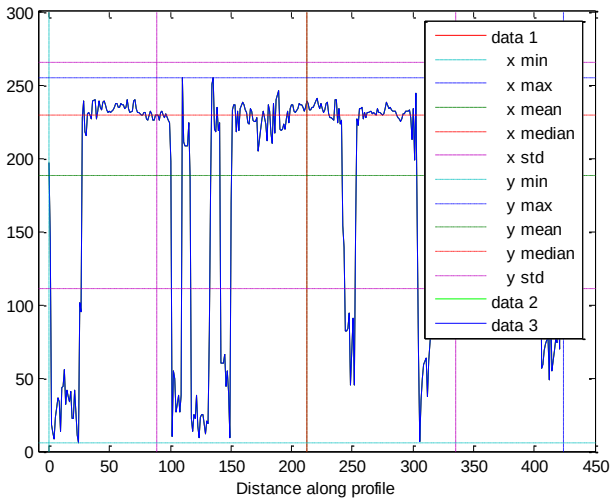


Table 1 Statistics for Sample Signature

	X	Y
Minimum Value	0	6
Maximum Value	424.1	255
Mean	212.1	188.1
Median	212.1	229
Standard Deviation	122.9	77.36
Range	424.1	249

The intensity profiles of a signature are extracted from a sample group of signature images of different persons. The values derived from each sample group are used in deriving a mean intensity profile for each group of samples. The mean values and standard deviations of all the profiles are computed and used for final verification. A sample plot for genuine signature is shown in figure 2 (a). Table 1 provides values computed from this plot.

Figure 2 (b) Intensity Profile of Test Signature

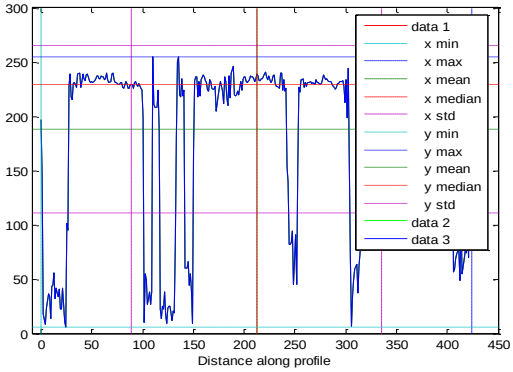


Table 2 Statistics for Test Signature

	X	Y
Minimum Value	0	5
Maximum Value	424	251
Mean	208	199.1
Median	208	230
Standard Deviation	120.6	75.71
Range	424.1	247

C. Verification Phase

In the next step the scanned signature image to be verified is fed to the system. It is preprocessed to be suitable for extracting features. It is fed to the system and its intensity profile is extracted. These values are then compared with the mean features that were used to train the system. Depending on whether the input signature satisfies the condition the system either accepts or rejects the signature.

The intensity profile (IP) extracted from database are compared with the intensity profile (IP) extracted from test signatures and based on the classification criteria the signatures are classified either genuine or forged.

Figure 2(c) Difference of Intensity Profiles of Sample Signature and Test Signature

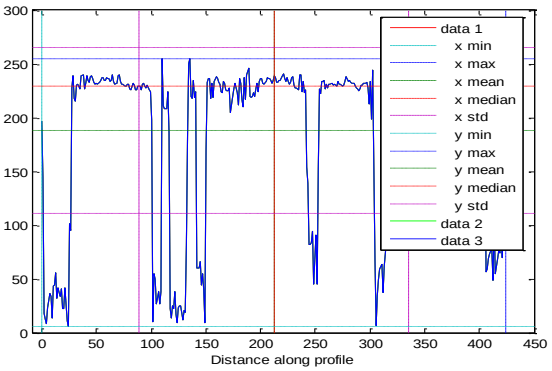
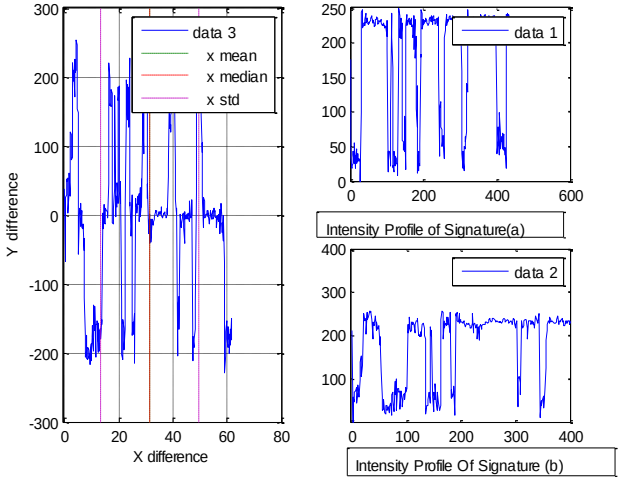


