

Offline Signature Verification System Using Energy on Grid Level

Hetal V. Davda¹, Sima K. Gonsai²

¹ Student, Dept. of Communication System Engineering, L.D.College of Engineering, Ahmedabad, Gujarat, India

² Asst. Professor, Dept. of Communication System Engineering, L.D.College of Engineering, Ahmedabad, Gujarat, India

¹ hetal_davda@yahoo.in, ² simagonsai@gmail.com

Abstract: *Signature is a behavioral biometric. One's signature may change over time and it is not nearly as unique or difficult to forge as iris patterns or fingerprints, however signature's widespread acceptance by the public, make it more suitable for certain lower-security authentication needs. Signature verification is split into two according to the available data in the input, Off-line and On-line. In this work we present offline signature verification system. Offline signature verification is difficult to design as many desirable characteristic such as order of strokes, the velocity and other dynamic information are not available in the offline. Although difficult to design, offline signature verification is crucial for determining the writer identification. In this proposed method we evaluate energy of signature on grid level as features. For this we have taken 5 genuine signatures for training and extract their features and stored as training features. Now for each writer we have taken 5 testing genuine signature and extracted their energy features and this features are compared with stored training feature of each writer using different distance metrics and we have find the best distances for energy features.*

Key Words: Energy Features, FAR, FRR, Threshold

I. Introduction

Signature is behavioural type biometrics characteristics of human and Signature has been a distinguishing feature for person identification. Even today an increasing number of transactions, especially related to financial and business are being authorized via signatures. Hence the need to have methods of automatic signature verification must be developed if authenticity is to be verified and guaranteed successfully on a regular basis. Approaches to signature verification fall into two categories according to the acquisition of the data: On-line and Off-line.

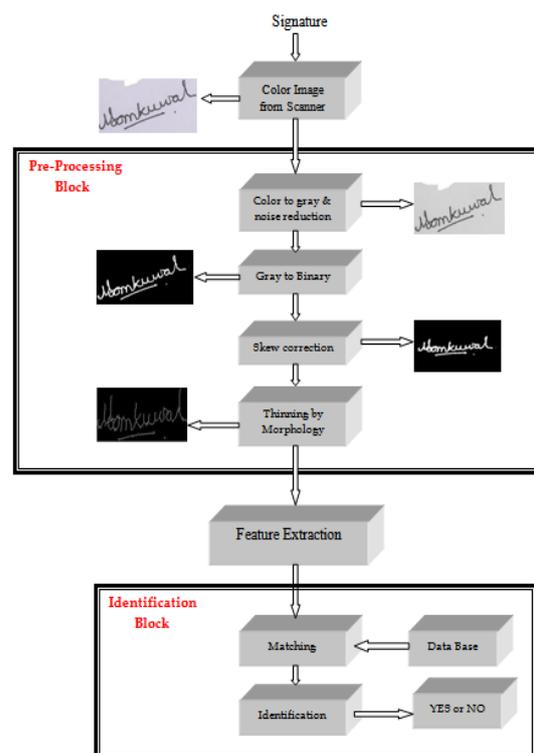
On-line data records the motion of the stylus while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure as functions of time. Online systems use this information captured during acquisition. These dynamic characteristics are specific to each individual 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 nature and the variety of the writing pen may also affect the nature of the signature

obtained. 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 designed system should also find an optimal storage and comparison solution for the extracted feature points.

II. General System Architecture

The system consists of three major modules: Image pre-processing module, feature extraction module and Identification module. The detailed system block diagram is shown in the Figure 1.



1 system architecture

Figure

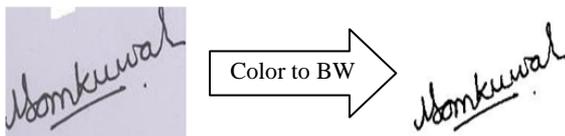
First, the signatures were collected in an A4 sheets and scanned those sheets. Signatures in the sheets were cropped and separated, and then the pre-processing module employs image processing algorithms to demarcate the region of interest from an input image. This module performs three major tasks, skew detection and correction, noise removal and thinning the input image. Next, the feature extraction module extracts the features from signature image. Finally, identification module employs a distance classifier which verify the signature by comparing the feature vector with the enrolled data in the database.

Pre-Processing Module

The pre-processing module includes 6 steps. These steps are described as follows.

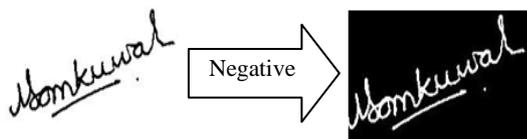
Step 1: Conversion from RGB to black and white image

For signature verification, form of the two signatures must be compared. Hence all the scanned images were converted to black and white images where white is represented by 1 and black is represented by 0. Hence the signature part of the image were represented by 0 and blank parts of the image (without any signature) by 1. This conversion also makes future coding easier.



