International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 9 66- 68

Online Signature Verification: Present State of Technology

[1]Manas Singhal, [2]Maitreyee Dutta
[1]Assistant Professor, E&C Engineering Department, MIT, Moradabad
[2]Professor and Head, E&C Engineering Department, NITTTR, Chandigarh

Abstract:- The way a person signs his or her name is known to be characteristic of that individual. Signatures are influenced by the physical and emotional conditions of a subject. A signature verification system must be able to detect forgeries, and, at the same time, reduce rejection of genuine signatures. Significant research has been conducted in feature extraction and selection for the application of on-line signature verification. All these features may be important for some problems, but for a given task, only a small subset of features is relevant. In addition to a reduction in storage requirements and computational cost, these may also lead to an improvement in general performance. On the other hand, selection of a feature subset requires a multi-criterion optimization function, e.g. the number of features and accuracy of classification. In this paper all these techniques are reviewed.

Keywords:- *FAR, FRR, EER.*

*****

I. INTRODUCTION

The use of biometrics poses many privacy concerns: when an individual gives out his biometrics, either willingly or unwillingly, he can disclose sensitive information about his personality and health status [3] which can be used to profile him. Moreover, data collected for some specific purposes might be used in the long run for different ones, a possibility usually referred to as function creep. Also, the uniqueness characterizing biometric data, and the fact that biometrics are permanently associated with their users, can be exploited to perform an unauthorized tracking of the activities of the subjects enrolled in different biometric databases. The use of biometrics can also raise cultural and religious concerns.

A template protection scheme should satisfy the following properties:

Renewability: for each user, it should be possible to revoke a compromised template and reissue a new one based on the same biometric data (revocability). Moreover, each template generated from a biometrics should not match with the others previously generated from the same data (diversity). The renewability property is needed to ensure the user's privacy.

Security: it must be impossible or computationally hard to obtain the original biometric template from the stored and secured one. This property is needed to prevent an adversary from creating fake biometric traits from stolen templates. In fact, although it was commonly believed that it is not possible to reconstruct an original biometric characteristic from the corresponding extracted template, some concrete counter examples, which contradict this assumption, have been provided in the recent literature, as in [4].

Performance: the recognition performance should not degrade significantly with the introduction of a template protection scheme, with respect to the performance of a nonprotected system.

II. LITERATURE REVIEW

On-line Signature Verification Based on GA-SVM [1]

Huang et al. proposed a method of verification of on-line handwritten signatures using both Support Vector Data Description (using SVM) and Genetic Algorithm (GA). A 27-parameter feature set including shape and dynamic features is extracted from the on-line signatures data. As a kernel based one-class classifier, SVM can accurately describe the feature distribution of the genuine signatures and detect the forgeries. Signature data form the SVC2013 database is used to carry out verification experiments. The proposed method can achieve an average Equal Error Rate (EER) of 4.93% of the skill forgery database. This method is using global features parameter for signature, although it has the advantages of strong anti-interference capability, convenient calculation advantages, but the signature on the local details distinguish ability is weak.

Identity Authentication using Improved Online Signature Verification Method [2].

Kholmatov et al. established a test signatures authenticity is by first aligning it with each reference signature for the claimed user, using dynamic time warping. The distances of the test signature to the nearest, farthest and template reference signatures are normalized by the corresponding mean values obtained from the reference set, to form a three dimensional feature vector. This feature vector is then classified into one of the two classes (genuine or forgery). Principal component analysis obtained a 1.4% error rate for a data set of 94 people and 619 test signatures (genuine signatures and skilled forgeries). In two-class pattern recognition problem they showed that the pressure information does not seem to be a useful feature in distinguishing forgeries from geniuses.

Online Handwritten Signature Verification using Neural Network Classifier Based on Principal Component Analysis [3].

