International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 06 | June -2017 www.irjet.net p-ISSN: 2395-0072

DISTANCE BASED VERIFICATION TECHNIQUE FOR ONLINE SIGNATURE SYSTEM

Prathiba M K[1] ,Bindushree B N[2], ,Bindushree T S[3], Chandrakala V[4] and Sahana B R[5]

[1]Professor , Dept. of electronics and communication Engineering, ATMECE Mysore, Karnataka, India
[2,3,4,5] UG Students Dept. of electronics and communication Engineering, ATMECE Mysore, Karnataka, India

---

Abstract – *This paper based on verification techniques for online signature verification system. For the purpose of extracting the features of the signature, histogram feature extraction technique is used. Each signature is symbolized as a feature vector. In case of verification of the online signature system Euclidean distance is calculated. Signature plays vital role in authentication of legal system. In order to avoid the unauthorized person to access the system signature verification is used. The proposed system is based on Euclidean distance verification techniques using histogram. Experimental results obtained using Euclidean distance method to get FAR and FRR of the individual's signature.*

Key Words: Online Signature, Feature Extraction, Euclidean distance, FAR and FRR.

1. INTRODUCTION

A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioural characteristic that the person possesses. Depending on the application context, a biometric system typically operates in one of two modes Verification / identification. In verification mode, the system validates a person's identity by comparing the captured biometric characteristic with the individual's biometric template, which is pre stored in the system database.

Alan McCabe et. al. [1] proposed a method for verifying handwritten signatures by using NN architecture. Various static (e.g., height, slant, etc.) and dynamic (e.g., velocity, pen tip pressure, etc.) signature features are extracted and used to train the NN. Several Network topologies are tested and their accuracy is compared. The resulting system performs reasonably well with an overall error rate of 3.3% being reported for the best case.

Ian W. Mc Keague, et, al.[2] proposed two methods for the detection of skilled forgeries using template matching. One method is based on the optimal matching of the one-dimensional projection profiles of the signature patterns and the other is based on the elastic matching of the strokes in the two-dimensional signature patterns.

A novel approach to off-line signature verification is proposed by Wei Tian et. al. [3]. Both static and pseudo dynamic features are extracted as original signal, which are processed by Discrete Wavelet Transform (DWT) and converted into stable features in each sub-band which can enhance the difference between a genuine signature and its forgery.

1.1 Methodology

The proposed signature verification consists of Data acquisition. Preprocessing and feature extraction and verification. Data is acquired from WACOM CTL-471/KOC.WACOM signature tablets. Database includes signatures of 25 users and corresponding to each user 5 signatures are taken which includes 3 genuine and 2 forged signatures. The acquired sample signature is as shown in Fig.1.

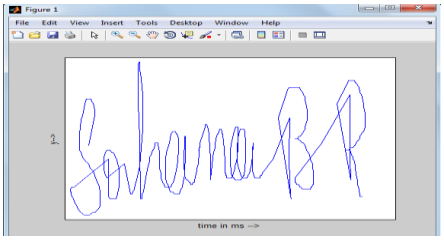

Fig -1: Acquired sample signature

Here total three parameters are taken into account Acquired parameters are: x-coordinate, y-coordinate, and angle. Out of which first two are directly acquired from the dataset and other is calculated using the x and y coordinates of a signature taken from the dataset.

1.2 Preprocessing

Height and width of signatures fluctuate from person to person and occasionally even the same person may exercise different sizes of signature. Therefore it is needed to get rid of the size variation and through the normalization process Constant signature size can be achieved.

2. FEATURE EXTRACTION

Feature extraction plays an important role in verification systems. In Feature extraction, the essential features are extracted from the original input signature based on the application, and fluctuate accordingly. The feature extraction process is an important step in developing the system since it is the key to differentiate one user's signature from another.

The features that are extracted from this phase are used to create a feature vector which is then used to uniquely characterize a candidate signature.
The histogram feature extraction of x-coordinate is as shown in Fig.2. At this stage the signature sample will varies from left to right.

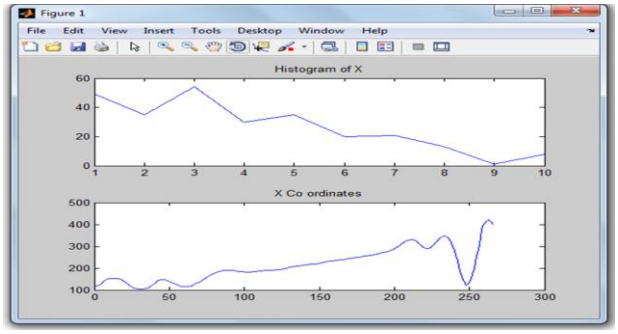

Fig -2: Histogram feature extraction of x-coordinate

The extraction of y-coordinate the signature varies different axis in y-coordinate is as shown in Fig.3

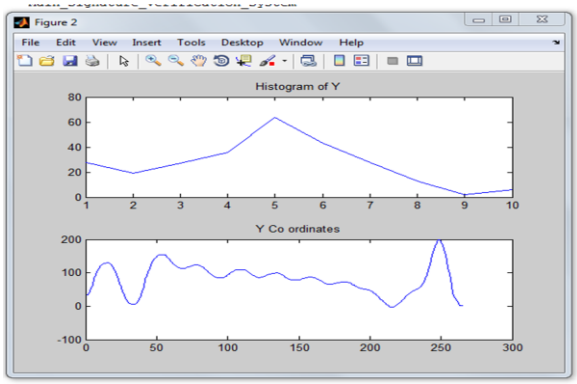

Fig -3: Histogram feature extraction of y-coordinate

The histogram feature extraction of angle in which the angle varies with respect to X and Y-coordinate is as shown in Fig.4.

