International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 22 (2017) pp. 12004-12007

Histogram Based on Line Signature Verification System

Prathiba M K [1] and Basavaraj L [2]

[1, 2] Department of Electronics & Communication Engineering,
ATME College of Engineering, Mysore, Visvesvaraya Technological University,
Belgaum 590 018, Karnataka, India.
[1]Orcid Id: 0000-0002-7797-9347

Abstract

Signatures have been considered a typical form of authentication in our society for hundreds of years. In order to avoid the unauthorized person to access the system signature verification is used. Signature is a simple, concrete expression of the unique variations in human hand geometry. The way a person signs his or her name is known to be characteristic of that individual. A signature verification system must be able to detect forgeries, and, at the same time, reduce rejection of genuine signatures. Signatures are subject to intra-personal variations. Hence, a signature verification system provides better results if the system is insensitive to intra-personal variability, but sensitive to interpersonal variability. Even when insensitive to intra-personal variations, the system must possess the discriminating power to foil skillful forgers. The proposed system is based on Euclidean distance verification techniques, to get FAR and FRR of the individual's signature.

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

INTRODUCTION

Human signature is a biometric measure of person's identification. In many sectors like banks, official documents, receipts etc. handwritten signature are verified to secure and identify the concerned person. Each individual has his own signature different with others but in most of the time it is not possible to produce the replica of the signature. The signature verification problem aims to minimize the intrapersonal differences. Signature verification can be categorized into following two parts: online and offline .Online handwritten signature verification deals with automatic conversion of characters which are written on a special digitizer, tablet PC or PDA, Wherein a sensor picks up the pen -tip movements as well as pen -up/pen-down switching.

An on-line signature verification system based on local information and a one-class classifier, i.e. the Linear Programming Descriptor classifier (LPD), was presented by Nanni and Lumini [1]. The authors investigated and described how the information was extracted as time functions of various dynamic properties of the signatures, and then the discrete 1-D Wavelet Transform (WT) was performed on these features. The DCT was used to reduce the approximation coefficients vector obtained by WT to a feature vector of a given dimension. Fabregas and Faundez-Zanuy [2] have presented a new system for on-line signature verification based on DCT feature extraction with discriminability feature selection. They performed a complete set of simulations with the largest available online signature database, MCYT, which consists of 330 people with genuine and skilled forgeries performed by five other different users.

Dimauro et.al.[3] in their study of local features stability have introduced a warping function that allows m to n points to be matched. However, such an approach may not be practical in cases of extreme values of features.

Lei and Govindaraju[4] analyzed the consistency and discriminative power of on-line features using a distance-based measure that is optimized for each feature of study. They view signature verification as a one category classification problem, and use the distances between features to distinguish them rather than the feature values themselves.

METHODOLOGY

The proposed method for online signature verification mainly consists of three phases; enrollment phase, feature extraction an verification phase. The x, y coordinates of the pen and movement of pen are extracted from signatures and represented as 1D time domain signals.

A. Signature Acquisition

Data collection is an important part of the signature verification process. It is necessary that the data obtained must be accurate. This part of the menace may be solved using digitizing tablets available that can accurately capture the data from the signature. Data is acquired from WACOM CTL-471/KOC.WACOM, The acquired sample signature is as shown in Figure 1.

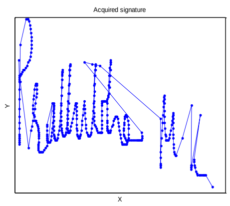

Figure 1: Acquired sample signature

Signature tablets. Database includes signatures of 25 users and corresponding to each user 20 signatures are taken which includes 10 genuine and 10 forged signatures.

B. Feature Extraction

The feature extraction process is an important step in developing the system, it plays a vital role in verification system. In Feature extraction, the crucial features are extracted from the original input signature. Since it is the key parameter which is used to differentiate one user's signature from another. In this work three parameters are taken into account: x and y-coordinates values are directly acquired from the dataset. The corresponding pen movement angle is derived using the x and y coordinates of a signature taken from the dataset is as shown in the Figure 2.The features that are extracted from this phase are used to create a feature vector which is then used to uniquely characterize a signature.

