Offline signature using Cross validation and Graph matching approach

Dipali K. Bhole[1], A. V.Vidhate[2] and Shrikant Velankar[3]

[1,3] *Vidyalankar Institute of Technology, Wadala, Numbai, India*
Email: dipali.bhole4@ gmail.com
shrikant.velankar@vit.edu.in
[2] *Department of Computer Engimeering at Ramrao Adik Institute of Technology, Navi Mumbai, India*
Email: {vidhate@rait.ac.in}

***Abstract*— Compared to physiologically Base biometric system such as fingerprint, face, palm-vein and retina, behavioral based system such as signature, voice, gait etc. are less popular and many are still in infancy. Signature verification is used for banking transactions. In this paper, we discussed Graph matching based approach for signature verification and cross-validation for same. Database signature is preprocessed in which signature extraction method is used to obtain high resolution for smaller normalization box. In Graph based approach the dissimilarity between two signatures are determined by finding minimum Euclidean distance by Hungarian method. In Cross-validation technique the authenticate the test signature. It is observed that this method gives remarkable reduction in Equal Error Rate (EER).**

***Index Terms*— Signature verification, offline signature, online signature, Image Processing, image Cropping. skeletonization , Image rotation**

I. INTRODUCTION

SIGNATURE has been a distinguishing feature for person identification through ages. Even today an increasing number of transactions, especially financial, are being authorized via signatures, hence methods of automatic signature verification must be developed if authenticity is to be verified on a regular basis. Approaches to signature verification fall into two categories according to the acquisition of the data: On-line and Off-line. On-line data records the motion of the stylus while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time. Online systems use this information captured during acquisition.

These dynamic characteristics are specific to each individual and sufficiently stable as well as repetitive. Off-line data is a 2-D image of the signature. Processing Off-line is complex due to the absence of stable dynamic characteristics. 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 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 idea is to perform the signature generating procedure in two phased. The first phase is performed off-line, before the message to be signed is known and the second phase is performed on-line, after the message to be signed is known. On-line/off-line signature is particularly useful in smart card application. The off-line phase is implemented either during the card manufacturing process or as a background computation whenever the card is connected to power, and the on-line phase uses the result of the off-line phase to sign actual messages.

The objective of signature verification is to discriminate between two classes: original and forgery, which are related to intra and interpersonal variability. The variation among signature of same person is called Intra personal Variation The variation between originals and forgeries is called Inter Personal Variation.

Signature verification is so different with the character recognition, because signature is often unreadable, and it seems it is just an image with some particular curves that represent the writing style of the person. Signature is just a special case of handwriting and often is just a symbol. So it is wisdom and necessary to just deal with a signature as a complete image with special distribution of pixels and representing a particular writing style and not as a collection of letters and words. The verification system must be able to detect forgeries and at the same time reduce rejection of genuine signatures

The two different types of forgeries considered for a signature verification system are: 1)Random forgeries 2) Skilled forgeries. The problem of signature verification becomes more difficult for skilled forgeries when compared to random forgeries.

A. Online Signature Verification System:

Signatures are captured dynamically using graphic tablet and are stored as a function of time. It avails spatial and temporal characteristics of signature such as speed, stroke-acceleration, pen-location and pen pressure. Online signatures are more unique and difficult to forge since dynamic features are available along with the static features. Different approaches for online signature verification are Artificial Neural Networks (ANN), Dynamic Time Warping (DTW), Hidden Markov Model (HMM) and Gaussian Mixture Model (GMM).

B. Offline Signature Verification System

In offline systems, signature is digitized using flatbed scanner and then stored as an image. It extracts static features, which are of three types: (i) *Global features:* provide information about specific cases of the signature shape such as signature area, signature height-to-width ratio, maximum horizontal and vertical histogram, horizontal and vertical center of the signature, horizontal and vertical local maxima numbers of the signature and number of edge point of the signature. (ii) *Mask features:* provide information about direction of the signature stroke i.e., skew angle of the signature. (iii) *Grid features:* are used for finding densities of signature parts. The various approaches for offline signature verification are based on neural networks, parallel processing, 2-D transform, histograms of directional data or curvature, horizontal and vertical projections of the writing trace of the signature, local geometric information, shape of the signature, the position of feature points located on the skeleton of signature and global shape descriptors. In evaluating the performance of the signature verification system, there are two important factors: the False Rejection Rate *(FRR)* of genuine signatures and the False Acceptance Rate *(FAR)* of forgery signatures.

