Cluster Dependent Classifiers for Online Signature Verification

S. Manjunath[1], K.S. Manjunatha[2(✉)], D.S. Guru[2], and M.T. Somashekara[3]

[1] Department of Computer Science, Central University of Kerala, Kasargod 671316, India
manju_uom@yahoo.co.in
[2] Department of Studies in Computer Science, University of Mysore, Manasagangothri, Mysore 570006, Karnataka, India
kowshik.manjunath@gmail.com, dsg@compsci.uni-mysore.ac.in
[3] Department of Computer Science and Applications, Bangalore University, Bangalore 560056, India
somashekara_mt@hotmail.com

Abstract. In this paper, the applicability of notion of cluster dependent classifier for online signature verification is investigated. For every writer, by the use of a number of training samples, a representative is selected based on minimum average distance criteria (centroid) across all the samples of that writer. Later k-means clustering algorithm is employed to cluster the writers based on the chosen representatives. To select a suitable classifier for a writer, the equal error rate (EER) is estimated using each of the classifier for every writer in a cluster. The classifier which gives the lowest EER for a writer is selected to be the suitable classifier for that writer. Once the classifier for each writer in a cluster is decided, the classifier which has been selected for a maximum number of writers in that cluster is decided to be the classifier for all writers of that cluster. During verification, the authenticity of the query signature is decided using the same classifier which has been selected for the cluster to which the claimed writer belongs. In comparison with the existing works on online signature verification, which use a common classifier for all writers during verification, our work is based on the usage of a classifier which is cluster dependent. On the other hand our intuition is to recommend to use a same classifier for all and only those writers who have some common characteristics and to use different classifiers for writers of different characteristics. To demonstrate the efficacy of our model, extensive experiments are carried out on the MCYT online signature dataset (DB1) consisting signatures of 100 individuals. The outcome of the experiments being indicative of increased performance with the adaption of cluster dependent classifier seems to open up a new avenue for further investigation on a reasonably large dataset.

Keywords: Writer representative · Signature clustering · Cluster dependent classifier · Online signature verification

R. Prasath et al. (Eds.): MIKE 2015, LNAI 9468, pp. 58–69, 2015.
DOI: 10.1007/978-3-319-26832-3_7

1 Introduction

Biometric based authentication is receiving a greater attention as a replacement for password or token based authentication modes. In biometric authentication, the identify of a person can be inferred either through physical biometric traits such as finger print, palm geometry, iris, face etc., or through behavioral biometric traits such as gait, voice, signature etc., [1]. Compared to other behavioral biometrics, signature is the most widely accepted means of authentication in many countries legally. Signature verification methods can be either offline (static) or online (dynamic). In an offline mode, verification is done based on the informations extracted from the signature image while in case of online mode, verification is done considering the additional dynamic informations extracted from the acquisition devices such as PDA, pressure sensitive tablet [2].

Different online verification methods proposed in the literature are categorized as parametric and function based approaches [1]. In parametric based approaches, suitable parameters extracted from the signature trajectory are used to represent the entire signature and verification is done considering the similar parameters of a test signature and reference signatures. In function based approaches, signature is represented by means of time functions of a signature trajectory and the verification is done by comparing the corresponding time functions of a test signature and reference signatures. Parameter based approaches enjoy the advantage of compact representation and also the matching time is less. Function based approaches takes more matching time but yet result in low error rates compared to parametric based approaches. Further parametric features are categorized as local and global features [2]. Local features are extracted from sampled points of a signature trajectory while global features correspond to the entire signature. Details about the different categories of feature for online signature are available in the review papers [3, 4].

In verification, which is a two class classification problem, the test signature is assigned the label of a genuine or a forgery class by comparing the test signature with corresponding reference signatures of a writer using a suitable classifier. For online signature verification, many classifiers have been attempted by different researchers such as distance based classifier [5], HMM [6, 7], SVM [8], PNN [9], Bayesian [10], Symbolic classifier [11], Random Forest [8]. The performance of a verification system is measured in terms of two error rates namely false acceptance rate (FAR) and false rejection rate (FAR). These two errors indicate the percentage of forgery samples wrongly classified as genuine signatures and percentage of genuine signature wrongly classified as forgeries respectively. The point where these two errors are almost equal for a particular threshold is called equal error rate (EER) which is estimated using receiver operating characteristics (ROC) curve.

