An Automated System for Offline Signature Verification and Identification Using Delaunay Triangulation

Zahoor Jan, Hayat Muhammad, Muhammad Rafiq, and Noor Zada

Department of Computer Science, Islamia College University Peshawar, Pakistan
zahoor.jan@icp.edu.pk,
{hayatvu,noorzadamohmand}@yahoo.com,
rafiqmscs@hotmail.com

Abstract. Offline signature is being used in a range of applications. When a fraud person replicates our signature and takes our identity then problem arises. Signature verification has been identified as a main competitor in the search for a secure personal verification system. Offline signature system is based on the scanned image of the signature. The proposed methodology consists of signature database, preprocessing, feature extraction and recognition. The proposed signature system functions based on Delaunay triangulation of a given signature sample. The false acceptance rate (FAR) and false rejection rate (FRR) rate in the proposed method is relatively reduced. The signature for genuine person is accepted while the forged signature is rejected.

Keywords: Signature verification, offline signature, Delaunay triangulation, false acceptance rate, false rejection rate.

1 Introduction

Biometrics is a technique that is associated to human characteristics and is based on physical and behavioral characteristics. The physical characteristic includes face recognition, fingerprints, DNA, hand geometry, iris scan and retina scan. While on the contrast the behavioral characteristics are signature recognition and voice recognition. In official matter humans are renowned by their signatures for authentication and authorization. Every individual has their own writing technique and for this reason their signature is used in the financial area for identity authentication. To build up a technique is very essential which is efficient in identifying the handwritten signature is accurate or forged. Advantages of offline signature recognition includes: it does not depend upon the age and it is also not affected by the occlusion, illumination, pose variation just like in case of other biometrics such as finger print and face recognition[1][2].

Signature verification is categorized in two groups i.e. on-line and off-line. On-line signature can be obtained by pen-tablets that find out dynamic characteristic of a signature in by analyzing its shape [3]. These features of the signature are based on pen pressure, velocity and number of strokes. On the contrast to off-line systems lack

Á. Rocha et al. (eds.), *New Contributions in Information Systems and Technologies*,
Advances in Intelligent Systems and Computing 353, DOI: 10.1007/978-3-319-16486-1_64

the characteristic such as the number and order of strokes, the velocity and other information therefore it is complex to design. The step of verification depends on static signature images only. Although off-line signature verification is difficult to design still it is important for the person identification as a lot of the financial transactions in current period are done on paper. It is very difficult to authenticate a signature. It consists of five associated problems i.e. signature database, pre-processing, feature extraction, recognition and performance evolution. A lot of work has been done on signature verification and identification, but still there is a vacant space for improvement [4][5].

Signature verification states that signature sample is original or fake while on the other hand signature identification means that by whom the given signature sample is written. By means of training samples, information about writers can be obtained [6]. A signature forgery is divided into three different types. Every forgery requires a different verification process. The types of forgeries are random forgery, unskilled forgery and skilled forgery. Random forgery is the one in which the writer is unaware of the shape of original signature. While the simple forgery states that in this case the writer knows the shape of original signature but does not have enough practice. Skilled forgery is that in which the forger knows the shape of original signature and have enough practice to replicate the signature. All three types are illustrated in the given figure 1 [7].

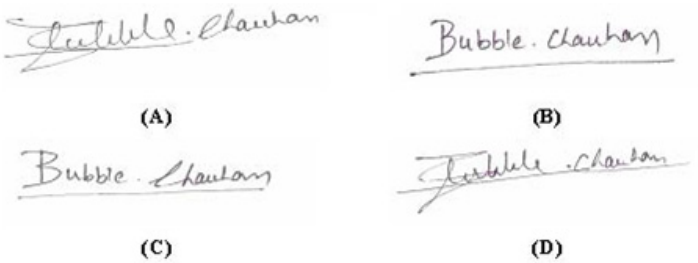


Fig. 1. Different types of forgeries

A) Original Signature B) Random Forgery
C) Simple Forgery D) Skilled Forgery

2 Related Work

For pattern recognition template matching is easiest and simplest method. For off-line signature verification DTW is the most common template matching technique. Many current methods still use this technique, though DTW is the simplest and oldest method to pattern recognition. Guo et al. [8] used this new approach for off-line

signature verification. In this method matching was done through DTW. FRR of nearly 6% and FAR of nearly 11.5% is achieved by considering only skilled forgeries. Fang et al. [9] proposed two new methods for the recognition of skilled forgeries. By using Fang's first method AERs of about 20.8% and 18.1% was achieved respectively, while Fang's 2nd method an AER of nearly 23.4% is achieved.

