Secure Signature Verification using Image Processing

J.Vinothkumar , *Assistant Professor,*

Department of Electronics & Communication, scsvmv University, Enathur

Abstract

The signature verification system using image processing is a technique where researchers are eagerly concentrating. The problem in the signature verification system is non availability of data for testing. Security using signature has to be developed with high accuracy. Here we studied the algorithms available in the market. For signature verification, we proposed a new method of signature verification using suitable algorithm. Our proposed system achieves 90% of accuracy.

Keywords— *Signature; Security; Skeleton; Pixel.*

I. INTRODUCTION

Security of data and information is a major issue where biometrics is playing increasingly important role in identification and authentication. Several technologies that have been developed in this area are based on physiological (fingerprint, face, iris) and behavioral traits (signatures, voices) etc. This study concerns with the handwritten signatures which are considered as behavioral trait. [1]A signature is a uniquely designed pattern to an individual and virtually impossible to duplicate. A signature is processed to obtain a test data which can be compared and tested for being authentic. The primary advantage of signature verification technology over other technologies is that signatures are already accepted as a common method of identity verification.

Signature verification problem can be accessed based on two approaches, dynamic and static. [2]Dynamic method is also known as 'on-line'. It uses digitizing tablets and stylus-operated PDAs which are connected with computer system to extract dynamic information like pressure, velocity, speed of writing etc. Static or 'off-line' method uses pen and paper; users write their signature on paper, digitize it through an optical scanner or a camera. The signature recognition system extracts features from the scanned image for verification. The features extracted from a scanned image basically include pixel images. Here, we deal with an offline signature verification technique. [3]Signatures are composed of special characters, therefore most of the time they can be unreadable. Also, Interpersonal variations and interpersonal differences make it necessary to analyze them as a complete image and not as letters and words put together. As the study proceeds further various image processing techniques are applied to the obtained images which are then verified using pattern matching algorithms. [4]The algorithms specified here are Pixel Based Method (i), Harris Algorithm Based (ii), Surf Algorithm Based.

II. RESEARCH ATTEMPTS

The signature verification system requires signature database which is obtained by collecting signatures of 100 people using offline method, images are stored as JPEG file type. [5] All signature sheets are manually cropped using a photo editor to separate them as an individual images. Thus a wide variety of signatures are obtained for preprocessing.

2.1 Pre-Processing

The preprocessing is applied to all the images. The purpose is to make the signature standard and ready for feature extraction. It improves the quality of image and makes is suitable for feature extraction. The preprocessing stage includes

2.1.1 Converting image to gray

The collected images are rgb images which are converted to greyscale.

2.1.2 Converting image to binary

A greyscale image is converted to binary to make the features simpler.

2.1.3 Thinning

Thinning makes the extracted features invariant to image characteristics like quality of pen and paper. Thinning means reducing binary objects or shapes to strokes that are single pixel wide.

2.1.4 Bounding box of the signature

In the signature image, construct a rectangle encompassing the signature. This reduces the area of the signature to be used for further processing and saves time.

2.2 Feature Extraction

The choice of powerful set of features is very crucial in verification systems. Here, the features extracted are based on the following algorithms.

Pixel based Method

A binary image contains only two values for each pixels .Typically, the two colors used for the binary images are black and white. For a given image the values of black pixels and white pixels can be obtained.

After preprocessing, the image obtained is a standard image of 100 x 200(pixels). The algorithm is defined to calculate the number of black pixels present in the image. To precede with the verification an mxn grid is formed over the image.

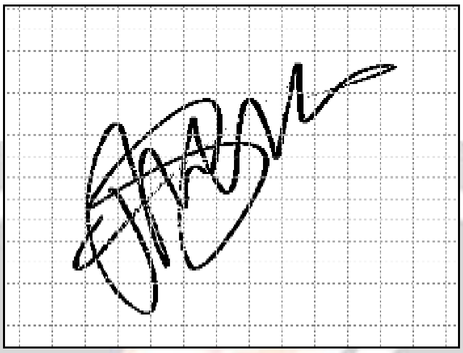

Figure 1. Skeleton signature

Here, a grid of 10x20 is formed which gives 200 individual cells over the image. Such divisions are made to for creativeness of the features extracted.