C. .Normalization

Normalization is used to increase the speed up process otherwise system will take more time to train the neural networks. The corresponding output obtained for the different features is as shown in the Figure 3.

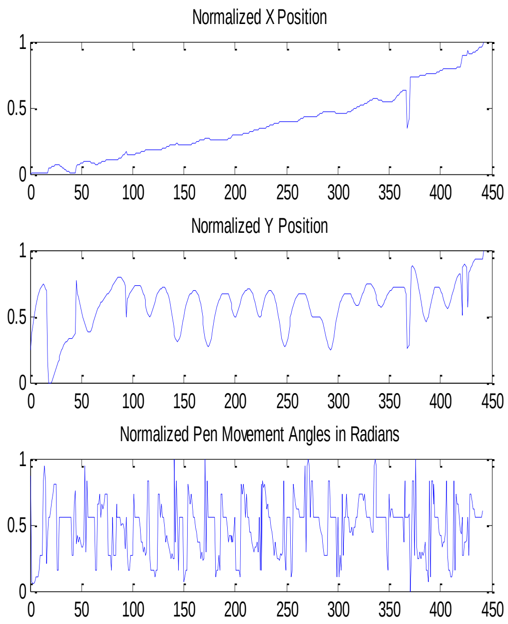

Figure 3: Normalized Features

Histogram is only used to plot the frequency of score occurrences in a continuous data set that has been divided into classes. A histogram is used to graphically summarize and display the distribution of a process data set. The spread is the range of the data and shape describes the type of graph. The four ways to describe shape are whether it is symmetric, how many peaks it has, if it is skewed to the left or right, and whether it is uniform. Histogram features are used to differentiate genuine and forged signatures the corresponding acquired signatures histogram of different features is as shown in the below Figure 4.

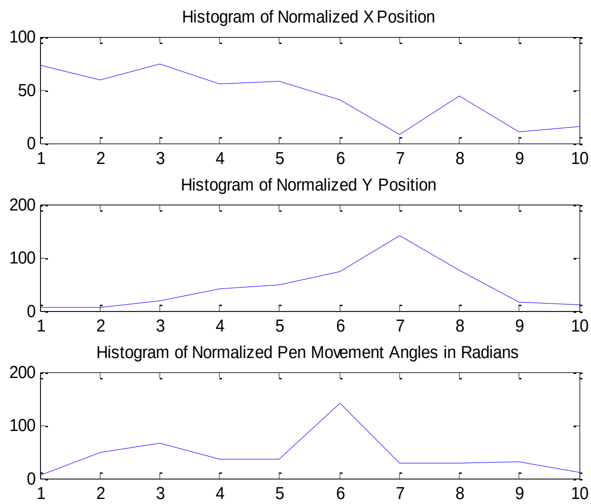

Figure 4: Histogram of Normalized Features

C. Verification

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

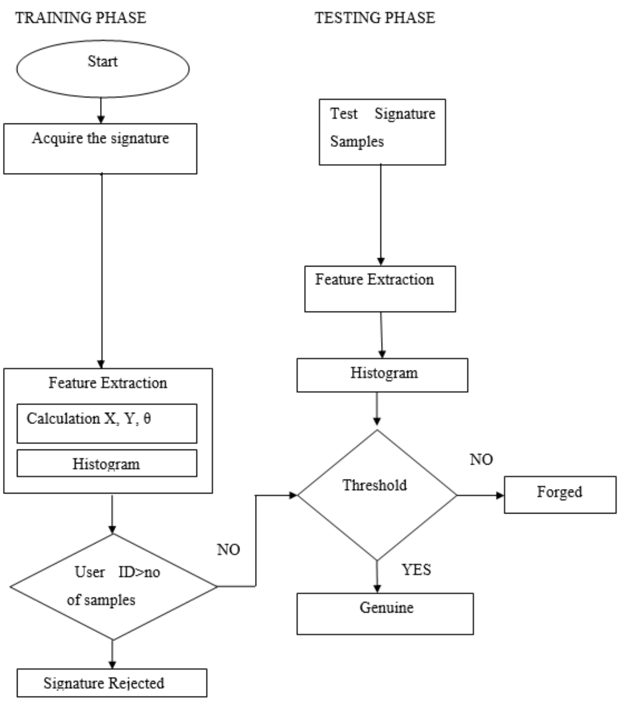

Figure 5: Flow of the proposed system

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.

