Hybrid Model with Fusion Approach to Enhance the Efficiency of Keystroke Dynamics Authentication

Ramu Thanganayagam and Arivoli Thangadurai

Abstract We propose in this paper a novel technique to enhance the performance of keystroke dynamic authentication using hybrid model with four fusion approach. Firstly, extract keystroke features from our database. Then generate template from extracted features, which is compact form of keystroke feature data. Hybrid model based on combination of Gaussian probability density function (GPDF) and Support Vector Machine (SVM) will convert test features into scores. At last, applied four fusion rules on hybrid model to fusing GPDF and SVM scores to improve the final result. Experimental results show that the performance of the proposed hybrid model can bring obvious improvement with error rate of 1.612 %.

Keywords Hybrid model · Biometric · Keystroke dynamic authentication and fusion approach

1 Introduction

Traditional authentication system using passwords, personal cards and PIN-numbers can easily be breached when a card is stolen or password is compromised. Furthermore, difficult passwords may be hard to remember by a legitimate user and simple passwords are easy to guess by an impostor. The use of biometrics offers an alternative means of identification which helps avoid the problems associated with conventional methods. Nowadays, losses due to identity theft is an issue of growing concern, especially considering the increased data exposure caused by some services on the Internet. In view of this scenario, there is a

R. Thanganayagam (✉)
Department of ECE, Kalasalingam University, Krishnankoil, India
e-mail: loginworld34@hotmail.com

A. Thangadurai
Department of ECE, Vickram College of Engineering, Arasanoor, India
e-mail: t.arivoli@gmail.com

A. Nagar et al. (eds.), *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics*, Smart Innovation, Systems and Technologies 43, DOI 10.1007/978-81-322-2538-6_10

need for enhanced authentication mechanisms, such as by the use of biometrics. In security area, biometrics tries to recognize users by physiological or behavioral features of the person. Among the current biometric technologies, keystroke dynamics is a promising alternative due to several factors [1, 2]. First, it usually does not need any additional cost with hardware, as a common keyboard is enough to acquire keystroke data. Second, keystroke dynamics recognition may be performed in background, while the user is typing an e-mail or entering a password. Consequently, day-to-day tasks of users are not disturbed, which may contribute to a better acceptability of this technology. Keystroke dynamic is a type of behavioral biometrics based on the users typing rhythm, which is unique for different people. Keystroke timing patterns are captured without users knowledge based on the keystroke events gathered while users typing on a keyboard.

1.1 Motivation and Contribution

Password based authentication is not secure due to several drawbacks [3]:

1. Someone stolen the password
2. Brute force attack (try all possible combination of start with one digit, two digit passwords and so on)
3. Dictionary attack (try with list of password in the dictionary instead of all possible combination)
4. Password guessed (if someone look over while type or note it down on paper if password is difficult to remember)
5. User shared password to others
6. Someone hacked the password.

To overcome the above drawbacks, introduced keystroke dynamic is an additional parameter to secure password authentication. Keystroke dynamic analyze the users way of typing on keyboard that is typing pattern and it measures the time interval between each events of user holding the key and switchover between the key (one key to another key). Individual keystroke pattern or features are different, so it is maintain consistency and uniqueness. We study different types of keystroke features and analyze the performance of individual and combination of features. We propose a Hybrid model with different fusion approach to combine the scores from Gaussian probability density function (GPDF) and support vector machine (SVM) with combination of feature data. The following contributions has been done:

- Created keystroke database of 100 users
- Extract four types of keystroke features and analyze the performance
- Keystroke feature data transform to scores using hybrid model
- The efficient combination of four fusion approach
- Evaluate Equal error rate (EER).

1.2 Organization

The rest of paper is organized in the following way: Sect. 2 discussed the review of related research in the field while Sect. 3 presents the proposed methodology, data collection, feature extraction and template generation. Section 4 presents our proposed hybrid model and Sect. 5 presents proposed fusion approach. The experimental results analyzed and discussed in Sect. 6. Finally, Sect. 7 provides conclusions.