Instead of deciding the label of a test signature based on the decision of a single classifier, the combined decision of several classifiers are taken into consideration which leads to several fusion based approaches [12–15]. In these works it is well established that fusion based approaches outperforms the performance of a single classifier. Recently [16] proposed a novel approach named multi-domain classification where a signature is divided into different segments and for each segment, the most profitable

domain of representation is detected. In the verification stage, DTW is used to evaluate the originality of each segment of the unknown signature.

In the above cited works, it is observed that the decision on acceptance or rejection of a test signature is taken by common classifier or common fusion of classifiers for all writers. The performance of a verification system depends on several factors such as features used, size and quality of training samples etc. As some writers are more consistent in signing than others, there will be variations in the training signatures of different writers which result in different distributions for different writers. Hence same classifier may not be effective for all writers.

For a verification system to be effective, it requires the usage of writer dependent characteristics such as writer dependent threshold and writer dependent classifier rather than using a common threshold and a common classifier for all writers. Most of the existing works are based on the usage of writer dependent threshold [2, 11, 12, 17]. In all these works, even though the threshold adapted is writer dependent, classifier used is same for all writers. Hence these models are referred to as writer independent models. Writer independent models are computationally efficient but they fail to consider the characteristics of individual writers. [18] proposed a hybrid model by exploiting the benefits of writer independent and writer dependent models for offline signature verification. But no attempt can be traced in the literatures on the usage of writer specific classifier for online signature verification.

Designing a verification model, with a suitable classifier for every writer is computationally expensive. Instead, we can group different writers into clusters and a suitable classifier can be designed for each cluster so that all the writers in a cluster can be trained with the same classifier. Clustering not only reduces the number of classifiers to be trained but also identify writers with a common set of discriminating features. Few attempts have been made for online signature verification based on clustering. [19] proposed an approach for online signature verification by clustering signature samples of a writer and representing each cluster in the form of interval valued symbolic feature vector. [20] proposed a cluster based approach for template creation. In these works, clustering is done to minimize the number of representatives for each writer but during verification, same classifier is used for all writers.

Considering these issues, in this work, we propose an approach for online signature verification by clustering different writers with similar characteristics and selecting a suitable classifier for each cluster. To preserve intra-class variation, a single template is created for each writer by considering the training samples which serves as a representative of the entire class. Template signatures are clustered into different groups using k-means clustering algorithm. To decide the suitability of a classifier for each writer, EER resulted from each classifier is taken into consideration and the classifier which yields lowest EER is selected as the best classifier for a particular writer. Finally the classifier that has been selected for majority of writers in each cluster is considered to be a suitable classifier for that particular cluster. During verification, the same classifier that has been selected for the cluster to which the writer belongs is used.

The paper is organized as follows. In Sect. 2 we discuss the different stages of our model. Description of the experimental frame work with description of the dataset used is given in Sect. 3. In Sect. 4, obtained results are presented. Comparative analysis of

our model with other existing contemporary model is given in Sect. 5. Conclusions are drawn in Sect. 6.

2 Proposed Model

The Proposed model has four different stages. In the first stage, a single template for each writer is created. In the second stage, using the template signature of each writer, writers are clustered by employing k-means clustering. In the third stage, we estimate the performance of each classifier for each writer of a cluster. The classifier which performs better for a maximum number of writers of that cluster is selected as the classifier for all writers of that cluster. The details of classifier selected for each clusters are stored in the database. The same procedure is carried out for all other clusters also. In the fourth stage, verification is carried out where the authenticity of the test signature is decided by means of the selected classifier. The architecture of the proposed model is shown in Fig. 1.

Let there be N number of writers say $W = \{W_1, W_2, W_{3,}\ldots, W_N\}$ for which an online signature verification system has to be designed. Let there be n number of samples for each writer, $W_i = \{S_1^i, S_2^i, S_3^i, \ldots S_n^i\}, 1 \leq i \leq n$ and m be the number of features extracted from each sample of each writer forming a database $Sig_{Database} = (N \times n) \times m$. The samples in the database $Sig_{Database}$ can be visualized as points in a m dimensional feature space. In feature space, the writers who have similar characteristics in terms of features will be close to each other. Hence we can group all writers into k clusters and study the suitability of selecting cluster dependent classifier.