A Neural network is computing method that consists of a huge number of processors contained with many interconnections. A Neural Network model tries to use organizational values in a system of weighted directed graphs. It has artificial neurons and the directed edges having weights and are interconnected between neuron outputs and neuron inputs. Baltzakis et al. [10] describe a NN system for the recognition of random forgeries. FRR and FAR of nearly 3% and nearly 9.8% is obtained respectively. Quek et al. [11] used a novel method which is based on fuzzy NN for detection of skilled forgery detection. When original signatures and forgeries are used then average of the EERs is 22.4%. Mohammed A. Abdala et al. [12] describe a new approach in which the identification rate is 95.95%.

HMMs is statistical model used a sequence of interpretations and their association with each other. Edson J. R. Justino et.al [13] presents a new method i.e. HMM. The key aim of this method is to show a strong and fast system for off-line signature verification. El-Yacoubi et al. [14] present a new method that is based on the principle of cross-validation and HMMs for the recognition of random forgery. AERs of nearly 0.46% and nearly 91% are achieved for the relevant data sets. Justino et al. [15] illustrate a distinct observation based on HMM that is used to identify simple, random and skilled forgeries. A FRR of nearly 2.83% and FAR of nearly 1.44%, 2.50% and 22.67% is achieved for random, simple and skilled forgeries respectively.

Samit Biswas et al. [16] present a new method which is based clustering technique. This method helps the society whether a given signature is genuine or fake. The clustering technique relies on a k-NN's technique thus it enables to deal with different sizes & shapes clusters. The proposed method very reliable and verifies the signature with higher accuracy. If the training set is large the run-time performance of k-NN is much reduced.

3 Proposed Method

The proposed method is reliable, robust and secure. Primarily the proposed authentication system will be used for verification and identification in medium level security analysis. Proposed methodology for the automated offline signature identification and verification system consists of signature database, preprocessing, feature extraction and recognition.

In this paper, we have used techniques based on Delaunay triangulation for signature identification and verification. First of all preprocessing of signature is performed which will be illustrated below in detail. The block diagram for the proposed algorithm is given as under:

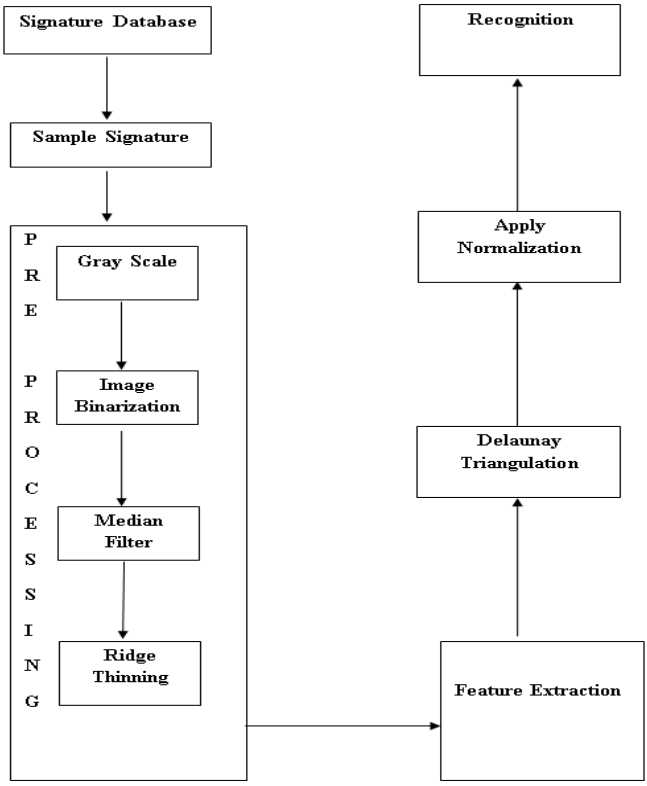


Fig. 2. Block diagram of the proposed Method

In this method we calculate the relative areas of the Delaunay triangles of different signatures. Then we will use Euclidean distance to compare the result of different signatures.

3.1 Preprocessing

First of all the preprocessing of signature samples are done. The preprocessing consists of following stages.

3.1.1 Convert the Image into Gray Scale

In preprocessing stage the signature image is first converted into gray scale. Color image have the combination of RGB colors but in our desired system we need gray scale image to give the best result. So the image is first converted into gray scale and the resulted image is as under.

