International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 5, May - 2014

Feature Extraction for Signature Verification Using Hilditch Algorithm

Ravikumar B Panchal[1]
Dept. of Electronics and communication
Darshan Institute of Engineering & Technology
Rajkot, India

Dr. Dhaval R Bhojani[2]
Dept. of Electronics and communication
Darshan Institute of Engineering & Technology
Rajkot, India

***Abstract*— In today's market Signature verification system is one of the most widely used biometrics for authentication purpose in banking sector as well as E-government sector. The development of such kind of system is necessary with the fact that the signature is widely used as personal verification. So Verification can be performed either Offline basis or Online basis. Online systems are having dynamic information in which signatures are taken by pressure tablet. Offline systems are having static information in which signatures are taken by scanner or camera. The present paper is done in the field of offline signature identify by extracting some special domain features. Here special domain features includes high intensity variation based features as well as loop based features. In this paper existing signature verification systems have been thoroughly studied and a model is designed to develop an offline signature Verification system. Main aim is to take various feature points of a given signature and compares them with the test signatures feature points by graph matching classifier. The final result gives execution time, threshold values, no of region made as well as standard deviation of selected signatures. The paper discusses the different stages of the process including: Signature preprocessing, feature extraction and verification by graph matching classifier.**

Keywords— ***Signature Verification, Database creation, Preprocessing, Feature extraction, verification and Authentication***

I. INTRODUCTION

Biometrics can be broadly classified as physiological and behavioural. Handwritten signature is a behavioural kind of biometric. It is first biometrics to be used before the arrival of PCs and laptops. Handwritten signature has long been used in the financial domain as well as in banking sectors for identity verification. In most of the case the verification process is done manually either by a person who is familiar to the signature database or by comparison process against a few signature templates. Signature verification is a system capable of strongly addressing two individual tasks as identification of the signature owners and taking decisions whether the signature is genuine or forge.

Signature verification system can be categorized in two major classes: on-line verification and offline verification. On–line verification requires a pointer and an electronic tablet which is connected to a PC that collects dynamic signature information. These dynamic characteristics are specific to each individual and sufficiently stable as well as repetitive. Online signature scheme identifies motion of the pen while doing signatures. These signatures can be verified based on various parameters like pen pressure, writing speed. These kinds of features are special and cannot be forged easily.

While in offline scheme, signatures are nothing but 2D images which are generated by scanning it or captured it from cameras. Off-line signature process is complex task due to the absence of dynamic geometry of signatures. Difficulty also comes in the fact that due to different modern and unconventional writing styles, it is harder to segment signature strokes. The nature as well as the different pattern of pen may also affect the nature of the signature obtained. Sometimes signatures of genuine person cannot do proper way due to illness, mood, and age relaxation or emotional behaviour. As a result large intra-personal as well as interpersonal variations are generating. An intelligent system has to be designed which should not only be able to consider these factors but also detect various types of forgeries within less amount of time. The system should neither be too sensitive nor too coarse. It should have an acceptable trade-off between a low false acceptance ratio as well as low false rejection ratio. The designed system should also find such kind of feature points that reduces less amount of storage as well as less amount of computational time [2].

II. TYPES OF FORGERY

The basic types of forgery include [1]:

A. Random forgery

Random forgery is done by a person who doesn't know the shape and structure of the original signature. Fig.1 (b).

B. Simple Forgery

In this type of forgery the person concerned has a vague idea of the actual signature, but is signing without any more practicing. Fig.1 (d).

C. Skilled Forgery

This type of forgery considers appropriate knowledge about the original signature along with sample time for proper practice. Our proposed scheme eliminates random and simple forgeries and also reduces skilled forgery to a great extentFig.1(c).

Fig.1 (a) Original Signature

Fig.1 (b) random Forgery

Fig.1(c) Simple Forgery

Fig.1 (d) Skilled Forgery

III. RELATED WORK

Lot of research has been done on online as well as offline signature verification system. As the extraction schemes change, performance can be improved. As a result system becomes more robust as well as accurate.

A novel feature extraction scheme has been suggested for offline signature verification [1]. This method used the concept of feature extraction with help of identifying geometric centre as well as Euclidean distance of different signatures. The performance of classifier used here is faster as well better for feature extraction. Results that are achieved by this method are better than all existing methods. The process of Threshold selection is done with help of standard deviation and average.

Another method for off-line signature identification and verification is proposed based on the description of the signature envelope and the interior stroke distribution in polar and Cartesian coordinates [2]. In this paper, a new geometrical feature for an offline signature verification system (ASV) is used. The proposed features can be calculated with a fixed-point microprocessor. Therefore, the features can be extracted from inside a personal device such as a smart card. The system is check out with various classifiers like SVM, HMM and EDC for identifying forgeries.

The Improved Offline Signature Verification Scheme Using Feature Point Extraction Method [3] is proposed for reducing FAR compare to different proposed methods. The scheme is based on selection of 60 feature points from the COG of the signature and compares them with trained feature points. The classification of the feature points depends on mean and variance. A smaller change of a signature results in a large change in the values of threshold distance from the COG. Therefore in this algorithm the value of FRR is increased.

The generation of a digital skeleton is often one of the first processing steps taken by a computer vision system when attempting to extract features from an object in an image. Various algorithms have been proposed to produce the skeleton of a digital binary pattern. The Hilditch thinning algorithm [4] is widely used as a useful method of preprocessing in image process is proposed for speeding real-time process. Hilditch proposed an algorithm to obtain the skeleton of one object in an image. There are two versions for this algorithm, one using 4×4 mask and the other one using 3×3 mask. With a 3×3 mask image, the result of process output can be saved to a memory “table”. The output results of all different 3×3 masks are saved to this “table” at the beginning of starting application. When an image will be processed, the thinning results of every 3×3 masks in the image can be extracted by the method of “looking for table”. Thus the thinning result is same but the process speed is high.

A method based on multi-feature and multi-stage verification is proposed in paper [5] for Chinese signature. This paper carries out a two level of verification to make decision. In the first stage input sign is compare with help of directive features and If result comes forge one then remaining execution will stop. But if it authorizes sign then the second stage verification will perform and the decision of the second stage is taken as the final decision.

There is another way to authenticate genuine signature by using Cross-validated Graph Matching algorithm [6]. In this paper, .here the high intensity was find out using normalized box near signatures. The signatures are compared by developing a bipartite graph from which a minimum cost complete matching is obtained and the measure of mismatch i.e., the Euclidean distance is determined.

The idea of finding the location variations of the strokes of signature geometry for signature verification is proposed and tested [7]. Two methods are proposed. The first method helps in determine the positional variation of the projection profiles of the signature, while the second method helps in finding out the actual positional variations of individual strokes in the 2-D signature patterns. In both methods, the statistics on these variations are computed. Here posional variations are finding out by applying various signatures as a input. The genuineness of the input is determined by judging the state of the training sets. The decision process involves the computation of a distance measure which takes the positional variations and the correlation between them into account.

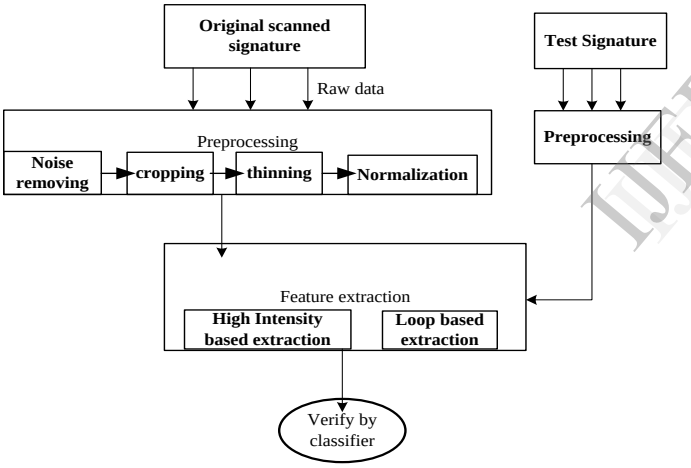
Another method for off-line Persian signature identification and verification is proposed that is based on Image Registration, Discrete Wavelet Transform and Image Fusion [8]. Training signatures of each person are registered to overcome scaling and shifting problems.To extract features in first step DWT is used to find details of signature. In next step several registered signs of each person is merged together to generate reference sign of person's signatures. In the verification stage Euclidean distance between the test image and each pattern is used in different bands. Experimental results confirmed the accuracy of the proposed method.