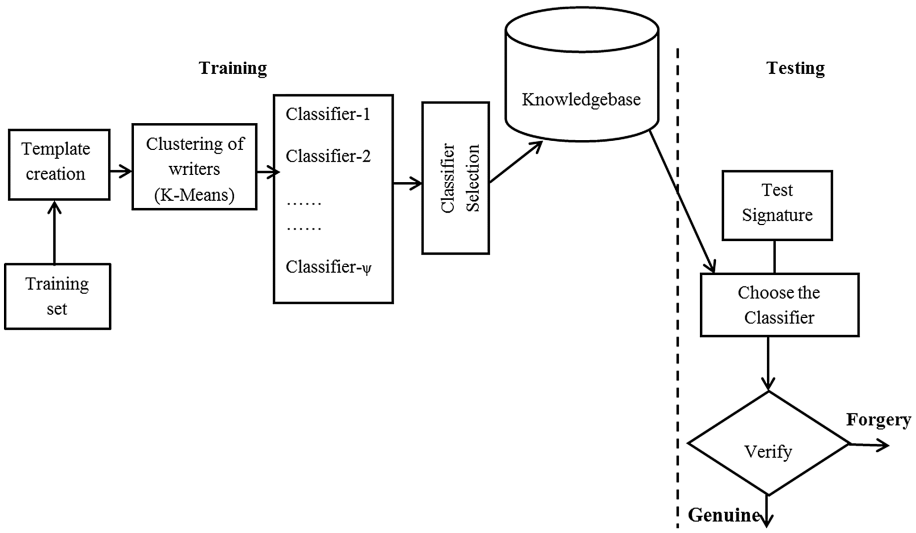

Fig. 1. Architecture of the proposed model

2.1 Template Creation

As we need to create a cluster of writers $W = \{W_1, W_2, W_3, \ldots, W_N\}$ and as we have n number of samples for each writer $W_i = \{S_1^i, S_2^i, S_3^i, \ldots S_n^i\}, 1 \leq i \leq n$, clustering of all writers using all n samples lead to a confusion in understanding to which cluster a writer belong as samples of same writer may belong to different clusters. Hence we intend to create a single template for each writer and then clustering different writers based on the chosen representative of each writer solves the above mentioned problem. Template signature for each writer is created considering n number of samples of each writer. The template signature for i^{th} writer W_i is created as follows.

1. Let $\{s_1, s_2, \ldots, s_n\}$ be the set of n genuine signatures of i^{th} writer available for training purpose.
2. Calculate the pair-wise distance $dist(s_j^i, s_{j'}^i)$ from s_j^i and $s_{j'}^i$ $j = 1, 2, \ldots, n$ and $j' = 1, 2, \ldots, n$, $j \neq j'$.
3. Compute the average distance of each signature $Avg(s_j^i) = \frac{1}{n-1} \sum_{j'=1}^{n} dist(s_j^i, s_{j'}^i)$, $j = 1, 2, \ldots, n$, $j \neq j'$.
4. Template signature of i^{th} writer is selected as a signature s_j^i which has a minimum average distance to other signatures of i^{th} writer and is given by $T_S^i = \min(Avg(S_j^i), j = 1, 2, \ldots, n$.

Similarly, we create template signature for all writers and let $T = \left\{T_S^i, T_S^i, T_S^3, \ldots, T_S^N\right\}$ be the set of template signatures of all N writers and termed as $TemplateSig_{Database}$ which is of size $N \times m$, as we have only template for each writer. These selected templates are stored in the database as representatives.

2.2 Clustering of Writers

Once the template signature database is created, different writers are clustered. The writer belonging to the same clusters have similar characteristics in the feature space. In this work, we have used k-means clustering which is a well-known partitional clustering algorithm widely used in the field of data clustering. The reason for adaption of k-means clustering in our work is due to its ease of implementation, simplicity, efficiency, and empirical success [21]. However any other clustering algorithm can be used for the purpose of clustering writers.