Fig. 3. A) Original Image B) Gray Scale Image

3.1.2 Image Binarization

From gray scale we convert the image into binarised form to get the black and white pixel of the image. For image binarization Otsu's method [17] is used. In Otsu's method we systematically examine the threshold value that reduces the intra-class variance, which is defined as a weighted sum of the two class's variances.

$$\sigma_{\omega}^2(t) = \omega_1(t)\sigma_1^2(t) + \omega_2(t)\sigma_2^2(t) \tag{1}$$

Weights ω_i are the probabilities of two classes which are disjointed by a threshold t and σ_i^2 variances of these classes. Otsu method displays that by reducing the intra-class variance is the identical as maximizing inter-class variance.

$$\sigma_b^2(t) = \sigma^2 - \sigma_w^2(t) = \omega_1(t)\omega_2(t)[\mu_1(t) - \mu_2(t)]^2 \tag{2}$$

The class probabilities ω_i and class means μ_i are stated. The class probability $\omega_1(t)$ can be calculated from the histogram which is illustrated as t:

$$\omega_1(t) = \sum_0^t p(i)x(i) \tag{3}$$

The class mean $\mu_1(t)$ is as under:

$$\mu_1(t) = \sum_0^t p(i)x(i) \tag{4}$$

In this $x(i)$ is that value which is at the center of the ith histogram bin. The $\omega_2(t)$ and $\mu(t)$ can be computed on the right side of histogram for that bins which is larger than t. An effective algorithm can be obtained by using this method.

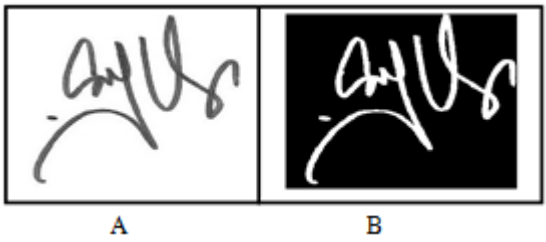


Fig. 4. A) Gray Scale Image B) Binarized Image

3.1.3 Median Filter

Then we apply the median filter to remove the noise so that to eradicate the pixels those are not the part of signature. The median filter is a kind of spatial filter in which the center value is replaced in the window. The mean filter kernel can be of any shape but it is frequently square. Figure shows the median filter application; in our case we used 3x3 median filter.

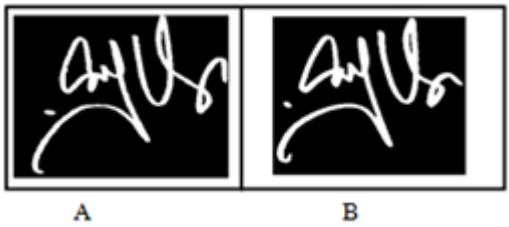


Fig. 5. A) Binarized Image B) Median Filter

3.1.4 Ridge Thinning

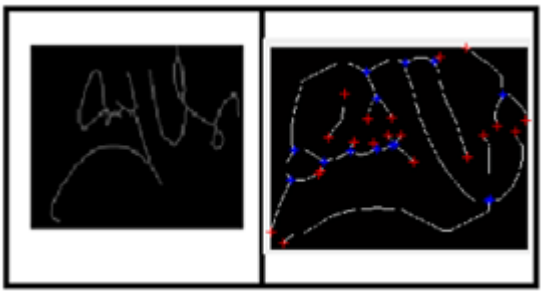
Ridge thinning and skeletonization of the signature is performed to get one pixel value of the signature. It eliminates pixels which are on the borders of objects but it does not break object apart. The remaining pixels make the skeleton of the image.

There are two sub-iterations of ridge thinning; one iteration is for the thinning algorithm. When someone identifies an unlimited number of iterations, then the iterations are repetitive till the image stops varying.

Fig. 6. A) Median Filter B) Ridge Thinning

4 Feature Extraction

In feature extraction phase the end points and intersection points are extracted so that we get the Delaunay triangle. End points are that which have only one neighbor while on the contrast intersection points have more neighbours. In figure below the red star shows the end point while blue point's shows intersection points of the signature.