Next we find out the cells which contain the black pixels hence those cells are only acknowledged which contain more than 3 black pixels.[6] The procedure is continued to determine the cells containing the black pixels.

We compute the amount of black pixels in the cells. The count of black pixels is evaluated for all images present in the database. For the verification of the images these counts are matched the user input. If the count is lies in the stored values than it gives an output of verified images.

The rate of acceptance for pixel based method is low since the possibility of gaining equal amount of pixels for a signature a two different instant is low. So, we proceed with next method which involves the corner points of the signature.

Harris Algorithm Based

Harris algorithm based method deals with calculating the corner points for the signature. Every signature has unique corner points based on different individual. The corners define a separate feature which can be used as a method to authenticate a signature.

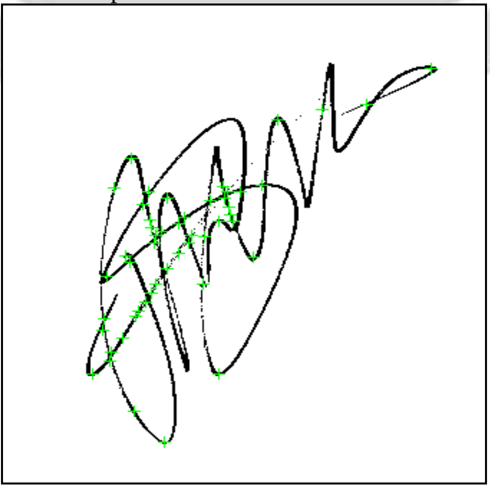

Figure 2. Corner points using Harris algorithm.

A corner is defined as the intersection of two edges or as apoint for which the there are two dominant and different edge directions in a local neighborhood of the point. Harris algorithm defines those points.
Steps

1. After the image preprocessing the Harris algorithm is applied. It gives the dominant points of the signature.
2. These are points of local intensity maximum or minimum, line endings, or a point on a curve where the curvature is locally maximal. Once, the corners are displayed we calculate the amount of corner points and their value.
3. Above steps are repeated for the user input and different set of corner values are obtained.
4. Corner values of the user input are compared with the previously obtained data. If the values match each other, than the signature is verified.

For this method a threshold of 70% gives a well-defined acceptance rate. But this does not gives the accuracy of the system, thus to get more accurate results next method is defined.

PROPOSED METHOD

Surf Based Algorithm

This algorithm is used to calculate the interest points in a signature. These points are the most dominant points in the image thus can be extracted as a feature for verification.

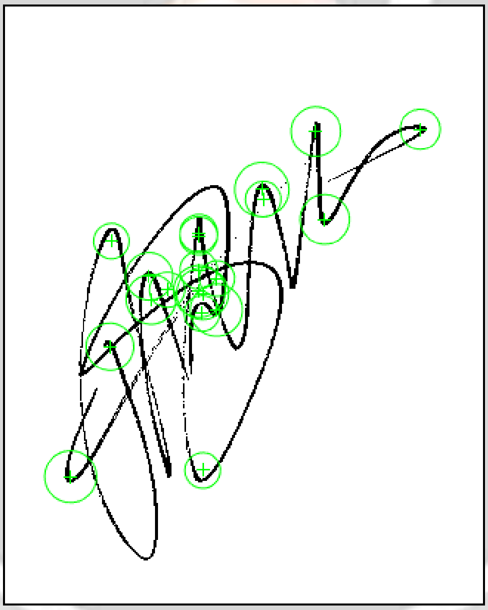

Figure 3. Surf Features

In this method the surf features are detected using surf algorithm i.e., computation of index points in a signature. The Points are based on the geometry and slope of the image. This algorithm can also include detection of corners based on Harris algorithm to increase the accuracy of the authentication.
Surf uses a blob detector based on Hessian matrix. The determinant of the matrix is used to measure the local change around the point and the points are chosen where the determinant is maximal. After applying the surf detection code the index points are displayed and calculated. The comparison of these points for different images provides the criteria for the signature verification. This method is more accurate than the previous mentioned as it includes Harris points as well.