II. RELATED WORK

Sharifah [1] proposed effect of number of Training samples on HMM based online signature verification. In offline, the signature form used during the online data collection was scanned into the PC. The scanning technique used is based on [2]. The image was scanned in 600 dpi resolution, grayscale type and stored using TIFF (Tag Image File Format) in order to preserve the information details. The scanned image is then preprocessed in order to remove unnecessary noise. A feature extraction process is then done onto the preprocessed image and use the feature as the observation sequence in building the HMM. At the end, the verification process is done based on the probability score given by the HMM.

Ya Qiao [3] proposed method for offline verification using Online Handwriting Registration. This method developed new criteria which combines the duration and amplitude variance of handwriting.

Xiaofeng [4] proposed efficient generic on-line/off-line signature without key exposure .In this method they introduced a special double –trapdoor hash family based on discrete logarithm assumption to incorporate to construct more generic offline/online signature scheme without key exposure.

Asma shakil [5] presented effect of different features, performance on Hidden Markov Modeling based on Online and offline signature verification system. For offline signature verification pixel density, center of gravity, distance and angle are considered

III. PROPOSED WORK

Model gives preprocessed operations that are involved in signature feature extraction which is discussed below in detail. Algorithm for Cross-validation of Graph matching is as follows:

1. Collect sample signatures
2. Preprocess the sample signatures.
3. Find out the reference signature from these sample signature.
4. Add reference signature in to final database.
5. Take the test signature that has to check whether genuine or forge.
6. Preprocess this test signature.
7. Extract the feature of test signature.
8. Compare extracted feature with reference signature value.
9. If value>= threshold value(this value set by programmer) then signature accepted else rejected as forge

In this algorithm we used Euclidian distance between two signatures . Using this Euclidian distances we can easily find out the reference signature. Here using this algorithm we are adding reference signatures in final database so minimizing number of comparisons

1. *Signature database :* The signature samples are Digitized using graphic tablet. This database also consist of skilled forgeries of genuine signature. The principal objective of preprocessing is to obtain a transformed image withenhanced quality. It includes –

--Convert to gray scale

-- Noise removal,

-- Edge detection

-- Skeletonization

-- Rotation,

-- Signature extraction and

-- Normalization

i. Convert to gray scale image : Here we converts RGB images to grayscale by eliminating the hue and saturation information while retaining the luminance[10].

ii. Noise removal is required to eliminate the pixels that are not part of the signature, but contained in the image. Generally signature image consists of salt and pepper noise, which is removed using median filter.

iii. Edge detection : Edge detection is used for feature extraction which aim at identifying points in a signature at which the signature brightness changes sharply or, more formally, has discontinuities. We used Canny Edge detector for edge detection This process detects outlines of an object and boundaries between objects and the background in the image

iv. Skeletonization : Skeletonization is a transformation of a component of a digital image into a subset of the original component.

v. Rotation of a signature is necessary as time domain approaches are sensitive to angle

vi. Signature Extraction *:* Extract the smallest box that covers the signature so that the extra background created due to rotation is removed. The smallest box is determined by the height and width of the signature and is then cropped to the measured dimension[7]. The allowance for little background is given in all directions so that the signatures do not touch the boundary of the box. Signature extraction increases the probability of occurrence of foreground signature when compared to background space i.e., high resolution of signature for smaller normalization box and hence reduces error rate.

Fig 1.Original image

Fig 2. Noise free Image

Fig 3. Image Edge Detection

Fig 4. Image after rotation

vii. Normalization Normalization is required to standardize the size of signatures having interpersonal and intrapersonal differences[8].

