ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(20), DOI: 10.17485/ijst/2015/v8i20/77735, August 2015* ISSN (Online) : 0974-5645

The Analysis of Online and Offline Signature Verification Techniques to Counter Forgery

Akondi Vyasa Bharadwaja*

SENSE, VIT University - 600127, Tamil Nadu, India;
akondi.vyasa2013@vit.ac.in

Abstract

Background: This paper reports precise examination of a few highlight extraction-based procedures for signature check. Dynamic features of Signature are captured for online verification procedure at the time of signing. Offline frameworks deal with the examined picture of a signature. A shot at the Offline Verification of signatures utilizing an arrangement of shape based geometric highlights has been taken. Pattern Slant Angle, Normalized Area, Height, Aspect Ratio, Width, area of signature pixels are the utilized features. Captured image should be Pre-processed to separate the signature part and remove the white noise, before extracting the features. **Methods**: The framework is at first prepared utilizing a database of signatures acquired from those people whose signatures must be confirmed by the framework. A mean signature is acquired coordinating the above features got from an authenticate test signatures. **Findings**: The claimed test signature is compared with the mean signature for the purpose of verification. Euclidian distance in the feature space between the claimed signature and the template serves as a measure of similarity between the two. On the off chance that this separation is not as much as a predefined edge (relating to least adequate level of likeness), the test signature is checked to be that of the guaranteed subject else distinguished as a phony.

Keywords: Dynamic Features, Offline Signature, Online Signature, Pre-processing, Signature, Static Features, Verification

1. Introduction

Signature Verification is the methodology of perceiving an individual's transcribed marks. Signatures have been by a long shot the most mainstream means for distinguishing the genuineness of people. Signature confirmation offers a brisk, basic and expense successful means for accepting the legitimacy of an archive by deciding the distinction between a unique mark and a fake one. The two most generally utilized methodologies for the confirmation of the marks are static and dynamic. Changing or Online Verification investigates the behavioural biometric of the manually written mark while it is being composed with the point of checking its credibility, therefore securing the character of the client. The client's vicinity is essential for the ongoing check of his/her marks. Static or Offline check hinders the need of client's vicinity as it thinks about the different qualities of a pre-recorded mark picture on request to achieve a sought conclusion.

Unconventional written work styles and different variables, for example, mental state, sickness, age and so on make the procedure of disconnected from the net mark confirmation more entangled. Then again, Online Signature Verification can helpfully use various parameters connected with the stylus and electronic composition cushion for deciding the validness of the mark. These parameters incorporate pace, height, width of the signature, number of pen ups and pen downs, distance of the signature and so forth. These properties make the signature unique and nearly impossible to forge.

The kind of verification technique online can likewise differ contingent upon the kind of use. For banks and other financial establishments, online signature check is not possible. At the point when checks and different reports touch base for freedom at the banks' end, disconnected from the net check gets to be obligatory, as the client is definitely not present at the time. This obliges a database of marks to be give to the banks. Check

* *Author for correspondence*

extortion recognition is one of the biggest difficulties confronting organizations and monetary establishments today. I.T sector adds to most of the misfortunes endured by the bank. False checks are so troublesome it couldn't be possible to distinguish for gifted frauds. Then again, with the vicinity of a disconnected from the net strategy for verification, this can be significantly diminished. In this way, of the two systems, Offline Signature Verification is more famous and broadly acknowledged owning to its low expenses and pertinence.

Different methodologies have been proposed for offline sign verification check[2-4]. However, the vast majority of these methodologies give great exactness for causal forgery. Dynamic signature confirmation framework is the point, at which a signature is composed onto an intelligent electronic gadget, for example, a tablet also, is perused on the web, and contrasted with the marks on document of the individual to check for realness. Numerous critical highlights are used with online signatures that are not available for the offline ones. As compared to offline signature verification online verification is obviously more robust this was discussed in many algorithms[5,6]. So, by this practical approach, both the online and offline signature verification systems to counter forgery are discussed here. By which we conclude the robustness of the dynamic verification is more robust when compared to the static system.