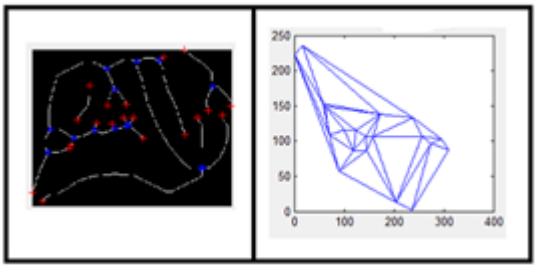


A B

Fig. 7. A) Ridge Thinning B) End points and Intersection points

5 Delaunay Triangulation

The 2-D Delaunay triangulation states that it contains a set of points in which the circumcircle contained no point for every triangle in the triangulation. To avoid the skinny triangles, the minimum angles of all the triangles are minimized by Delaunay triangulation. The Delaunay triangulation was named by Boris Delaunay in 1934 [18].



A B

Fig. 8. A) End points and Intersection points B) Delaunay Triangulation

6 Normalization

In normalization of the above Delaunay first area of Delaunay triangles is calculated by using Heron's formula as under.

$$s = \frac{a+b+c}{2} \tag{5}$$

$$A = \sqrt{s(s-a)(s-b)(s-c)} \tag{6}$$

And then the relative area of the Delaunay triangles is calculated by dividing the current area value by maximum area value.

The formula to find the relative area is given as under.

$$\rho_{rel(i)} = \frac{\rho_i}{\rho_{max}} \tag{7}$$

$$Where\ \rho_{max}\ is\ the\ maximum\ area\ value.$$

Then the relative area is sorted in proper order. We calculate total numbers of Delaunay triangles. Also we find the angles of each and every triangle. And then from all these values the feature vector is calculated for each signature.

7 Recognition

At last we find the Euclidian distance of signature. And then compare the result with other signatures in the database.

The length between p and q is the Euclidean and is represented by $\overline{pq}$. In coordinates $p = (p_1, p_2, \ldots p_n)$ and $q = (q_1, q_2, \ldots q_n)$ which are the two points in Euclidean distance space. The distance p and q is as under:

$$\begin{aligned} d(p,q) &= \|p - q\| \\ &= \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + \cdots + (p_n - q_n)^2} \\ &= \sqrt{\sum_{i=1}^{n} (p_i - q_i)^2} \end{aligned} \tag{8}$$

The genuine signature is accepted and the forged signature is rejected.

8 Experimental Results and Discussion

Our signature database consists of 420 signatures from 30 people. Among them 60 signature are simple forgeries while the other 60 signatures are skilled forgeries. We matched our algorithms with 60 feature points Scheme [19]. The accuracy of identifying genuine signature was 98%.

Our algorithm shows promising result. It accepts only genuine signatures and discards forged ones. The FAR and FRR is quite less in case of using our algorithm. The FAR and FRR is calculated by the following formula.

$$FAR = \frac{Number\ of\ forgeries\ accepted}{Number\ of\ forgeries\ tested} \times 100 \tag{9}$$

$$FRR = \frac{Number\ of\ original\ rejected}{Number\ of\ original\ tested} \times 100 \tag{10}$$

The proposed algorithm effectively rejected skilled forgeries and was ideal in rejecting simple forgeries. The method we used have less FAR and FRR as related to the FAR and FRR of other structural features [20].

Table 1. Comparative analysis of FAR

Types of Forgery	60 feature points Scheme[19]	12 feature points Scheme[19]	Proposed technique
Simple	0.98	9.75	**0.58**
Skilled	2.08	16.36	**1.66**

Table 2. Comparative analysis of FRR

False Rejection Rate (FRR)	
60 feature points Scheme[19]	20.83
12 feature points Scheme [19]	14.58
Proposed technique	**10**

9 Conclusion and Future Work

The main objective of this research is to identify genuine signature and to reject the forged ones. The role of offline signature verification and identification in the field of forensic application cannot be ignored and this method will be helpful to avoid fraud cases.

A new algorithm for offline signature verification and identification is presented in this paper. The proposed method shows promising results in the field of signature verification and identification. This method is reliable and it differentiates genuine from forged signature samples. End points and intersection points are easily extracted from which Delaunay triangulation is determined. The computational time of this method is quite less than other existing techniques. After Delaunay triangulation is constructed then area, relative area, total number of triangles and different angles of triangle is calculated. From that feature vectors are calculated for each signature and then by Euclidean distance formula the resultant values are matched. The FAR and FRR rate in this method is quite less than other techniques. It is matched with other techniques and its result is appreciating.

Delaunay triangulation is discussed in this paper and can also be used in the field of finger prints identification and face recognition. Two new approaches have been proposed but the enhancement should still be improved. It is an open research area. A few proposals for future work are being suggested. If we use correlation statistical approach in future work should get nearly the desired results. By using correlation technique the fraud in every field should be reduced.