Let $T = \{T_S^1, T_S^2, T_S^3, \ldots, T_S^N\}$ be the $TemplateSig_{Database}$ of N writers where each template signature is represented by m dimensional features. We apply k-means algorithm on this data with a suitable parameter k and the parameter k is selected empirically which is discussed in the experimental section.

Let $CG = \left\{C_1, C_2, \ldots, C_k\right\}$ be k clusters of writers, where $C_i = \left\{T_S^a, T_S^b, \ldots, T_S^l\right\}$ is a cluster containing l number of template signatures of different users obtained by k-means clustering. As each template signature corresponds to a writer, $C_i = \left\{T_S^a, T_S^b, \ldots, T_S^l\right\}$ can be rewritten as $C_i = \left\{W_a^i, W_b^i, \ldots, W_l^i\right\}$ where, W_j^i being the

j^{th} writer of i^{th} cluster. For each writer in each cluster, we identify the suitable classifier and select the classifier for the cluster as discussed in the following subsection.

2.3 Cluster Dependent Classifier Selection

The decision regarding the classifier suitable for a particular cluster is arrived as follows. We have clustered N writers into k clusters i.e., $CG = \{C_1, C_2, \ldots, C_k\}$ and $C_i = \{W_a^i, W_b^i, \ldots, W_l^i\}$, where W_j^i being the j^{th} writer of i^{th} cluster. For each writer in an individual cluster we collect all n number of samples. Out of n number of samples, n_1 samples are used for training purpose and n_2 samples are used for validation. For validation we need forgery samples also and hence we considered n_3 number of forgery samples during validation process.

Let there be ψ number of classifiers. Given a writer W_a^i of i^{th} cluster with n number of samples and m numbers of features, we have a data matrix of size $n \times m$ for i^{th} writer. Out of $n \times m$ data matrix, $n_1 \times m$ is used as training set and trained each of the ψ classifiers. Using $n_2 \times m$ and $n_3 \times m$, False acceptance rate (FAR) and False rejection rate (FRR) are calculated and finally Equal error rate (EER) is obtained for each classifier. Calculation of FAR, FRR and EER is discussed in Sect. 3, that is for i^{th} writer we have

$$E_c = \left\{ EER^i_{C_1}, EER^i_{C_2}, EER^i_{C_3}, \ldots, EER^i_{\psi} \right\} \tag{1}$$

where $EER^i_{C_j}$ refers to EER of C_j^{th} classifier for i^{th} writer.

The experimentation is carried out with X number of trails by changing the training and validation samples. The training and validation samples are randomly selected without overlapping in each of the X trails. In each trial, the classifier with a minimum error rate is selected.

$$\text{i.e } \psi^X_{sel} = \min \{E_c\} \tag{2}$$

Let $\psi_{sel} = \{\psi^1_{sel}, \psi^2_{sel}, \psi^3_{sel}, \ldots, \psi^X_{sel}\}$ be the set of classifiers selected in X different trials, where ψ^p_{sel} is the classifier selected at p^{th} trial. In order to select the best classifier among the ψ_{sel} list, we rank the classifiers based on its frequency of selection for a particular writer as defined in (3).

$$Frequency\ (\psi_j, W_a^i) = \frac{Number\ of\ times\ \psi_j\ is\ selected\ for\ i^{th}\ writer}{Number\ of\ trails\ conducted} \tag{3}$$

The classifier having the highest frequency of selection say ψ_j^{ia} shall be the best classifier for the writer W_a^i of i^{th} cluster. Similarly for all writers in the cluster, the classifier is selected using the above mentioned procedure. The classifier which is selected with the highest frequency is selected as the classifier for all writers belonging to i^{th} cluster. Similarly, for all other clusters, the classifier is selected and the selected

classifier is assigned as best classifier for those writers belonging to that corresponding cluster. In the knowledgebase we store the classifier selected for each cluster and later this will be used in verifications stage. Once the classifier is decided for the entire cluster, we train the system for all writers of that cluster with the selected classifier before the verification stage.