The system should not be either too sensitive or too coarse. There should be an appropriate trade-off between low False Acceptance Rate (FAR) and low False Rejection Rate (FRR). The quality performance measures which are used are FRR and FAR. The ratio of unaccepted genuine test signatures to the trained total genuine test signatures is called FRR. The ratio of accepted forgeries to the total submitted forgeries is called FRR. When manually chosen threshold is altered in order to increase the FAR, the FRR will invariably decrease and vice versa.

2. Approach

The issue is approached in two stages. At first an arrangement of marks are acquired from the subject and fed to the framework. These marks are pre-processed then the pre-processed pictures are utilized to concentrate pertinent geometric parameters that can recognize marks of distinctive persons. These are utilized to prepare the framework. The mean estimation of these highlights is gotten. In the following step the checked mark picture to be confirmed is fed to the database. It is pre-processed to be suitable for extraction of features. It is sustained to the framework and different features are extracted from them. These qualities are then contrasted and the mean features that were utilized to prepare the framework. The Euclidian distance is figured and a suitable edge every client is picked. Contingent upon whether the information mark fulfils the limit condition the framework either acknowledges or rejects the mark. In the off line signature verification use the photo copies of the images for training where as in the dynamic system use the live environment by connecting the tablet to the system take the inputs. Only the features that are extracted from the static environment is done by the stylus and the pad and the remaining algorithm remains almost the same. Since the velocity and time and so on cannot be observed from the still image.

Section III includes pre-processing steps, Section IV discusses about the extracted features and Section V deals with verification procedure. Section VI lists the details of implementation and simulation results. Section VII gives the conclusion of the work. Figure 1 shows the flow chart which illustrates the steps followed in the proposed work.

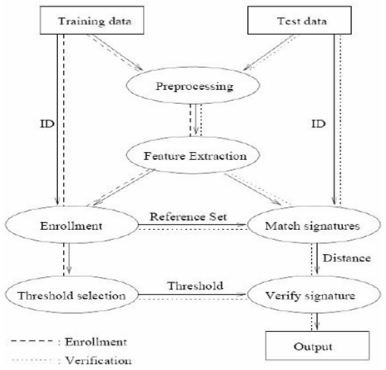

Figure 1. Flowchart for the proposed methodology.

For an online signature verification system, input is dynamic. This input is normally captured through a digital tablet. This input is digitized and fed for processing. First of all pre-processing is done on the input received and then some features are extracted from the captured online data on the basis of which the signature is validated. The process of reading the real time inputs of the signatures from the pen tablet and stylus into the CPU to process and store in the signature database is called Data acquisition.

Processing and storage is done further by the real time inputs send to the CPU by the pen tablet. In the online signature approach the intake of the signature and data acquisition are shown directly as training data in the Figure1

Digitizing tablet is used for obtaining signature. Figure 2 shows the pen/digitizing tablet. This tablet lets us to gather distinctive part of penmanship contrasted and pen-and-paper penmanship. Instead of 2-D picture on paper, measure a direction stream from which infer an estimate of the typical 2-D picture.

Figure 2. Digitizing tablet.

3. Pre-processing

This stage includes following five steps:

- Resizing.
- RGB to Grey conversion.
- Rotating the image.
- Thinning.
- Cropping.

3.1 Resizing

The loaded signature image may be of some arbitrary size. So all the images are resized to a certain size so that any two signature images can be compared irrespective of their initial sizes.

3.2 RGB to Grey Conversion

The loaded signature image may be colour image. As cannot process colour image, convert it to grey image.

3.3 Rotating the Image

The image is rotated so that the image rests on the base line of the image. This is done by calculating the inclination of the signature first and then rotating the image by that much amount.

3.4 Thinning

The goal of thinning is to eliminate the thickness differences of pen by making the image one pixel thick. Thinning is mainly done because not all the signatures are done by using a pen of same thickness.