2. *Selection of Reference Signatures :* The signature of an individual varies with time and mood, which results in a problem of selecting reference signatures from the set of available genuine signature samples

IV. RESULT AND DISCUSSION

The Cross Validation principle decides the validity of the genuine signature to be in the reference set by comparing it with other genuine signatures.

Decision factor of S1

(DF_1) =Mean(DV_1)/SD(DV_1)

(DFm) =Mean(DV3)/SD(DV_3)

The average of all decision factors is determined as given in an Equation (4)

$$DF_{avg} = DE_1 + DF_2 + ... + DF_m$$

The signature having Decision factor value nearer to DF_{avg} selected as reference signature. This reference signature is used for comparison with any input signature

The extracted feature of test signature *d* is compared with the threshold value *Dth* • If *d* is less than or equal to *Dth* , then the test signature is accepted as genuine else it is rejected as forgery[9].

1. Genuine test: Genuine signatures are verified against reference signatures to compute False Rejection Rate *FRR*. Out of available 24 genuine signatures of one person, 1 is selected as reference and remaining 23 are used for testing. Therefore, the total number of test signatures equals 23 * 5 = 115. total number of test signatures.

2. Skilled forgery test: Skilled forgeries are verified against reference signatures to compute False Acceptance Rate *FAR-S.* All the 30 skilled forgeries of a person are tested yielding a total of 30 * 5 = 150 test signatures.

For verification the normalization box size are varied.

To achieve logical results, the signatures must have the same size, which means normalized one[6], in our approach the reference sizes are [125 270].

These tests are performed using different sizes of normalization box:105*190,100(250,125*270,150*300. For every specific normalization box decision threshold value is varied

Table 1: EER of skilled forgeries of CGMOSV

Normalization Box	CGMOSV
100*190	26.33
105*250	29.0
125*270	27.33
150*300	24.0

V. CONCLUSION

In this paper, we analyzed CGMOSV algorithm in which the signatures are compared using Graph matching and the Euclidean distance is considered as the dissimilarity measure between them. The Cross-validation principle is used in the selection of reference set of signatures. The pre-processing of signature is carried out with signature extraction to reduce Equal Error Rate *EER.* It is observed by selecting reference signature number of comparisons are reduced compared to existing algorithm.

REFERENCES

[1] Sharifah Mumtaz Syed,Asma Shakil ,Study on Effect of number of training Samples on HMM Based Offline and Online Signature Verification System, 2008 IEEE

[2] Sharifah Mumtazah Syed Ahmad, Asma Shakil,,Mustafa Agil Muhamad Balbed, "Offline Signature Verification System using Hidden Markov Model in MATLAB Environment", *7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science* (ACACOS 2008), Hangzhou, China, April, 2008

[3] Y. Qiao, 1. Liu and X. Tang, "Offline Signature Verification using Online Handwriting Registration," *Association for Computing Machinery, Inc. CVPR,* pp. 1-8, June 2007

[4] Xiaofeng chen,fangguo zhang,Haibo Tian , Efficient generic on-line/off-line signature without key exposure,information science 178 (2008)4192-4203

[5] Asma Shakil,Sharifah mumtazah Syed Ahmad , Digital Image Computing Techniques and application ,2008,IEEE

[6] Bassam Al-Mahadeen, Signature Region of Interest using Auto cropping, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 2, No 4, March 2010

[7] Debasish Jena, Improved Offline Signature Verification Scheme Using Feature Point Extraction Method, Proc. 7th IEEE Int. Conf. on Cognitive Informatics-2008

[8] Yu Qiao,Offline Signature Verification Using Online Handwriting Registration, 2007 IEEE

[9] Madasu Hanmandlu,,Off-line signature verification and forgery detection using fuzzy modeling Pattern Recognition 38 (2005) 341 – 356,2004

[10] Javed Ahmed Mahar,Off-Line Signature Verifi'cation of Bank Cheque Having Different,Background Colors,2007 IEEEE