Table 3 Statistics for Difference of Intensity Profile

	X	Y
Minimum Value	0	1
Maximum Value	0.1	4
Mean	4.1	-11
Median	4.1	-1
Standard Deviation	2.3	1.65
Range	0	2

Figure 3(c) Difference between intensity profiles of forged signatures



III. Results

False Acceptance Rate (FAR) and False Rejection Rate (FRR) are the two parameters used for measuring performance of any signature verification method. The results of our simulation for forged and genuine signatures are as shown in the table 4. The system is robust; it rejected all the casual forgeries. Out of all the genuine signatures that were fed in, 4 were rejected as forgeries. FAR and FRR are calculated by given equations.

FAR = (number of forgeries accepted/number of forgeries tested) * 100

FRR = (number of originals rejected/number of originals accepted) *100

This yielded a False Rejection Rate (FRR) of 5.26%. Also out of 50 skilled forgeries fed into the system, 5 signatures were accepted. This gave us a False Acceptance Rate (FAR) of 10%.

Table 4: Results for genuine and forged Signatures

Nature Of Signature	False Acceptance Rate	False Rejection Rate
Original	------	5.26%
Casual Forgery	0%	------
Skilled Forgery	10%	------

IV. Conclusions

The methodology followed by us uses various geometric features to characterize signatures that effectively serve to distinguish signatures of different persons. We can see that the best performance was given by dominant intensities in a signature. The system is robust and can detect random, simple and semi-skilled forgeries but the performance deteriorates in case of skilled forgeries. By observing the individual performance of each signature, we found that the complexity of the signature, and the character of the signature do not affect the performance of the intensity profile method. We are further going to enhance our work by including correlation coefficient for signature classification. Using a higher dimensional feature space and also incorporating dynamic information gathered during the time of signature can also improve the performance.

V. References

[1] A.K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, January 2004.

[2] Diana Kalenova, "Personal Authentication Using Signature Recognition", Department of Information Technology, Laboratory of Information Processing, Lappeenranta University of Technology.

[3] J. Fierrez-Aguilar et al., "An off-line signature verification system based on fusion of local and global information," in Proc. BIOAW,LNCS-3087, pp. 295–306, 2004.

[4] H B kekre, V A Bharadi, "Specialized Global Features for Off-line Signature Recognition", 7th Annual National Conference on Biometrics RFID and Emerging Technologies for Automatic Identification, VPM Polytechnic, Thane, January 2009.

[5] Faundez-Zanuy, M., 2005. Biometric recognition: why not massively adopted yet?, s. Syst. Mag., 20(8): 25-28.

[6] Hemanta Saikia,KC Sarma, 2012, "Approaches and Issues in Offline Signature Verification System "International Journal of Computer Applications (0975 – 8887) Volume 42– No.16, March 2012.

[7] Batista, L., Rivard D., Sabourin R., Granger E., Maupin P. 2007. "State of the art in off-line signature verification" In: Verma B., Blumenstein M. (eds.), Pattern Recognition Technologies and Applications: Recent Advances, (1e). IGI Global, Hershey (2007).

[8] Arya M S and Inamdar V S. (2010). "A Preliminary Study on Various Off-line Hand Written Signature Verification Approaches". 2010 International Journal of Computer Applications. Volume 1, No. 9 (pp 0975 – 8887)

[9] Ramachandra , Ravi, Raja, Venugopal and Patnaik, Signature Verification using Graph Matching and Cross-Validation Principle, Int. J. of Recent Trends in Engineering (IJRTE),Vol. 1 (1), May 2009,Page(s): 57-61.

[10] Samaneh and Moghaddam, Off-Line Persian Signature Identification and Verification Based on Image Registration and Fusion", Journal of Multimedia, Vol 4, No 3 (2009).

[11] Larkins and Mayo, "Adaptive Feature Thresholding for offline signature verification", 23rd International Conference In Image and Vision Computing New Zealand (2008), pp. 1-6.

[12] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004

[13] Bence Kovari. "The development of off-line signature verification methods, comparative study," 2007. microCAD 2007 International Scientific Conference.

[14] "Pattern Recognition, special issue on automatic signature verification," June 1994, Vol. 8, no. 3.

[15] K. Anil Jain. "Handwritten Signature Recognition" Michigan State University - Biometrics. [Online] http://www.cse.msu.edu/~cse891/Sect601/SignatureRcg.pdf.

[16] J. Matas, J. Buri´anek, J. Kittler "Object Recognition using the Invariant Pixel–Set Signature" BMVC, British Machine Vision Association, (2000).