3.5 Cropping

As don't need the entire image, we crop a boundary across the signature. Now the image contains only the area in which signature is present.

Automatic global thresholding is used to extract binary image from the gray image. Global threshold can be calculated automatically with the following algorithm[6].

- Threshold T is the primary value selected in such a way that it lies midway between the extremes of the gray level values.
- Threshold T is used for segmenting the image.
- Calculate the mean gray level values μ1 and μ2 for both groups of pixels.
- Calculate new threshold depending upon the step 3

$$T = \frac{(\mu 1 + \mu 2)}{2}$$

1. In successive iterations, repeat steps 2 to 4 until the difference in T is lesser than 0.5.

4. Feature Extraction

These are the features for offline signature verification

- Height of the signature.
- Width of the signature.
- Area of signature pixels.
- Normalized area.
- Signature height-to-width ratio (Aspect ratio).
- Slant Angle.
- Total number of pixels in the signature.

4.1 Height of the Signature (H)

The normal signature height when its base line is normalized to ground.

4.2 Width of the Signature (W)

The normal signature width when its base line is normalized to ground.

4.3 Area of the Signature Pixels

It is the number of pixels which belong to the signature. This feature provides information about the signature density. It is denoted by K

4.4 Normalized Area

Ratio of signature pixels area to the bounding box area is called Normalized area.

4.5 Signature Width to Height Ratio (Aspect Ratio)

It is obtained by dividing signature width to signature height. Signature height and width can change. Width-to-height ratios of one person's signatures are approximately equal.

4.6 Slant Angle

Signature is imagined to be resting on a fictional line called Base line. The inclination angle between base line and the horizontal line is called Slant angle.

4.7 Number of Pixels in the Signature (N_p)

The total number of "ON" pixels present in the signature.

The above are the features for offline signature verification system. Which are static in nature since they are obtained from the stationary image? Now the dynamic or the online signature methodology needs the dynamic features. Which are as listed below?

4.8 Online Features

- Signing time.
- Signature width.
- Signature height.
- Number of pen-ups.
- Number of pen-downs.
- Total signature length.
- Velocity of pen or stylus.

4.8.1 Signature Time

It is the time required for a user to complete the total sign.

4.8.2 Signature Width

It is the shortest distance between the both extremes along the horizontal axis.

4.8.3 Signature Height

It is the shortest distance between the both extremes along the vertical axis.

4.8.4 Number of Pen-Ups

It is the number of times the pen is lifted up from the surface of contact during the period of signature.

4.8.5 Number of Pen-Downs

It is the number of times the pen is placed on the surface of contact during the period of signature.

4.8.6 Total Signature Length

It is the total distance of the signature measured when we convert that curve into a single line.

4.8.7 Velocity of the Pen or Stylus

It is the velocity with which a writer keeps his sign on the tablet.

5. Verification

The above depicted highlights are removed from an example gathering of mark pictures of diverse persons. The features obtained from every specimen gathering are utilized as a part of determining a mean signature for every subject. The mean qualities and standard deviations of all the features are processed and utilized for last check. A client characterized limit relating to the base satisfactory level of likeness for every individual was physically assessed. Since clients don't give priority for their unique signatures to get rejected, we picked the edge on the lower side to dodge dismissal of unique marks.

Let μ_i denote the mean and σ_i denote standard deviation for the i^{th} feature and F_i denote its query image value. The Euclidian distance δ in the feature space measures the proximity of a query signature image to the mean signature image of the claimed person. This is how the distance is calculated.

$$\delta = \frac{1}{n}\sum_{i=1}^{n}\left([\mathrm{Fi} - \mu i]/\sigma i\right)^2$$

The signature is said to be verified when this Euclidian distance has a value less than the global threshold.

6. Implementation Details and Simulation

6.1 Results

Figure 3 shows the results of pre-processed signature which has images of loaded, resized, thinned, rotated and cropped signature.