Based on the methods mentioned above the best results were obtained for the Surf Based Algorithm method thus, it is preferred. A threshold is set for the signatures to be accepted as genuine thus for which false acceptance rate (FAR) and false rejection rate (FRR) defined.
FAR (False Acceptance Rate): The false acknowledgement proportion is given by the amount of fake marks acknowledged by the framework as for the aggregate number of examinations made and is given by:

FAR=$No.of\ Forgeries\ accepted\ /No.of\ Forgeries\ tested$

FRR (False Rejection Rate): FRR (False Rejection Rate): The false rejection rate is the aggregate number of real signature dismissed by the framework concerning the aggregate number of correlations made and is given by:

$$\text{FRR}=No.of\ Forgeries\ rejected/\ No.of\ Forgeries\ tested$$

Experiment Results

The proposed method is carried out via offline signature verification system which uses Surf Algorithm Based method for accurate results. The method showed signs of improved FRR.

Table 1

Threshold	FAR (%)	FRR (%)
90	5.2	32
80	9.3	16
70	17	4.1
60	29	0
Average	14.3	10.9

According the results obtained the surf algorithm gives a 90% success rate when the threshold is high.

3. Conclusion

The study presents methods of offline signature recognition techniques using pattern recognition. The methods mentioned in this paper use features extracted from the preprocessed signature images. The extracted features are used to recognize similar patterns between two signature images. All Three mentioned method use pattern recognition as base. The first method uses pixel values to recognize the image as genuine; here the chance of getting best pixel values is less thus gives an accurate value at a threshold of 60% which does not satisfy the required results. To improve the accuracy of acceptance of the signature image we move to next method Harris Algorithm method which uses corner points as the feature to be extracted. This method gives a desired result at a threshold of 75%, but still not precise. We introduce Surf Algorithm which uses index points for feature extraction along with the Harris Algorithm. This method provides desired result with a threshold of 90% which is more accurate than the previous methods. This study aims at reducing the cases of forgery in business transactions.

REFERENCES

[1] S.Sibi Chakkaravarthy, Sajeevan G, Varun Kumar.K.A, Automatic Leaf Vein Feature Extraction for First Degree Veins, Volume 425 of the series Advances in Intelligent systems. pp 581-592.

[2] Correa, E., Green, W., Jaramillo, C., Jaen, M.C.R., Salvador, C., Siabatto, D., Wright, J.: Protocol for leaf image acquisition and analysis, version2,May13,2014.www.ctfs.si.edu/data/documents/LeafScan_WAGreen_draft.pdf

[3] Ehsanirad, A.: Plant Classification Based on Leaf Recognition. International Journal of Computer Science and Information Security 8(4), 78–81 (2010)

[4] Fu, H., Chi, Z.: A two-stage approach for leaf vein extraction. In: IEEE Int. Conf. Neural Networks & Signal Processing, China, December 14–17 (2003)

[5] Fu, H., Chi, Z.: Combined Thresholding and neural network approach for vein structure extraction from leaf images. IEEE Proc.-Vis. Image .

[6] 1. Ma Mingming,W.Sardha Wijesoma,Eric Sung, "An Automatic On-line Signature Verification System Based on Three Models", in Proc. Canadian Conf on Electrical and Computer Engineering, vol 2,pp 890-894,May2000 .

[7] Vu Nguyen, Michael Blumenstein, Vallipuram Muthukkumarasamy ,Graham Leedham, “Off-line signature verification using enhanced modified direction features in conjunction with neural classifiers and support vector machines”, in Proc. Int Conf of Pattern Recognition , vol 4 , pp. 509 – 512 , 2006.

[8] Hand written signature verification methods K R Radhika, M K Venkatesha and G N Sekhar rkr.ise@bmsce.ac.in, principal_rnsit@yahoo.com.

IJARIIE