The verification is based in the distribution of features, in order to compare two distributions Euclidean distance and histogram are used. The Euclidean distance between two signals is used to find minimum difference between two time series.

RESULTS AND DISCUSSION

To validate the implemented system, the Accuracy of the system is computed. Which in turn depends upon the FAR and FRR. Therefore the performance online Signature Verification systems are mainly evaluated by two most important performance metrics. The False Acceptance Rate (FAR) and the False Rejection Rate (FRR). FAR or type II error is the percentage of forged signatures that were falsely verified as genuine. FRR or type I error is the percentage of genuine signatures that were falsely rejected as unauthentic. These two error rates should be as low as possible for a good online signature verification system. The two types of error usually have different effects associated with them depending on the security requirements of the application.

The experiments are carried out separately for genuine and forgeries. Both are available in database. Out of twenty signatures the first ten signatures are used for training. This procedure is repeated for forgeries. While the remaining 10 trails of the genuine signatures and 10 trails of the forged signatures of 25 users are used for testing. A writer dependent threshold is selected to obtain the high acceptance rates of genuine signature and significantly lower rates for the forgeries. For each users FAR, FRR and Accuracy is calculated for individual user. It has been observed that overall accuracy of the on line signature verification system is 92.4% is indicated in the Table1.

Table 1: Accuracy of the System.

User ID	**FRR (%) (Genuine)**	**FAR (%) (Forgery)**	**Accuracy (%)**
User 1	0	20	90
User 2	0	10	95
User 3	10	20	85
User 4	0	20	90
User 5	10	0	95
User 6	0	10	95
User 7	10	10	90
User 8	0	10	95
User 9	10	10	90
User 10	0	10	95
User 11	10	10	90
User 12	0	10	95
User 13	10	10	90
User 14	0	10	95
User 15	0	20	90
User 16	0	10	95
User 17	0	20	90
User 18	0	10	95
User 19	0	0	90
User 20	0	10	95
User 21	0	10	95
User 22	0	20	90
User 23	0	10	95
User 24	10	10	90
User 25	0	10	95
Average (Accuracy %)			92.4

CONCLUSION

Biometric software security systems are most reliable for a person's authentication and verification with a high level of accuracy. Online signature verification system provides most acceptable and low cost system. The proposed methods used x, y coordinates of the pen movement values. Proposed method is evaluated by computing FAR, FRR and Accuracy of the system. It is concluded that with features, we achieved 92.4% accuracy by using Euclidean distance for matching. This work can be improved by using efficient matching technique, by finding more accurate threshold. In future we intend to evaluate the methods on different databases and investigate the stability of the features. Efficient feature selection method can improve the results.

REFERENCES

[1] Nanni, L. and Lumini, A., “novel local on-line signature verification system “Pattern Recognition Letters, 2008, pp. 559–568. G.Y. Goldstein. “Strategic Innovation Management: Trends, Technology, Practice: A Monograph”. Taganrog: Publishing House TRTU, 2002.

[2] Fabregas, J. and Faundez-Zanuy,. “On-line signature verification system with failure to enroll management”, Pattern Recognition Letters, 2009, pp. 2117–2126.

[3] Dimauro, G., Modugno, R., Pirlo, G. and Sarcinella, L., "Analysis of stability in hand-written dynamic signatures”, Proceedings of the 8th International Workshop on Frontiers in Handwriting Recognition, IWFHR, 2002, pp. 259–263 P. Drucker. “Management Challenges in the 21stCentury”. Moscow: Publishing House "Williams", 2003.

[4] H. Lei, V. Govindaraju “A comparative study on the consistency of features in on-line signature verification”, Pattern Recognition Letters, 26 (15) (2005), pp. 2483– 2489.