2.4 Signature Verification

During verification, given a test signature S_{test} of a claimed writer i, the genuinity of S_{test} is verified as follows. First identify the cluster label to which the claimed writer i belongs. Once the cluster label is known, the classifier ψ^i suitable for the cluster to which the writer i belong is selected for verification. The given unknown sample S_{test} is fed to the classifier ψ^i and the claimed identity is established as a genuine or a forgery.

3 Experimental Setup

In this section, description of the database used for experimentation along with training and testing details is presented.

Database: We have evaluated the performance of our model on MCYT (DB1), a subcorpus of MCYT dataset, consisting of signatures of 100 writers. MCYT (DB1) contains 50 signature samples of 100 writers. Out of the 50 samples of each writer, 25 are genuine and the remaining 25 are skilled forgery samples. We have considered 100 global features for each writer and complete list of 100 global features can be found in the work of [12].

Experimental Setup: We conducted experimentation under two different training conditions (a) with 05 genuine signatures (b) with 20 genuine signatures. The reason for selecting 05 and 20 genuine signatures for training is to compare our model with other existing models for online signature verification. We conducted verification experiments with both skilled and random forgeries. Skilled forgery is nothing but the forgery created by professional forgers with sufficient practice and random forgery is nothing but the genuine signature of other writers. In case of testing with skilled forgery, all the remaining genuine signatures and all the 25 skilled forgeries are used for calculating FRR and FAR respectively. These two categories of testing are mentioned as Skilled_05 and Skilled_20 respectively. Similarly in case of testing with random forgery, all the remaining genuine signatures and one signature from every other writer is used for estimating FRR and FAR respectively. These two categories of testing are mentioned as Random_05 and Random_20 respectively. To fix-up the classifier for each cluster, the training set is further divided into training and validation set. Based on the error rate obtained with validation set, the classifier for each cluster is decided. For validation purpose, we have considered 50% of the available genuine signatures and equal number of random forgeries.

After creating a representative for each writer and clustering of writers as discussed in Sects. 2.1 and 2.2, we estimate the FAR, FRR and EER for each writer resulting from each of the available classifiers. For each writer, the classifier which resulted in lowest EER is considered as the suitable classifier for that writer. Finally, the classifier which has been selected for majority of writers in each cluster is decided as the suitable classifier for the entire cluster. Once the classifier for all clusters are fixed up, we test the performance of the system on the unseen test data. The resulting FAR, FRR and EER obtained with test sample is reported as the error rate of the system. We conducted experimentations with different number of clusters varying from 5 to 10. In this work, for classifier selection, we have considered 06 different classifiers namely Naïve Bayesian (NB), Nearest neighbor (NN), Support vector machine (SVM), Probabilistic neural network (PNN), Fisher Linear discriminating analysis (FLD) Principal component analysis (PCA) classifier which are widely used in the field of pattern recognition.

4 Experimental Results

We conducted 10 different trials by randomly selecting training and testing samples in each trial to measure the performance of the system. In this work we used FAR, FRR and EER as the performance measures which are generally used for measuring the performance level of a biometric system. The EER obtained for different categories of testing with the proposed model is given in Table 1.

Table 1. EER of the proposed model under varying number of clusters for different categories of testing

No. of clusters	Skilled_05	Skilled_20	Random_05	Random_20
5	13.10	1.00	9.21	0.40
6	13.00	1.10	7.60	0.40
7	12.83	1.00	7.95	0.40
8	12.60	1.20	6.52	0.40
9	12.69	1.20	8.03	0.40
10	12.75	1.20	8.13	0.40

Further to demonstrate the superiority of cluster dependent classifier over a common classifier, we also conducted experiments without any classifier selection. In this case, the same classifier has been used for all writers. Result obtained with the usage of common classifier for all writers is shown in Table 2. From Table 2, it can be deduced that, usage of a common classifier results in higher EER compared to cluster dependent

classifier thereby establishing the superiority of the proposed model. In Table 2, the labels C_1, C_2, C_3, C_4, C_5 and C_6 denote the classifier NB, NN, SVM, PNN, FLD and PCA respectively. For instance, the row corresponding to C_1 denote the EER obtained when the NB classifier is used.