The method for identifying genuineness of bank cheque signatures is proposed [9]. It describes how signature is identifies in cheques using various verification algorithm. Here proposed algorithm can be used for an effective signature verification system in the banking industry. The proposed methodology verifies a cheque by recognizing and analyzing the major details in a cheque, which includes the account holder's signature. The results show the FAR and FRR in the verification process and the success ratio.

In [11] the author presented new approach for signature predefine area was preprocessed. He used new auto cropping preparation on the basis of the image view, where the intensity value of pixel is the parameter of cropping. This approach provides both the chances of improving the performance of security systems based on signature images, and also the chances to use only the region of interest of the used image to suit layout design of biometric systems.

IV. PROPOSED SYSYTEM ARCHITECTURE

In order to design a system, which will detect the forge signatures by comparing some special features with original one, the following architecture has been proposed.



The design process can be categorized into four main parts:

A. *Database Creation*

Here we have taken total 100 signatures from total 10 faculty members of my college DIET. Here each faculty member has to sign their own total 5 genuine signature. This all signatures are stored in database. Each 10 signature includes 3 genuine signature and 2-training signature. While rest 5-signature is used for test signatures. Here all test signatures are done by us for find out forgery among all. Table 1 represents the information regarding to whole database.

B. *Preprocessing*

The principal objective of preprocessing is to obtain a transformed image with enhanced quality. It includes Noise removal, cropping, Thinning and Normalization.

TABLE I. DATABASE OVERVIEW

Sr no	Notification	No of signatures			Total
		Genuine	*Training*	*Test*	
1	KKG	3	2	5	10
2	DA	3	2	5	10
3	DP	3	2	5	10
4	DDV	3	2	5	10
5	DRB	3	2	5	10
6	MNP	3	2	5	10
7	MRK	3	2	5	10
8	NH	3	2	5	10
9	RJK	3	2	5	10
10	NR	3	2	5	10

1) Noise removing

Due to lack of accuracy in scanning process of signatures creates noise in the images. This is due to dust or alignment problems of scanners lens. So a filter is needed which removes such kind of noises and make signature smooth enough. It is required to eliminate single white pixels on black background and single black pixels on white back ground. When we scan signature from paper then some unwanted pixels comes with the scanned image that is not a part of the signature. So this unwanted part must be removed before feature extraction.

2) Cropping

Cropping process removing unnecessary white back ground from the image. So as result it reduces the size of signature. The resultant signature only includes the main framework of the signature.

3) Hilditch thinning

Thinning is a morphological process necessary for the reduction of data and execution time. To reduce all objects in an image to lines, without changing the whole structure of the image, use the bwmorph function. Here we are using Hilditch thinning algorithm for it. Here 3*3 masks are used for fast response. For accurate thinning process one must follows the processing steps which are predefined.

C. *Feature extraction*

Each person's signature has different style. When someone tries to copy other's signatures then they basically try to maintain the shape. But some important features can make a signature difficult to be copied. Now this features are analyzed and are used in this proposed method to differentiate genuine from forge one. Here we use high intensity variation and cross over points as a feature extraction.

1) High intensity variation

Person usually does signatures with reference to fix angle. While doing signature person follow same kind of writing technique. So as result different intensity is generated the entire signature. Use of ball point as well as ink pan also create large different in intensity. This feature can be extracted easily to compare genuine and test signatures. Figure.2 and figure.3 represents the examples which includes high intensity variation points shown by arrow in it.

Fig.2

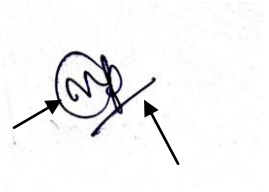


Fig.3

2) Cross Over loop

Each user has some monopoly in doing signature. Here each and every time shape of some special letter is always remaining constant. So as result it creates same cross over points. This point is very helpful for identify authors own signature among all. Figure 4 and figure 5 represents example of which includes cross over points shown by arrow in it.

Fig.4

Fig.5

D. *Classification/verification*

Here extracted features are used for identify if the signature is genuine or forge. So for that classifier is very helpful.here we are using graph matching method for classification. Here hungerian algorithm is used for giving the 2 dimensional matrix which includes max deviation and total amount of thresholds of all signatures. Now from that signatures are comparing and final output represents whether signature is accept or reject.the final output also gives total amount of time required for algorithm execution.

V. ALGORITH FOE PROPOSED SCHEME

Step 1: Hand written signature is scanned.
Step 2: Signature is preprocessed and converted into binary or gray scale as per requirement, removing noise from signatures, thinned signature and finally normalize the signature.

Step 3: Special domain feature as high intensity variation points and cross over points are extracted from genuine as well as test signature.

Step 4: Compared features with help of graph matching method as a classifier.

VI. IMPLEMENTATION AND RESULTS

A. *Noise remove*

Here in our work the signatures that we have scanned include paper and shot noise. We applied a noise removal technique, which basically based on the size of pixel. In this algorithm some pixels, which are not connected with rest of the signature and have less than 8 pixel values are considered as noise and removed using MATLAB (R2012a). We choose 3 reference signatures named as MNP, MRK and RJK. The output of each signature is shown below from figure 6 to figure 11

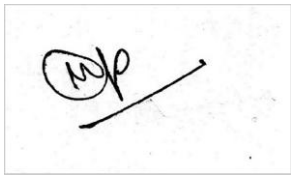


Fig.6 Noisy Signature _MNP

Fig.7 Removing noise_MNP

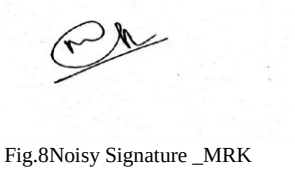


Fig.8Noisy Signature _MRK

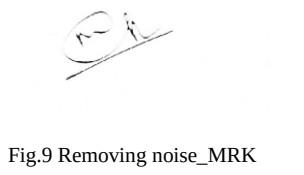


Fig.9 Removing noise_MRK

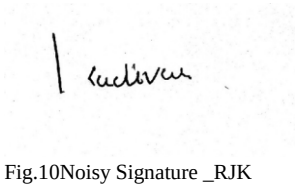


Fig.10Noisy Signature _RJK

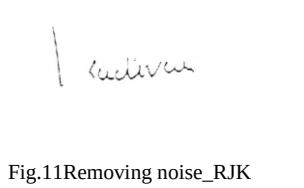


Fig.11Removing noise_RJK

B. *Cropping*

Cropping process removing unnecessary white back ground from the image. So as result it reduces the size of signature. The resultant signature only includes the main

framework of the signature. Figure represents thinning outputs as below from figure 12 to figure 14.

Fig.12 Cropping_MNP

Fig.13Cropping_MRK

Fig.14 Cropping_RJK

C. *Thinning*

To reduce all objects in an image to lines, we are using Hilditch thinning algorithm. Here for fast response we choose 3*3 masking. Figure 15 to figure 17 shows the resultant thinning output of reference signatures obtained by database respectively.

Fig.15 Thinning_MNP

Fig.16 Thinnning_MRK

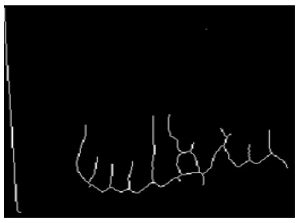


Fig.17 Thinning_RJK

D. *Feature Extraction*

After getting the preprocessed signature it is then come to find the forgery using feature extraction. Here we find out it with help of high intensity variation points and cross over loops from signatures. These features could be difficult to copy for a fake person. Figure represents high intensity variation points by blue colored "+" sign and cross over points are represented by "red circled" sign.

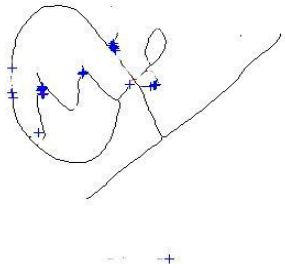


Fig.18 Extracted Features_MNP

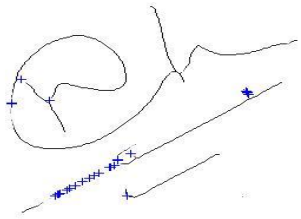


Fig.19 Extracted Features_MRK

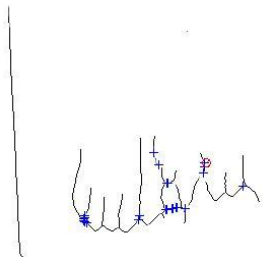


Fig.20 Extracted Features_RJK

VI. CLASSIFICATION RESULTS

A classification result gives the brief view of execution time, threshold value, no of region made as well as standard deviation for all MNP, MRK and RJK signatures. The values are represented in bellowed table.

TABLE.II RESULTS

Idendity	Threshold point	Standard deviation	Execution Time(S)	Region Made
MNP	90	1000	10.86	36
MRK	90	800	6.49	41
RJK	77	800	38.67	43

VII. CONCLUSION

The proposed signature identification system is based on some special features extraction which includes high intensity variations and loop based features. It uses a compact and efficient storage of feature points, which reduces memory overflow and results in faster comparisons of the data to be verified. Here in this paper we identify the genuineness of the signatures using such kind of features. Here verification of these signatures are mainly depends on threshold points as well as standard deviations. This parameters are compared by graph matching method. This technique can be added with any existing verification system for better result. The result gives either signature is accept or reject. The execution time as well as identification process of our system is better among other class of offline signature verification system.

REFERENCES

[1] Banshidhar Majhi, Y Santhosh Reddy, D Prasanna Babu, "Novel Features for Off-line Signature Verification" International Journal of Computers, Communications & Control, pp. 17-24, 2006.

[2] Migual A. Ferrer, Jesus B. Alonso and Carlos M. Travieso, "Off-line Geometric Parameters for Automatic Signature Verification Using Fixed-Point Arithmetic", IEEE Tran. On Pattern Analysis and Machine Intelligence, vol.27, no.6, June 2005.R. Chen et al., "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks," IEEE Commun. Mag.,pp. 50–55, Apr. 2008.

[3] Ming Yin, Seinosuke Narita, "Speedup Method for Real-Time Thinning Algorithm" DICTA2002: Digital Image Computing Techniques and Applications, Melbourne, Australia, 21--22 January 2002Y.-C. Liang et al., "Sensing-Throughput Trade-off for Cognitive Radio Networks, "IEEE Trans. Wireless Commun., pp. 1326–37 ,April 2008.

[4] Yingna Deng, Hong Zhu, Shu Li, and Tao Wang, "Signature Verification Method Based on the Combination of Shape and Dynamic Feature", Department of Automation and Information Engineering, Xi'an University of Technology, 710048 Xi'an China, 2005.

[5] Ramachandra, A. C. Pavithra, K. and Yashasvini, K. and Raja, K. B. and Venugopal, K. R. and Patnaik, L. M., "Cross-validation for graph matching based Offline Signature Verification", In: INDICON 2008, India, pp: 17-22,2008.

[6] Fang, B., et al, "Off-line signature verification by the tracking of feature and stroke positions", Pattern Recognition, pp. 91-101, 2003.

[7] Samaneh Ghandali, Mohsen Ebrahimi Moghaddam, "Off-Line Persian Signature Identification and Verification Based on Image Registration and Fusion", Journal of Multimedia, June 2009.

[8] M.Jasmin Pemeena, Priya darsini ,K.Murugesan, Srinivasa Rao Inbathini, A.Jabeena, and K.Sai Tej "Bank Cheque Authentication using Signature" ,International Journal of Advanced Research in Computer Science and Software Engineering , May 2013.

[9] Raman Maini & Himanshu Aggarwal, "Study and Comparison of Various Image Edge Detection Techniques", International Journal of Image Processing (IJIP), 2010.

[10] Bassam Al-Mahadeen, Mokhled S. AlTarawneh and Islam H. AlTarawneh "Signature Region of Interest using Auto cropping" IJCSI International Journal of Computer Science Issues, March 2010.

[11] Ravi J, Sundernag Hosamani and K B Raja "Off-line Signature Identification Based on DWT and Spatial Domain Features" IEEE-20180

[12] Guangyu Zhu, Yefeng Zheng,David Doermann, Stefan Jaeger, "Signature Detection and Matching for Document Image Retrieval", IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, NOVEMBER 2009.