Iranmanesh et al. proposed a systematic approach to online signature verification through the use of multilayer perceptron (MLP) on a subset of principal component analysis (PCA) features. The proposed approach illustrates a feature selection technique on the usually discarded information from PCA computation, which can be significant in attaining reduced error rates. The experiment is performed using 4000 signature samples from SIGMA database, which yielded a false acceptance rate (FAR) of 7.4% and a false rejection rate (FRR) of 6.4%. 200 users with 8,000 signature samples have been used with accuracy of 93.1%. Paper shows that not only the components (as features) retrieved from principal component analysis, but also other elements, such as latent and score values, could be used to achieve a high accuracy rate. On-Line Signature Verification [4].

Jain et al. used a digitizing tablet to captures both dynamic and spatial information of the writing. The similarity between an

input signature and the reference set is computed using string matching and the similarity value is compared to a threshold. In this paper number of strokes are used as a global feature.

Online and Offline Signature Verification : A Combined Approach [5].

Radhika et al. focused on both online and offline features of handwritten signatures and aims at combining their results to verify the signature. The online and offline method verifies the signature separately and finally their results are combined and the signature is verified using SVM. Paper also compares the results of online, offline and combined approach. The online approach deals with the videos of signing process and the pen track is used for forming the feature vector. Whereas offline signature verification deals with the scanned images of the signatures and uses the gradient and projection features for forming the feature vector.

Signature Verification Using Static and Dynamic Features [6].

Vatsa et al. explained that the texture and topological features are the static features of a signature image whereas the digital tablet captures in real-time the pressure values, breakpoints, and the time taken to create a signature. 1D - log Gabor wavelet and Euler numbers are used to analyse the textural and topological features of the signature respectively. A multi-classifier decision algorithm combines the results obtained from three feature sets to attain an accuracy of 98.18%.

A Survey on Signature Verification Approaches [7].

Pawar presented the approaches of signature verification system according to their different steps and also gave the performance evaluation on the basis of FAR, FRR and ERR so they can be analysed for their efficiency to get better result.

Online Signature Verification for Multi-modal Authentication using Smart Phone [8].

Forhad et al. have implemented a multi factor biometric authentication system that utilizes mobile platform. This model can easily be implemented with existing single or multi factor authentication model which will enable a more sophisticated and dependable authentication for day-to-day use. To increase the accuracy, one can include more features in the biometric reference string.

Feature Extraction Based DCT on Dynamic Signature Verification [9].

Rashidi et al. presented a simple and efficient approach to on-line signature verification, based on a discrete cosine transform, which was applied to 44 time signals, such as position, velocity, pressure and angle of pen. The forward feature selection algorithm is used to search for the best performing feature subsets. The proposed system is tested with different classifiers, with skilled forgery.

Offline Signature Recognition using Neural Networks Approach [10].

Karouni et al. presented a method for Offline Verification of signatures using a set of simple shape based geometric features. The features that are used are Area, Center of gravity, Eccentricity, Kurtosis and Skewness. Before extracting the features, scanned image was pre-processed to remove any spurious noise present. The system is initially trained using a database of signatures obtained from those individuals whose signatures have to be authenticated by the system. Artificial neural network (ANN) was used to verify and classify the signatures: exact or forged, and a classification ratio of about 93% was obtained under a threshold of 90%.

III. INFERENCES DRAWN OUT OF LITERATURE REVIEW

It can be observed from the literature survey that most of the work has done to:

S.N.	Authors	Title	Strength, Tools & Technology	Weakness or Research Gap	Opportunities	Remark
1.	H. Dong, G. Jain	"On-line Signature Verification based on GA-SVM"	Use of global features parameters of signature, it has the advantages of strong anti-interference capability and convenient calculation	The local details distinguish ability is weak	The local parameters can be included along with global parameters to improve performance.	Some local parameters can be included.
2.	A. Kholmatov, B. Yanikoglu	"Identity Authentication using Improved Online Signature Verification Method"	The distances of the test signature to the nearest, farthest and template reference signatures normalized by mean values obtained from the reference set, to form a three dimensional feature vector.	FAR is much higher with sampling technique.	FAR with sampling can be reduced with increasing the signature parameters.	Pressure information does not seem to be a useful feature in distinguishing forgeries from genuines.
3.	V. Iranmanesh, S. Ahmad, W. Adnan, S. Yussof, O. Arigbabu, F. Malallah	"Online Handwritten Signature Verification using Neural Network Classifier based on Principle Component Analysis"	The proposed approach illustrates a feature selection technique on the usually discarded information from PCA computation, which can be significant in attaining reduced error rates.	Out of 50 selected features very few were used for training of NN.	Neuro-Fuzzy Technique can be applied to improve performance.	Other elements, such as latent and score values, could be used to achieve a high accuracy rate.