2 Related Works

Recent years, researchers were focusing on the collection of number of users keystroke biometric data for accurate evaluation on user database benchmark, decreasing the evaluated result errors or improve accuracy and concentrating keystroke latency as feature data. Hosseinzadeh et al. [4] conducted experiment on keystroke authentication using Gaussian Mixture Model. Training and testing data were collected from 8 users who typed their full name consecutively ten times No complexity pattern involved in the name characters due to smaller character length, so it can be easily replicated. Experiment was utilized only two extracted keystroke features and Expectation Maximization algorithm used to train the Gaussian Mixture Model. Then, Log-likelihood test platform was performed to identify the probability of closest data of testing and training data to confirm genuine user authentication. Overall experiment result is 2.4 % FRR and 2.1 % FRR, this error rate is high and also the number of users tested is not enough to conclude the final results obtained. Sang and Shen et al. [5] authors were implemented SVM classifier in the keystroke dynamics. Keystroke data collected from ten users. Experiment was performed on one class SVM which is simulating genuine data and two-class SVM is used to separate genuine and imposters' data. The results are reliable but significant weakness is only ten samples were collected. In [6] authors have implemented Hidden Markov Models as classifier in keystroke recognition. Twenty people were enrolled to this experiment with their password ten times in four different sessions. However, lower length of eight digit password implemented. A total of 800 samples collected which is enough for the experiment. The final result of EER is 3.6 % which is considerably higher error rate. Guven et al. [7] proposed new classifier for keystroke authentication. New classifier is similar to neural network structure. Keystroke raw data was collected from sixteen users, then extracted the keystroke latency (successive key press or down). Experiment was conducted on similar to neural network structure to calculate the weights using statistical method. Statistical method include mean and standard deviation of the keystroke latencies. User test sample latency value was compared to standard deviation of reference latency, result is genuine if test latency fall two times within the standard deviation reference latency, then assume whole string being considered as valid. Due to assumption, experiment produced result with high error rate of FRR of 17 % and FAR of 26 % which was poor performance of keystroke authentication. Azevedo et al. [8] developed hybrid system based on the combination of stochastic optimization algorithm (Genetic algorithm) and support vector machine (SVM) and particle swarm optimization. Hybrid system select the keystroke features from enrolled users. Experiment was implemented on SVM uses a Genetic algorithm and particle swarm optimization. First test was conducted on SVM with Genetic algorithm (evolutionary algorithm) for feature selection with minimum error rate of 5.18 % when FAR of 0.43 % and FRR of 4.75 %. Second test was carried on particle swarm optimization with global acceleration of 1.5 gave a minimum total error of 2.21 % with error rate of 0.41 % FRR and 2.07 % FAR. This paper, proposed hybrid model with different fusion approach which is merge the scores produced by the GPDF and SVM. This approach is able to considerably improve the overall result.

3 Proposed Methodology

We introduce hybrid model in this research, which are the combination of two matching function namely the Gaussian Probability Density Function (GPDF) and Support vector machine (SVM). Figure 1 shows proposed hybrid model with two keystroke features combined and applied fusion rules against the combinations performed on SVM and GPDF. Hybrid model is developed to calculate the score between the test user templates against the reference user template (stored in database). Then, fusion applied for both SVM and GPDF matching scores. The function of fusion is fusing both matching scores and then fused output score is compared with a predefined threshold before making a final decision. The decision should be accepted if fusion output score is greater than threshold value or else rejected the user authentication. In this paper, four fusion rules are studied.

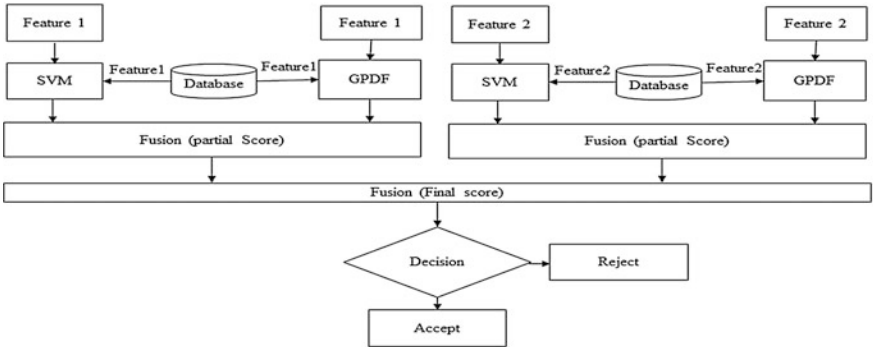

Fig. 1 Proposed hybrid model with two keystroke features

3.1 Data Collection

Captured keystroke biometric data with the help of GREYC Keystroke software developed at GREYC Laboratory [9]. This software is downloadable from the following address www.ecole.ensicaen.fr/~rosenber/keystroke.html. 100 users' data was collected with an interval of 6 months apart. These users are university academic and administrative staffs. Initially, each user is allowed to choose their choice of username and password during the enrolment process. Next, same users have to continuously type fixed line of text "credential evaluation" for fifteen times. So we collect fifteen samples of each user and total of 1500 (100 user * 15) samples are stored in the database.

3.2 Feature Extraction and Template Generation

When user type a character on keyboard, two types of events occurred namely, key press (P) and key release (R). Based on occurrence of specific events, we can extract keystroke feature data. Four types of keystroke features could be generated [10] as shown Fig. 2. Extracted four features: (Press-to-Release PR = $R_1 - P_1$) the time between a key being pressed until the key being released, (Press-to-Press PP = $P_2 - P_1$) time between two successive keys being pressed, (Release-to-Press RP = $P_2 - R_1$) time between a key being released to the next key being pressed and (Release-to-Release RR = $R_2 - R_1$) the time between two successive keys being released. RP feature value may occur negative due to next key being pressed before