Features Extracted (Mean Values of the Genuine Candidate)
Theta=37.58deg;
Area of signature pixels (delta)=331776;
Height=3.2;
Length=6.2;
Normalized area=0.0803;
Aspect ratio=1.93;
Number of pixels=15680;

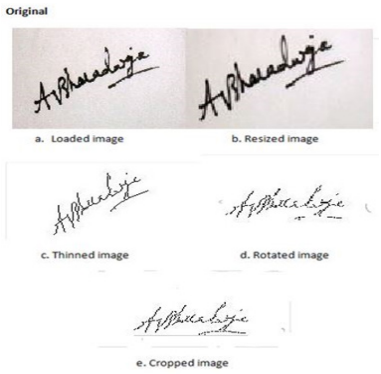

Figure 3. Pre-processing step output images.

6.2 Results for Offline Signature Verification

Figure 4 – Figure 10 represents the features extracted after pre-processed on the Y-axis where as on the X-axis have taken the samples from few users. The first sample is the mean value of the features extracted from 30 different signatures from the genuine user.

Features Extracted After Data Acquisition (Mean Values) from the Online Signature Verification System
Height=4.626.
Width=6.465.
Time=4.310sec.
No of pen up's=0.
No of pen down's=1.
Distance of signature=1568.1 pixels.
Velocity=363.82pixels /sec.

6.3 Results for Online Signature Verification

Figure 11 – Figure 17 represents the features extracted after pre-processed on the Y-axis where as on the X-axis have taken the samples from few users. The first sample is the mean value of the features extracted from 30 different signatures from the genuine user.

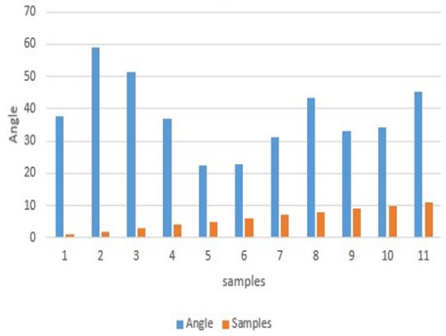

Figure 4. Signing angles calculated for different users vs samples.

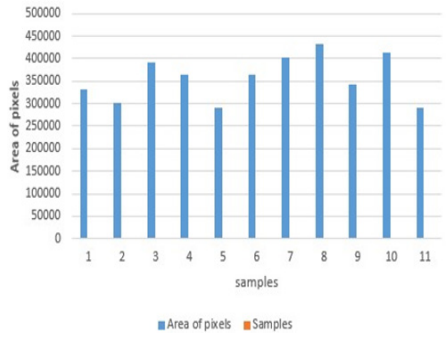

Figure 5. Area of pixels vs samples.

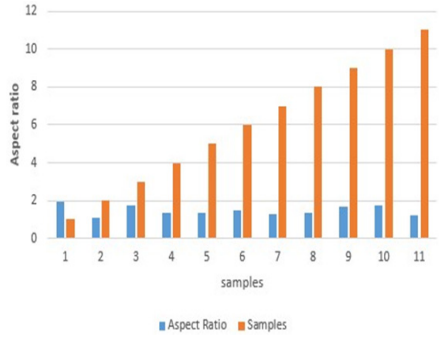

Figure 6. Aspect ratio calculated for different users.

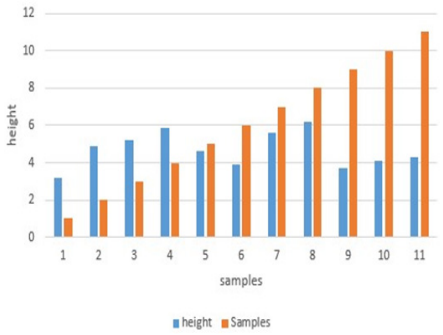

Figure 7. Signature height calculated for different users.