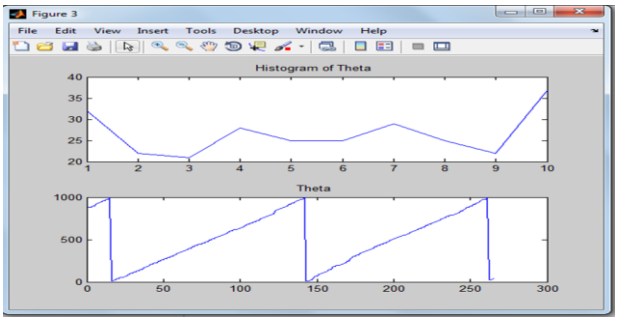

Fig -4: Histogram feature extraction of y-coordinate

Euclidean distance has been used for the verification of the signature.

The various steps involved in the proposed system are as as shown in the Fig.5.

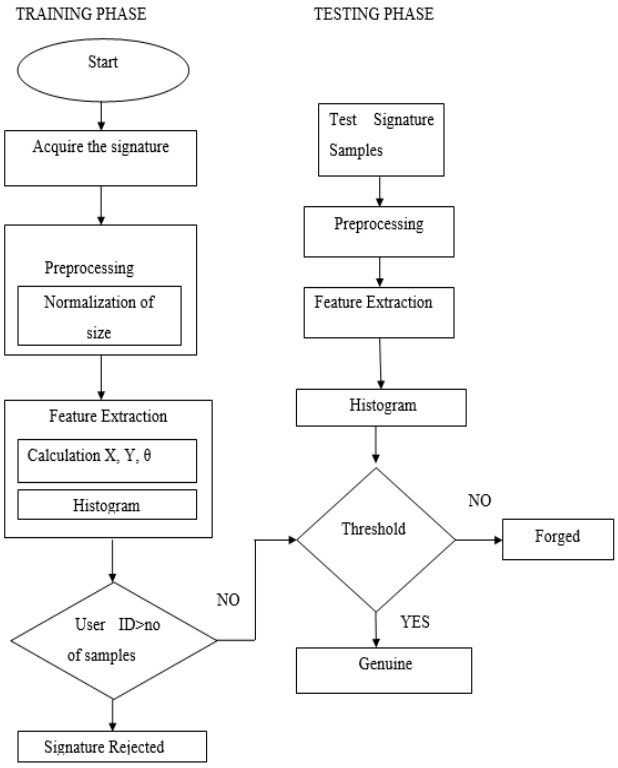

Fig -5: Flow of the proposed system

For the genuine signature the result of verification system is as shown in Fig.6.

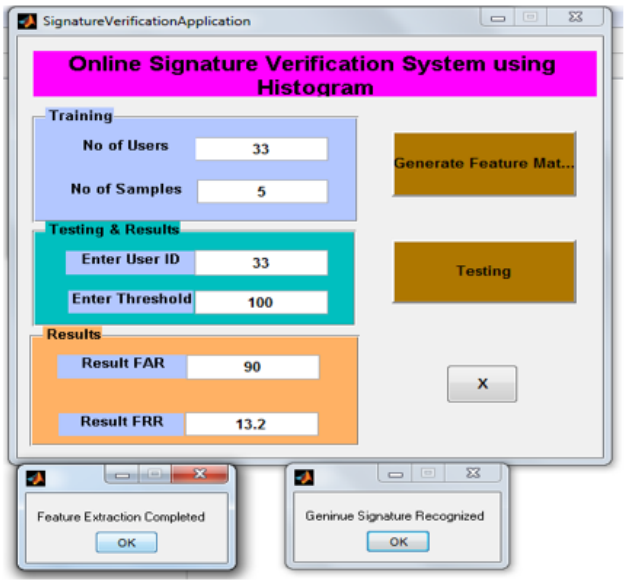

Fig -6: Output of genuine signature

3. CONCLUSIONS

In online signature verification the user must provide a set of reference signatures to enroll in the system. Features are then extracted from the signatures. To verify a test signature, the same processes are applied. The test signature is then matched to all the other reference signatures. The method used to match signatures is based on the concept of histogram using Euclidean distance method. The dissimilarity values obtained is then compared to a threshold to decide whether the signature is genuine or a forgery. With the improvement in the forgery signatures enrolled, the overall system performance can be increased.

REFERENCES

[1] Alan McCabe, Jarrod Trevathan and Wayne Read, "Neural Network-based Handwritten Signature Verification", Journal of computers, vol. 3, no. 8, August 2008..

[2] Ian W. McKeague, "A statistical model for signature verification", May 14, 2004.

[3] Wei Tian, Yizheng Qiao and Zhiqiang Ma, "A New Scheme for Off-line Signature Verification Using DWT and Fuzzy Net", 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing.