International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

ONLINE BIOMETRIC SIGNATURE VERIFICATION BASED ON BOTH LOCAL AND GLOBAL SYSTEM

Siraj Nisha[1], Deepesh A [2]

[1]P G scholar, Dept. of Computer Science And Engineering, Musaliar College of Engineering and Technology, Pathanamthitta
[2]Associate professor, Dept. of Computer Science And Engineering, Musaliar College of Engineering and Technology, Pathanamthitta

---

Abstract - *Signature verification is an important topic in biometric authentication. Signature verification can be either Offline or Online based on available data in the input. In this paper, we focus on online signature verification since this biometric trait is widely used one. The proposed system is based on two main stages. The first one is a data preprocessing stage, applied in order to reach high similarity between signatures coming from different devices. The second one is feature selection global feature based system and time function based system are used. For additional we use Z-score normalization and KNN classifier for better performance. Equal error rate(EER) has been used as optimization criterion and the result prove the robustness of proposed system.*

Key Words: DTW, Equal error rate, global feature - based system, KNN classifier, time functions - based system, Z-score normalization.

1. INTRODUCTION

Signature is widely used for personal identification and verification. Verification can be either Offline or Online based on available data in the input. Online systems use dynamic information of a signature and is captured by data acquisition devices like pressure-sensitive tablets and webcam at the time the signature is made. Offline systems take as input the scanned image of a signature. It is useful for verification of signatures found on bank checks and documents. Today, signatures can be captured by multiple electronic devices such as pen tablets, Personal Digital Assistants (PDAs), grip pens, smart phones, etc. There are many challenges in signature verification, one of the main challenge is related to signature variability. The main goal of this project is to analyze and improve the system performance in case for online signature verification. This paper is focused on online Signature verification. There are many methods for online signature verification. Signature verification systems differ only in their feature selection and decision strategy. The on-line signature verification techniques can be classified into two areas.

1. Features extracted from the visible parts of the signature.

2. Features extracted from invisible parts of the signature.

In this work, for on-line signature verification, there are two approaches for feature extraction: global features-based systems and time function based system. Global features- based systems extract global information from a signature. global information are signature duration, number of pen ups, signature bounding box, trajectory length or average signing speed, etc. time functions- based systems extract the signature time functions .time functions are X and Y pen coordinates, pressure, acceleration, stroke length etc.

2. PROPOSED SYSTEM

In the proposed system, build a novel method for signature verification. It involves the two main procedures: Data preprocessing and Feature extraction. The first step, data preprocessing is applied in order to reach high similarity between signatures coming from different devices. In the second step, global features based systems and time functions based systems are used. A total of 100 global features and Mahalanobis distance algorithm are used for the global features based system and a total of 21 time functions and DTW algorithm are used for the time functions based system. For additional, we use Z-score normalization and K nearest neighbor classifier. Z-score normalization is applied for feature normalization. Z-score normalization is used to avoid sampling errors and provide better performance. K nearest neighbor classifier is used to train the training data and input data. It provide better performance compared to existing system.

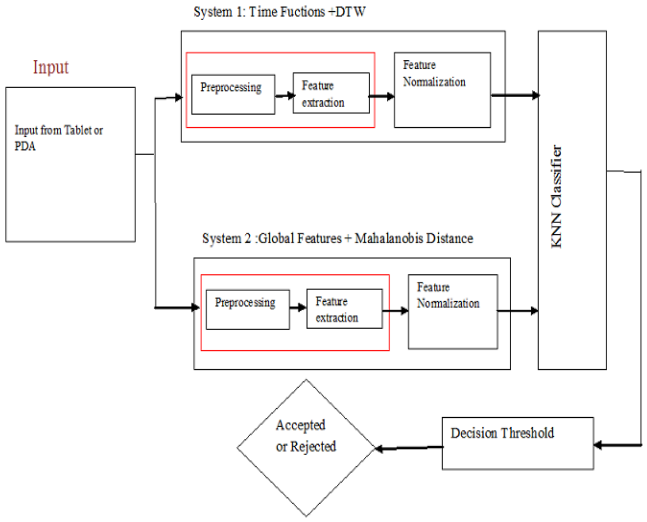

Fig 1: Architecture of proposed system

Fig. 1 shows the architecture of the proposed system. it consists of two stages :data preprocessing and feature selection. This approach is applied to two common systems in online signature verification-local and global systems. A total of 100 global features and Mahalanobis distance algorithm are used for the global features based system and a total of 21 time functions and DTW algorithm are used for the time functions based system for similarity comparison of signatures. Finally, Sequential Forward Feature Selection (SFFS) algorithm is used to select global features-based system with 28 global features and time functions-based system with 7 time functions for all the comparison cases. This features are normalized by z-score normalization and output is trained with KNN classifier.

2.1 Online Signature Verification

It consists of the following

- Data preprocessing step
- Feature extraction and selection
- The proposed global features-based system (global system), and time functions-based system (local system)
- K Nearest Nieghbour(KNN) classifier

2.1.1 Data preprocessing

This is the first stage of proposed system. The aim is to obtain signatures with the same type of information , time and spatial position standard formats. To improve the performance of the system, Z-score normalization based on the mean and standard deviation was applied to both systems. It achieved best results compared to existing system.

2.1.2 Feature extraction and selection

The second stage of system is focused on obtaining a selection of global features and time functions (local features). In this paper, a global features-based systems with a total of 100 features and time functions-based systems with a 21 time functions are considered. Due to the low amount of training data in a signature, Sequential Forward Feature Selection (SFFS) algorithm is used to obtain the 28 global features and 7 time functions which improves the performance of the system.

2.1.3 Global feature based verification system

The Mahalanobis distance is used to compare the similarity between a signature and training set of signatures. Training set of signatures is used to create user model. User model is defined as,

$$C = (\mu, X)$$

where μ is a mean of feature vectors extracted from each signature of user and X is a diagonal covariance matrix. The matching score is obtained as

$$s(x, C) = \cdot(x - \boldsymbol{\mu})^{T} (\mathbf{X})^{-1}(x - \boldsymbol{\mu})^{\cdot -1/2}$$

The score s(x, C) is a specific threshold, which is used to consider the signature is genuine or not.

2.1.4 Time function based verification system

DTW algorithm is used to compare the similarity between time functions from each signatures. Matching scores are obtained as:

$$\text{score} = e^{-D/K}$$

where D represent the minimal accumulated distance and K represent the number of points aligned between two signatures.

2.1.5 K-Nearest Neighbour (KNN)classifier

The main goal of this classifier is to classify the unseen data correctly which is not available in the training dataset. classifier separates data into training and testing set. In this paper we use K-Nearest Neighbour classifier for classification of the signatures because it is simplest classification technique. The classification of signatures are based on votes of its neighbours which represented by k. K-NN classifies the signature in to a particular class which has majority of votes. K-NN computes the distance between feature values of the test signature and the feature vector values of every training

signature. The classification data set consists of few genuine signatures and same number of forged signatures, which is used to test the trained classifier and obtain best results.

3. RESULTS

In this paper we built database of about 80 signatures from about 15 different persons. 5 signatures per person was used for testing and 2 good signature samples were collected for signature verification purposes. Two signatures samples was used to identify forgeries. There are two stages in our system:

Enrollment phase: The user produces several signatures. The online signature data captured by PDA or Tablet . Then this data preprocessed and some features are extracted and selected. The extracted features used as reference data.

Verification Phase: The test signature given as input for verification.. The extracted features of test signatures compared with the reference signature enrolled in data base.

In order to validate the implemented system, we evaluate the verification performance system on the remaining 80 users. The EER for the existing and proposed systems are studied. the proposed system provides an average relative improvement of 10.0% EER for skilled forgeries and 36.3% EER for random forgeries. It provide better performance than existing system.

	Skilled forgeries		Random Forgeries	
No of Trials	Existing	Proposed	Existing	Proposed
Sig 1:10 times	8.9	6.5	3.5	2.1
Sig 2: 15 times	12.4	10.3	3.3	2.6
Sig 3: 8 times	21.5	17.4	10.5	4.8
Sig 4: 10 times	14.3	12.1	4.8	4.6

Table 1: Validation Result: System Performance in Terms of EER(%)

4. CONCLUSION

In this work, the main goal was to analyze the challenging problem of online signature verification. Two main stages are proposed in this paper. The first stage is a data preprocessing stage, applied in order to reach high similarity between signatures coming from different devices. The second stage is feature selection, global feature based system and time function based system are used to select the best features . This proposed system has been successfully applied to the two main system approaches in on-line signature verification.

Two different systems are considered in this work: a global features- based and time functions-based systems. The performance of the proposed system have provided an average relative improvement of 38.5% EER and 13.0% EER respectively for skilled forgeries compared to the existing systems, whereas the relative improvement for random forgeries is 58.3% EER and 25.5% EER respectively compared to the existing systems. K nearest neighbor classifier and z score normalization are used to provide better performance than existing system.

ACKNOWLEDGEMENT

I am extremely grateful to my PG Coordinator Prof. Shyjila.P.A, Associate Professor of Computer Science and Engineering department and my guide Prof.Deepesh A, Associate Professor of Computer Science and Engineering department,Musaliar College of Engineering, Pathanamthitta for his valuable guidance, timely suggestions and for providing all the vital facilities like providing the Internet facilities and important books, which were essential in the completion of this work . Finally, I would like to thank every individual who gave me even the slightest support to make my project a success.

REFERENCES

[1] D. Impedovo and G. Pirlo, ,"Automatic signature verification: The state of the art," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 38, no. 5, pp. 609–635, Sep 2008.

[2] [2] R. Vera-Rodriguez, R. Tolosana, J. Ortega-Garcia, and J. Fierrez, "e-BioSign: Stylus- and finger-input multi-device database for dynamic signature recognition," in Proc. 3rd Int. Workshop Biometrics Forensics (IWBF), Mar 2015.

[3] [3]W. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," IEEE Commun. Surveys Tuts., vol. PP, no. 99, p. 1, Dec 2014.

[4] [4] J. Fierrez-Aguilar, L. Nanni, J. Lopez-Peñalba, J. Ortega-Garcia, and D. Maltoni, "An on-line signature verification system based on fusion of local and global information," in Proc. 5th IAPR Int. Conf. Audio-Video-Biometric Pers. Authentication(AVBPA),vol.3546.,pp. 523–532 Jul 2005.

[5] [5]M. Martinez-Diaz "Dynamic signature verification for portable devices," M.S. thesis, Dep. Comput. Sci., Univ. Autónoma Madrid, Madrid, Spain, Nov. 2008.

[6] [6]R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Feature- based dynamic signature verification under forensic scenarios," in Proc. 3rd Int. Workshop Biometrics Forensics (IWBF), Mar. 2015.

[7] [7]J. Fierrez, J. Ortega-Garcia, D. Ramos, and J. Gonzalez-Rodriguez, "HMM-based on-line signature verification: Feature extraction and signature modeling," Pattern Recognit. Lett., vol. 28, no. 16, pp. 2325–2334,Dec. 2007.