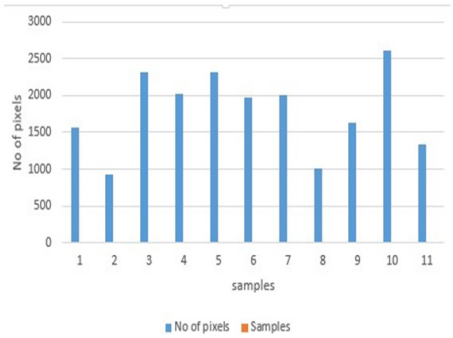

Figure 8. No. of pixels calculated for different users.

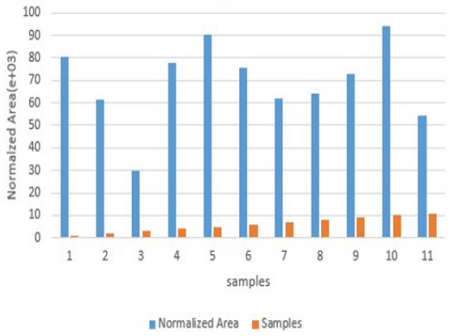

Figure 9. Normalized area calculated for different users.

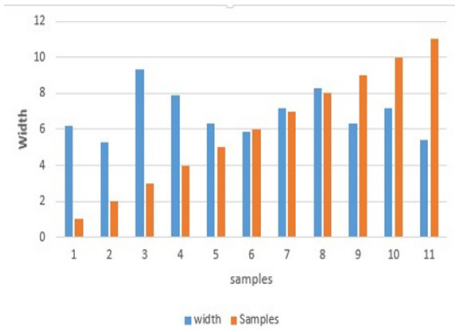

Figure 10. Signature width calculated for different users. users.

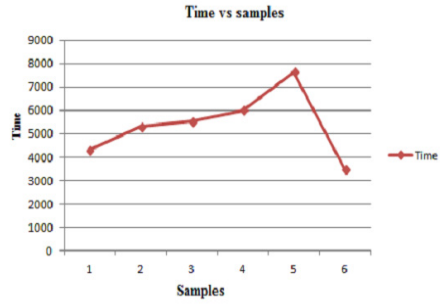

Figure 11. Samples vs. time (in ms.).

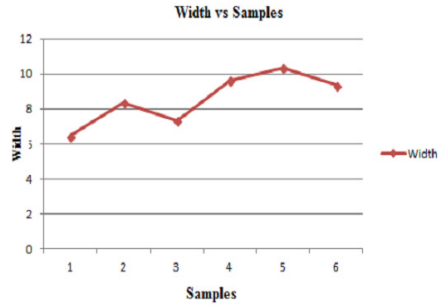

Figure 12. Width vs samples.

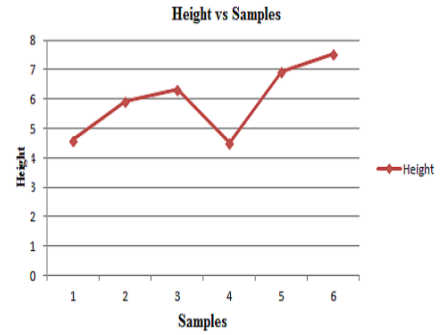

Figure 13. Height vs samples.

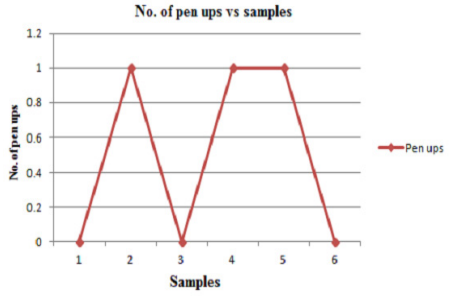

Figure 14. Pen ups vs samples.