References

[1] Radhika, K.R., Venkatesha And, M.K., Sekhar, G.N.: Pattern recognition techniques in off-line hand written signature verification - a survey. In: Proceedings of World Academy of Science, Engineering and Technology, vol. 36 (December 2008) Issn 2070-3740
[2] Guest, R.: Age dependency in handwritten dynamic signature verification systems. Pattern Recognition Letters 27, 1098–1104 (2006)
[3] Ooi, S.-Y., Toeh, A.B.-J., Ong, T.-S.: Offline verification through biometric strengthening. In: Workshop on Automatic Identification Advanced Technologies, pp. 226–231 (June 2007)
[4] Chen, S., Srihari, S.: A new off-line signature verification method based on graph matching. In: Proc. IEEE 18th Int. Conf. on pattern Recognition, vol. 2, pp. 869–872 (2006)
[5] Rabasse, C., Guest, R.M., Fairhurst, M.C.: A Method for tHE Synthesis of Dynamic Biometric Signature Data. In: Proc. 9th International Conference on Document Analysis and Recognition, vol. 1, pp. 168–172 (2007)
[6] Sharma, A., Parekh, P., Bhatia, U.S.: Forensic Signature Verification. In: International Conference on Frontiers in Handwriting Recognition, ICFHR (November 2010)
[7] Majhi, B., Santhosh Reddy, Y., Prasanna Babu, D.: Novel Features for Off-line Signature Verification. International Journal of Computers, Communications & Control 1(1), 17–24 (2006)
[8] Guo, J.K., Doermann, D., Rosenfeld, A.: Forgery detection by local correspondence. International Journal of Pattern Recognition and Artificial Intelligence 15(4), 579–641 (2001)
[9] Fang, B., Wang, Y.Y., Leung, C.H., Tse, K.W.: Off-Line Signature Verification by the Analysis of cursive strokes. International Journal of Pattern Recognition and Artificial Intelligence 15(4), 659–673 (2001)
[10] Baltzakis, H., Papamarkos, N.: A New Signature Verification Technique based on a Two-Stage Neural Network Classifier. Engineering Applications of Artificial Intelligence 14, 95–103 (2001)
[11] Quek, C., Zhou, R.W.: Antiforgery: a novel pseudo product based fuzzy neural network driven signature verification system. Pattern Recognition Letters 23, 1795–1816 (2002)
[12] Abdala&, M.A., Yousif, N.A.: Offline Signature Recognition and Verification Based on Artificial Neural Network. Eng & Tech. Journal 27(7), 20
[13] Justino, E.J.R., Bortolozzi, F., Sabourin, R.: Off-line Signature Verification Using HMM for Random, Simple and Skilled Forgeries. In: Sixth International Conference on Document Analysis and Recognition (September 2001)
[14] El Yacoubi, A., Justino, E.J.R., Sabourin, R., Bortolozzi, F.: Off-Line Signature Verification Using HMMs and Cross-Validation. In: IEEE International Workshop on Neural Networks for Signal Processing, pp. 859–868 (2000)
[15] Justino, E.J.R., Bortolozzi, F., Sabourin, R.: Off-Line Signature Verification Using HMM for Random, Simple and Skilled Forgeries. In: International Conference on Document Analysis and Recognition (ICDAR 2001), Seattle, USA, vol. 1, pp. 105–110 (2001)
[16] Biswas, S., Kim, T.-H., Bhattacharyya, D.: Features Extraction and Verification of Signature Image using Clustering Technique. International Journal of Smart Home 4(3) (July 2010)

[17] Sezgin, M., Sankur, B.: Survey over image thresholding techniques and quantitative performance evaluation. Journal of Electronic Imaging 13(1), 146–165 (2004), doi:10.1117/1.1631315
[18] Delaunay, B.: Sur la sphère vide, Izvestia Akademii Nauk SSSR. Otdelenie Matematicheskikh i Estestvennykh Nauk 7, 793–800 (1934)
[19] Jena, D., Majhi, B., Panigrahy, S.K., Jena, S.K.: Improved Offline Signature Verification Scheme Using Feature Point Extraction Method. IEEE Xplore (October 18, 2008)
[20] Zafar, S., Qureshi, R.J.: Off-line signature verification using structural features. In: Proceedings of the 7th International Conference on Frontiers of Information Technology, p. 72 (2009)