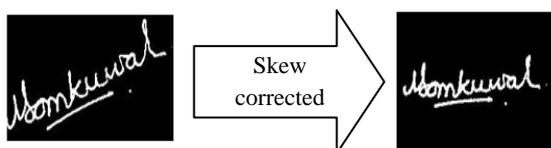
Step 2: Inverting the image

This conversion can be easily done by using the inbuilt inversion function (\sim) of MATLAB. Now, the signature part becomes coded by 1 while blank spaces are coded by 0. This makes logical comparisons a lot easier.



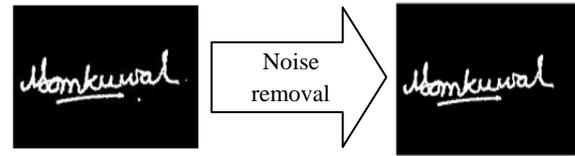
Step 3: Skew detection and correction

Skew detection and correction is a necessary pre-processing step in signature verification system in any language. In this step, Hough transform is used to detect the Skew of signatures and affine transform is used to correct the skewed signatures.



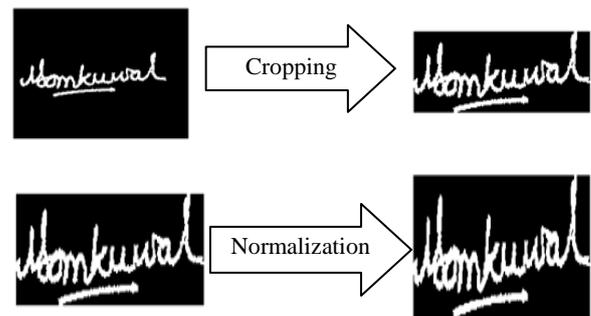
Step 4: Noise removal

The bwareopen function of MATLAB was used to remove the dots arising in the image due to improper scanning (noise). This function removes all connected components that have fewer than 5 pixels from a binary image.



Step 5: Signature cropping and image normalization (resizing)

In this step, region of interest is determined using auto cropping approach. Region of Interest (ROI) is the signature object itself. Using cropping we segment the signature smoothly. Size difference may be a problem in comparing the two signatures. Therefore signatures are normalized with respect to width, height or both. To achieve logical results, the signatures must have the same size, which means normalized one, in our approach the reference sizes are [128 256].



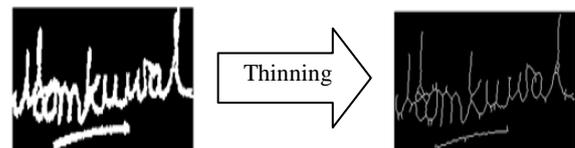
Step 6: Thinning the normalised image

Thinning is a morphological operation that is used to remove selected foreground pixels from binary images, somewhat like erosion or opening. In this mode it is commonly used to tide up the output of edge detectors by reducing all lines to single pixel thickness.

In a system, there is a need for thinning of images due to following reasons:

1. To reduce the amount of data required to be processed.
2. To reduce the time required to be processed.

The signature output using thinning algorithm is shown in below.



Feature Extraction

Feature extraction plays an important role in offline signature verification system. In the proposed system we use features based on energy of signature on grid level.

Energy of Signature on Grid Level

In this proposed feature extraction method we derived features from the total energy a writer uses to create their signature. It is hypothesized that the planned execution of the signature uses the same amount of energy whereas original writer uses different energy for signatures [5]. Local features are extracted from a portion or a limited area of the pattern and local features provide more detailed information. So we divided the whole signature image into small 16×32 block and for each

block we have calculate the energy and save as a feature vector. Pseudo code for extraction of energy of each block is

```

Function energy (binary image im)
    sum←0
    height← height of sub block
    width ← width of sub block
    for each black pixel in im
        sum ← sum + square of im ( pixel)
    end for
    energy =sum / (height × width)
    return energy
end function
    
```

Identification

In the identification mode, the system recognizes an individual by comparing the extracted features with those stored in the database. The system conducts a comparison to verify the claimed identity of the user. The calculated feature vectors for an input image should enter a comparison process to determine the user's identity. This comparison is made against stored user templates. Various methods for this comparison like Radial basis function neural networks (RBF), Multilayer perceptron (MLP), k-Nearest Neighbor (k-NN), Support vector machines, Bayes method and Euclidean distance are suggested in literature. Here comparison is made by different distance matrices which are discussed in experimental results. Out of those distances, city block distance gives good results for signature verification. The database feature vector is represented as the mean of the set of training feature vectors for a person.