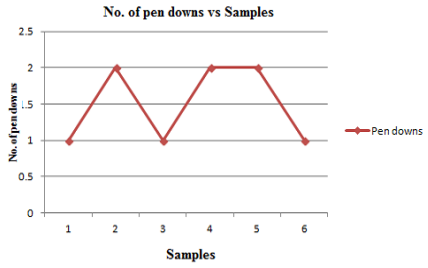

Figure 15. Pen downs vs samples.

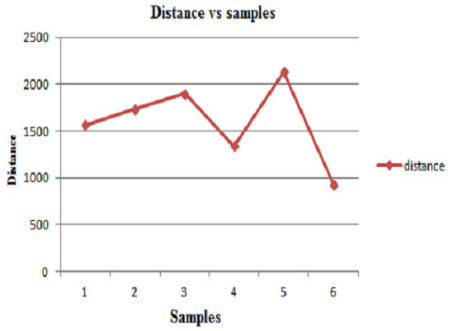

Figure 16. Distance vs samples.

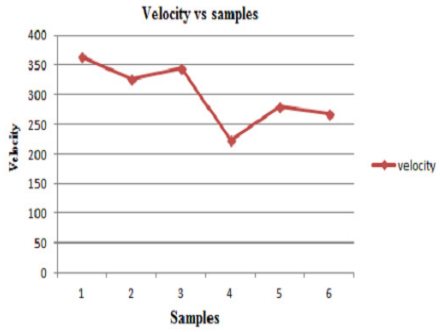

Figure 17. Velocity Vs samples.

Table 1. FAR and FRR for offline signature verification

Nature of the signature	Number of samples	False acceptance ratio	False rejection ratio
Original	30	---	10%
Forgery	35	11.4%	---

Table 2. FRR and FAR for online signature verification

Nature of the signature	Number of samples	False acceptance ratio	False rejection Ratio
Original	30	---	6.66
Forgery	35	8.57	---

30 original signatures and 35 forged signatures both for off-line and online signature verification systems. Out of 30 original signatures 3 are rejected and out of 35 forged signatures 4 were accepted as genuine. This is for offline, where as for online 2 were rejected from the original data base and 3 were accepted from the false samples or forged signatures. The results of our simulation for forged and genuine signatures are as shown in the tabular forms 1 and 2.

7. Conclusion

This paper has displayed a far reaching and precise examination of a few highlight extraction-based procedures for signature check. The significance of single person highlights and edge values for every individual has been illustrated. Presumably the most critical result is the high accuracy rate for on-line check, demonstrating the capability of this methodology for genuine applications. It is additionally beneficial to note that new clients can be consolidated effortlessly through the programmed preparing capacities of the classifier. A positive amazement is the high rate got for off-line acknowledgment. Once more, this can be considered as vital reasonable result, since disconnected from the net acknowledgment is less demanding to acknowledge and needs less sensitive equipment.

8. References

1. Qi Y, Hunt BR. Signature verification using global and grid features. Pattern Recognition. 1994 Dec; 27(12):1621–29.
2. Ibrahim SIA. Offline Signature Verification Using Graph Matching. Turk J Elec Engin. 2007; 15(1):89–104.
3. Chen S, Srihari S. A new offline signature verification method based on graph matching. 18th International Conference on Pattern Recognition; Hong Kong. 2006; 2:869–72.
4. Chandra L, Puja L, Gupta R, Tayal A, Ganotra D. Improved adaptive binarization technique for document image analysis. Proceedings of the Second International Conference on Computer Vision Theory and Applications (VISAPP); 2007. 2007 Mar 8-11; Barcelona, Spain. 1. p. 317–21.
5. Jain AK, Pankanti S, Bolle R, Editors. Biometrics: personal identification in networked society. Lower Dordrecht; 1999.
6. Baltzakis H, Papamarkos N. A new signature verification technique based on a two-stage neural network classifier. Engineering Application of AI. 2001 Feb; 14(1):95–103.
7. Christofides N. Graph theory: An algorithmic approach. New York, Academic Press Inc.;1977.