4.	A. Jain, F. Griess, S. Connell	"Online Signature Verification"	The similarity between an input signature and the reference set is computed using string matching and the similarity value is compared to a threshold. number of strokes as a global feature	Signature database does not contain any data from skilled forgers.	Algorithm may be verified for database containing data from skilled forgers, more parameters might be include to improve the performance afterwards.	Number of strokes are used as a global feature
5.	K Radhika, Gopika S	"Online and Offline Signature Verification: A Combined Approach"	The online and offline method verifies the signature separately and finally their results are combined and the signature is verified using SVM.	Execution time will be very high due to online and offline techniques implemented together.	Very few parameters are used for comparison purpose.	Gradient And Projection Features are used For Forming The Feature Vector.

IV. CONCLUSION

A lot of research work is going on in the field of signature verification. But still there is not even a single application that is using signature verification method. A lot of focus is required in this field. Significant research has been conducted in feature extraction and selection for the application of on-line signature verification. All these features may be important for some problems, but for a given task, only a small subset of features is relevant.

REFERENCES

[1]. D. Huang and G. Jian, "On-line Signature Verification Based on GA-SVM," Int. J. Online Eng., vol. 11, no. 6, pp. 49–53, 2015.
[2]. A. Kholmatov and B. Yanikoglu, "Identity Authentication using Improved Online Signature Verification Method," Pattern Recognit. Lett., vol. 26, no. 15, pp. 2400–2408, 2005.
[3]. V. Iranmanesh, S. Mumtazah, S. Ahmad, W. Azizun, W. Adnan, S. Yussof, O. A. Arigbabu, and F. L. Malallah, "Online Handwritten Signature Verification Using Neural Network Classifier Based on Principal Component Analysis," Sci. World J., vol. 2014, pp. 1–8, 2014.
[4]. A. K. Jain, F. D. Griess, and S. D. Connell, "On-Line Signature Verification," Pattern Recognit. 35, vol. 35, pp. 2963–2972, 2002.
[5]. K. S. Radhika and S. Gopika, "Online and Offline Signature Verification : A Combined Approach," Procedia - Procedia Comput. Sci., vol. 46, pp. 1593–1600, 2015.
[6]. M. Vatsa, R. Singh, P. Mitra, and A. Noore, "Signature Verification Using Static and Dynamic Features," NEURAL Inf. Process., pp. 350–355, 2004.
[7]. S. D. Pawar, "A Survey on Signature Verification Approaches," Int. J. Comput. Sci. Inf. Technol., vol. 6, no. 2, pp. 1068–1072, 2015.
[8]. N. Forhad, B. Poon, M. A. Amin, and H. Yan, "Online Signature Verification for Multi-modal Authentication using Smart Phone," Proc. Int. MultiConference Eng. Comput. Sci., pp. 18–21, 2015.
[9]. S. Rashidi, A. Fallah, and F. Towhidkhah, "Feature Extraction Based DCT on Dynamic Signature Verification," Sci. Iran., vol. 19, no. 6, pp. 1810–1819, 2012.
[10]. A. Karouni, B. Daya, and S. Bahlak, "Offline Signature Recognition using Neural Networks Approach," Procedia Comput. Sci., vol. 3, pp. 155–161, 2011.
[11]. I. Bhattacharya, P. Ghosh, and S. Biswas, "Offline Signature Verification using Pixel Matching Technique," Procedia Technol., vol. 10, pp. 970–977, 2013.
[12]. A. Pansare, "Handwritten Signature Verification using Neural Network," Int. J. Appl. Inf. Syst., vol. 1, no. 2, pp. 44–49, 2012.