III. Experiment Results

The experiment is performed on English language. To evaluate the performance of the proposed signature verification system, the image database from different persons are collected. The dataset of language is obtained from scanning of each signature. Here we have performed the experiment on database containing 80 persons each of having 5 training and 5 testing signatures. So total 400 signatures for database.

Comparison of different distance matrices for features based on energy of grid level

A crucial parameter for classification is the choice of an appropriate distance metrics to measure the similarity or dissimilarity between two signature images. It is essential to explore the different similarity measures to find out best distance metric for signature matching. In conventional signature matching technique, Euclidean distance is used to find the similarity between the test image and database image. Similarity score is used to find the best match of test image from the database image. Test image is more similar to the database image if the distance between the test image and database image is small. P and Q represent the feature vectors for database image and test image respectively.

The proposed method is tested with 6 distance matrices which are shown in below. Each and every distance gives the different FAR and FRR values such that we can choose the

distance matrix that can gives the minimum FAR and FRR values (Equal error rate).

1. Euclidean distance:

Euclidean distance metric is defined for p=2. In Euclidean distance metric difference of each dimension of feature vector of test and database image is squared which increases the divergence between the test and database image.

$$d_{euc} = \sqrt{\sum_{j=1}^N |P_j - Q_j|^2}$$

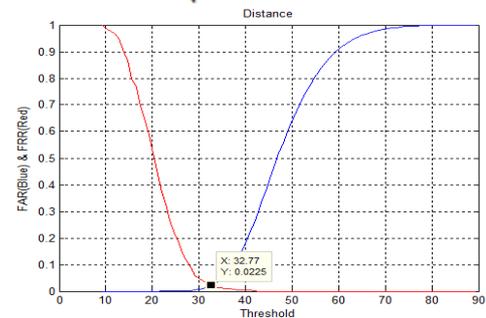


Figure 2 FAR and FRR of energy features for Euclidean distance

2. City Block distance:

This distance metric is defined for p=1. Absolute difference at each dimension of feature vector is given by an equation called City Block or Manhattan distance. This is the moderate approach to minimize the difference if dissimilarity is more.

$$d_{city} = \sum_{j=1}^N |P_j - Q_j|$$

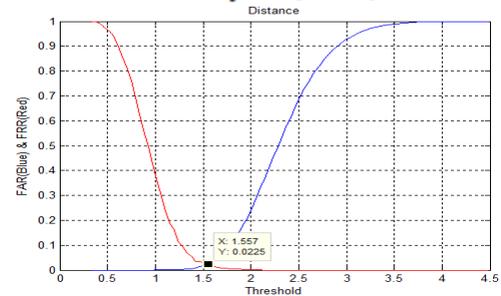


Figure 3 FAR and FRR of energy features for City Block distance

3. Hellinger distance:

In this distance square root of sum of squared square root difference at each dimension is taken which minimizes the difference if similarity between feature vectors is more. Hellinger is more robust over the squared chord distance. This distance cannot be used for feature space with negative values.

$$d_{Helling} = \sqrt{\sum_{j=1}^N (\sqrt{P_j} - \sqrt{Q_j})^2}$$

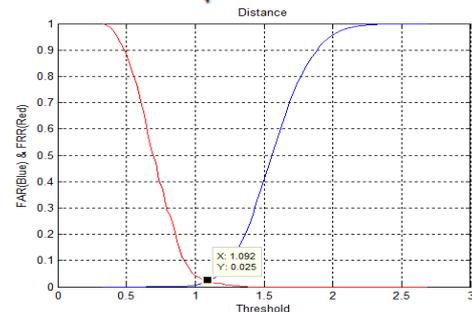


Figure 4 FAR and FRR of energy features for Hellinger distance

4. Chebyshev

Chebyshev distance maximum metric or L_∞ metric is a metric defined on a vector space where the distance between two vectors is the greatest of their differences along any coordinate dimension. The Chebyshev distance between two vectors or points p and q , with standard coordinates P_j and Q_j , respectively, is

$$d_{Chebys} = \text{Max} (|P_j - Q_j|)$$

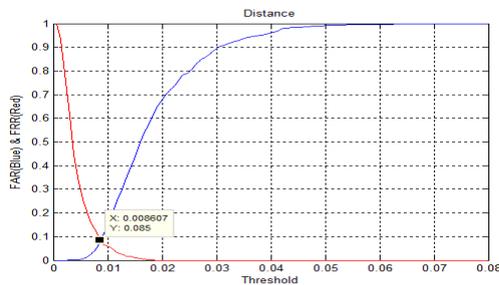


Figure 5 FAR and FRR of energy features for Chebyshev distance

5. Square Chord Distance:

In Squared chord distance sum of square of square root difference at each dimension is taken which increases the difference for more dissimilar feature vectors. This distance cannot be used for feature space with negative values.