Table 2. EER with the usage of common classifiers for different categories of testing

Classifier Label	Skilled_05	Skilled_20	Random_05	Random_20
C_1	27.21	6.00	27.50	7.60
C_2	13.19	1.40	8.27	0.60
C_3	13.27	1.25	8.19	0.60
C_4	16.89	13.60	14.24	14.00
C_5	14.40	3.90	11.11	2.20
C_6	12.90	1.50	8.31	0.60

5 Comparative Study

In this section we present a comparative analysis of the proposed model with other existing models for online signature verification. It is well known that comparing different verification models is challenging due to change in the dataset used for experimentation, features used, training and testing size. To have a fair comparison, we have taken into consideration other models which have used MCYT (DB1). In Table 3, we compare the EER of our model with other existing models for online signature verification models. From Table 3, it is clear that, none of the individual models got lowest EER for all four categories of testing. Our model outperforms all other models in case of Skilled_20 and Random_20. Generally a writer dependent model required more training samples for capturing the characteristics of individual writer [18]. In case of skilled_05 and random_05 since only 05 signatures are available for training purpose, the error rate we achieved is high compared to other models. All other models mentioned in Table 3 are writer independent models. Even in case of Skilled_05, the EER that we achieved is lower than the EER of BASE model [15], cluster based symbolic model [19] and forgery quality estimation model with GMM [22]. In case of Random_05, the EER of our model is lower than the EER of NND classifier model [14] and BASE model [15]. In Table 3, for some categories of testing, the respective authors have not quoted the result and hence the corresponding entries are left blank.

Table 3. Comparative analysis of various online signature verification models based on EER

Model	Skilled_05	Skilled_20	Random_05	Random_20
Proposed model	12.6	1.0	6.5	0.4
Single class classifier Model [14]				
a. Parzen Window Classifier (PWC)	9.7	5.2	3.4	1.4
b. Nearest Neighbour descriptor (NND)	12.2	6.3	6.9	2.1
c. Mixture of Gaussian Description(MOGD_3)	8.9	7.3	5.4	4.3
d. Mixture of Gaussian Description (MOGD_2)	8.1	7.0	5.4	4.3
e. Support Vector Descriptor	8.9	5.4	3.8	1.6
Two class classifier model [15]				
a. BASE	17.0		8.3	
b. KHA c. Random subspace(RS) d. Random subspace with ensemble (RSB) e. Fusion of RSB+KHA	11.3 9.0 9.0 7.6		5.8 5.3 5.0 2.3	
Symbolic classifier [11]	5.8	3.8	1.9	1.7
Cluster based symbolic classifier [19]	15.4	4.2	3.6	1.2
Forgery quality estimation model [22]				
a. DTW	6.5			
b. HMM	11.5			
c. Gaussian Mixture Model (GMM)	17.7			

6 Conclusion

In this work, we have made a successful attempt on the introduction of notion of cluster dependent classifier for online signature verification. Our intuition is to recommend a suitable classifier only for those writers with similar characteristics and a different classifier for writers of different characteristics. We have clustered representatives of each writer obtained from the training sample for recommending a suitable classifier for each cluster. The outcome of the proposed model outperforms existing state of the art works reported in literature for online signature verification in achieving lowest EER for a large training size.

Acknowledgement. The authors would like to thank J.F. Aguilar and J.O. Garcia for sharing MCYT-100, a sub corpus of online signature data set and thanks to Prof. Anil K. Jain for his associated support to get the dataset.