$$d_{Sqch} = \sum_{j=1}^N (\sqrt{P_j} - \sqrt{Q_j})$$

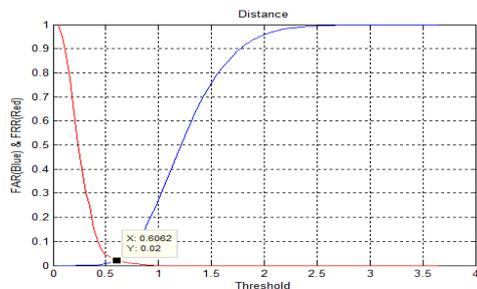


Figure 6 FAR and FRR of energy features for Square chord distance

6. Squared Euclidean Distance:

Squared Euclidean distance computes sum squared difference at each dimension of feature vector.

$$d_{SqEucl} = \sum_{j=1}^N (P_j - Q_j)^2$$

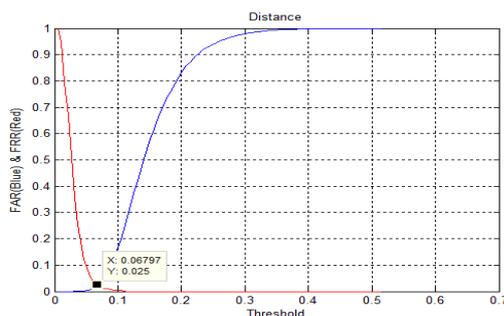


Figure 7 FAR and FRR of energy features for square euclidean distance

Types Of Distances	FAR (%)	FRR (%)	Threshold	Time (sec.)
Euclidean	2.25	2.25	32.87	4.837
Cityblock	2.25	2.25	1.557	0.969
Hellinger	2.5	2.5	1.092	2.148
Chebyshev	8.5	8.5	86	1.975
Squarechord	1.52	2.5	0.5695	2.2978
Square euclidean	2.5	2.5	0.067	0.889

Table 1 FAR and FRR for different distances for energy features

IV. Conclusion

Our traditional method i.e. Euclidean distance gives moderate FAR and FRR values and time taken for calculation also more compare to Cityblock distance. Hellinger distance gives good FRR and FAR values and time taken for calculation is more compare to all distances. Whereas Cityblock and Squareeuclidean give good FAR and FRR values for energy features and both have low calculation time. Cityblock is good for energy features.

V. Future Scope

Future work will include the automation of off-line handwritten signature trajectory recovery; the extraction of energy information from more different parts of the signature; appropriately organizing the extracted information for use with SVMs

References

- i. Anil K. Jain, Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004
- ii. Anil K. Jain, Patrick Flynn and Arun A. Ross, "Handbook of Biometrics", Springer Science & Business Media, LLC, USA, 2008
- iii. Banshider Majhi, Y. Santhosh Reddy, "Novel Features for Off-line Signature Verification", International Journal of Computers, Communications & Control, vol.1, no.1, pp 17-24, 2006 (IJECIT) Volume 2, Issue 7, January 2013.
- iv. Priya Metri, Ashwinder Kaur, "Handwritten Signature Verification using Instance Based Learning", International Journal of Computer Trends and Technology- March to April Issue 2011.
- v. Vu Nguen and Graham Leedham, "Global Features for the Off-Line Signature Verification Problem", IEEE computer society, 2009.
- vi. Madhuri Yadav, Alok Kumar, Tushar Patnaik, Bhupendra Kumar, "A Survey on Offline Signature Verification", International Journal of Engineering and Innovative Technology
- vii. Ssamit Biswas, Tai-hoon Kim, Debnath Bhattacharyya, "Features Extraction and Verification of Signature Image using Clustering Technique", International Journal of Smart Home, Vol.4, No.3, July, 2010.
- viii. Pprashanth C. R. and K. B. Raja, "Off-line Signature Verification Based on Angular Features", International Journal of Modeling and Optimization, August 2012.
- ix. MM.S.Shirdhonkar, Manesh Kokare, "Off-line Handwritten Signature Identification Using Rotated Complex Wavelet Filters", International Journal Of Computer Science, vol 8, Issue 1, pp 748-753, 2011.
- x. Mmina Fakhalai, Hamid Reza, "off line signature recognition based on contourlet transform", International Conference on Machine Learning and Computing, vol.3, pp 198-203, 2011

Observation Table