References

1. Plamondon, R., Lorette, G.: Automatic signature verification and writer identification: the state of the art. Pattern Recogn. **2**(2), 107–131 (1989)
2. Jain, A.K., Griess, F.D., Connell, S.D.: On-line signature verification. Pattern Recogn. **35**(12), 2963–2972 (2002)
3. Impedovo, D., Pirlo, G.: Automatic signature verification: the state of the art. IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. **38**(5), 609–635 (2008)
4. Zhang, Z., Wang, K., Wang, Y.: A survey of on-line signature verification. In: Sun, Z., Lai, J., Chen, X., Tan, T. (eds.) CCBR 2011. LNCS, vol. 7098, pp. 141–149. Springer, Heidelberg (2011)
5. Khan, M.K., Khan, M.A., Khan, U., Ahmad, I.: On-line signature verification by exploiting inter-feature dependencies. In: Proceedings of the ICPR, pp. 796–799 (2006)
6. Fierrez, J., Garcia, J.O., Ramos, D., Rodriguez, J.G.: HMM-based on-line signature verification: feature extraction and signature modeling. Pattern Recogn. Lett. **28**(16), 2325–2334 (2007)
7. Zou, J., Wang, Z.: Application of HMM to online signature verification based on segment differences. In: Sun, Z., Shan, S., Yang, G., Zhou, J., Wang, Y., Yin, Y. (eds.) CCBR 2013. LNCS, vol. 8232, pp. 425–432. Springer, Heidelberg (2013)
8. Parodi, M., Gómez, J.C.: Legendre polynomials based feature extraction for online signature verification. Consistency analysis of feature combinations. Pattern Recogn. **47**, 128–140 (2014)
9. Meshoul, S., Batouche, M.: A novel approach for Online signature verification using fisher based probabilistic neural network. In: IEEE International Symposium on Computers and Communications (ISCC), pp. 314–319 (2010)
10. Muramatsu, M., Kondo, M., Sasaki, M., Tachibana, S., Matsumoto, T.: A markov chain monte carlo algorithm for bayesian dynamic signature verification. IEEE Trans. Inf. Forensics Secur. **1**(1), 22–34 (2006)
11. Guru, D.S., Prakash, H.N.: Online signature verification and recognition: An approach based on Symbolic representation. IEEE Trans. Pattern Anal. Mach. Intell. **31**(6), 1059–1073 (2009)
12. Fiérrez-Aguilar, J., Nanni, L., Lopez-Peñalba, J., Ortega-Garcia, J., Maltoni, D.: An on-line signature verification system based on fusion of local and global information. In: Kanade, T., Jain, A., Ratha, N.K. (eds.) AVBPA 2005. LNCS, vol. 3546, pp. 523–532. Springer, Heidelberg (2005)
13. Nanni, L., Majorana, E., Lumini, A., Campisi, P.: Combining local, regional and global matchers for a template protected on-line signature verification system. Expert Syst. Appl. **37**(5), 3676–3684 (2010)
14. Nanni, L.: Experimental comparison of one-class classifiers for on-line signature verification. Neurocomputing **69**(7–9), 869–873 (2006)
15. Nanni, L., Lumini, A.: Advanced methods for two-class problem formulation for on-line signature verification. Neurocomputing **69**, 854–857 (2006)
16. Pirlo, G., Cuccovillo, V., Impedovo, D., Mignone, P.: On-line signature verification by multi-domain classification. In: 14th International Conference on Frontiers in Handwriting Recognition (ICFHR), pp. 67–72 (2014)
17. Fiérrez-Aguilar, J., Krawczyk, S., Ortega-Garcia, J., Jain, A.K.: Fusion of local and regional approaches for on-line signature verification. In: Li, S.Z., Sun, Z., Tan, T., Pankanti, S., Chollet, G., Zhang, D. (eds.) IWBRS 2005. LNCS, vol. 3781, pp. 188–196. Springer, Heidelberg (2005)

18. Eskander, G.S., Sabourin, R., Granger, E.: Hybrid writer-independent–writer-dependent offline signature verification system. IET Biometrics **2**(4), 169–181 (2013)
19. Guru, D.S., Prakash, H.N., Manjunath, S.: On-line signature verification: an approach based on cluster representation of global features. In: International conference on Advances in Pattern Recognition (ICAPR), pp. 209–212 (2009)
20. Liu, N., Wang, Y.: Template selection for on-line signature verification. In: 19th International Conference on Pattern Recognition (ICPR), pp. 1–4 (2008)
21. Jain, A.K.: Data clustering: 50 years beyond K-means. Pattern Recogn. Lett. **31**(8), 651–666 (2010)
22. Houmani, N., Salicetti, S.G., Dorrizi, B.: On measuring forgery quality in online signatures. Pattern Recogn. **45**(3), 1004–1018 (2012)