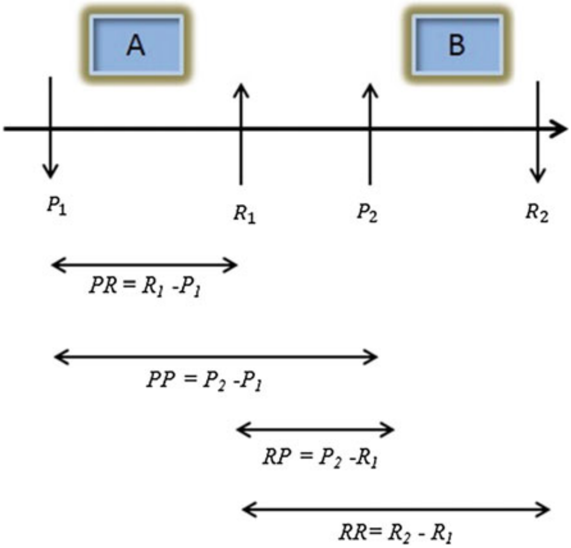

Fig. 2 Four keystroke features extracted from phrase "AB"

previous key being released. Template generation is the compact form of four keystroke features, which is extracted from raw keystroke data. Each user keystroke data could be converted to one template which consists four types of features of their mean and standard deviation of keystroke feature of each character of fixed phrase text. User templates are stored in database and could be retrieved for authentication purpose. The formula of mean (μ) and standard deviation (σ) as below,

$$\mu = \frac{1}{T} * \sum_{j=1}^{T} t_j \quad and\ \sigma = \sqrt{\frac{\sum_{j=1}^{T} \left(t_j - \mu\right)^2}{T}} \tag{1}$$

where T represents the number of training samples and t_j denotes the value of each keystroke feature. The user is required to continuously type fixed phrase text “credential evaluation” for 15 times which yields fifteen samples from each user. Testing purpose, randomly divide fifteen samples of each user into five and ten whereas five samples are converted to templates serves as reference for future authentication and ten samples reserved for testing purpose. Generated five templates are stored in the database for comparison while test user authentication.

4 Hybrid Model

Hybrid model have two matchers namely, GPDF and SVM. Test and reference feature data will be converted into individual template. Each template consists four types of features (PR, PP, RP, RR) of their mean and standard deviation of keystroke feature of each character of fixed phrase text. We use both template of two different combination of features (example: PR and RP) fetch into hybrid model which consists of: (1) GPDF used to compute the score between test feature template and reference feature template. (2) SVM used to compare the scores of each typing patterns of test feature template and reference feature template to identify genuine or imposter data. Two matcher scores are in the range of 0 to 1. Then apply fusion to two matcher output scores, get the final score which will decide the genuine or imposter user.

4.1 Gaussian (Normal) Probability Density Function (GPDF)

GPDF [11, 12] is used to analyze the data. It represents the normally distributed data in the bell shaped curve with mean value is the centroid and variance is a measure of dispersion of data around mean. This paper, GPDF is used to calculate the matching score between user test feature data template and reference feature data template. Matching score between the ranges of 0 to 1. GPDF modified form as below

$$Score_{GPDF} = \sum_{i=1}^{N} \exp\left[-\frac{(n-\mu)^2}{2\sigma^2}\right] \tag{2}$$

where $Score_{GPDF}$ represents the GPDF matching score, n denotes the test keystroke feature of a particular character, μ and σ^2 denotes the mean and variance of each character from reference feature data, respectively. Calculate the matching score between two templates of test and reference data by apply variance and mean of reference data and test data into the Eq. (2). Eventually decide the final result of matching score if closer to 1, then reference feature data template and test feature data template are similar. Now the test was conducted for one feature of the template, the matching score named as sub score. Same experiment should be performed for all four features of the template, eventually final score has been calculated with average of all sub scores.

4.2 Support Vector Machine (SVM)

SVM is to compare the scores of each typing patterns of training data samples and test data samples for identifying authorized and unauthorized user. We have done experiment on linear version of SVM which maps the input user data into a high dimensional feature space through linear kernel. Detail description of SVM can be found in [13]. SVM is the determination of the optimal hyper plane which will optimally separate the two classes of genuine and imposter of input user dataset. Based on linear kernel function, SVM maps the input user dataset samples in a high-dimensional feature space and then separate the dataset from the origin with a maximum margin. SVM algorithm function *f* is defined as the region that majority of data from input dataset which contained in one pattern (genuine) as +1, and data outside this region is −1 (imposter), function *f*(*x*) as below

$$f(x) = \sum_{i}^{N} \alpha_i y_i K(x_i, x) + b \tag{3}$$

where N represents the size of training data and x_i denotes the supporting vector. $K(x_i, x)$ is the kernel function representing the inner product between x_i and x in feature space. To maximize the margin that is distance between the nearest point of the training set and the hyper plane is called optimization problem. It could be solved can be stated as

$$\max_{\alpha_i \geq 0} \sum_i \alpha_i - \frac{1}{2}\sum_{j,k} \alpha_j \alpha_k y_j y_k K(x_j, x_k), \quad 0 \leq \alpha_i \leq C \; for \; \forall_i \quad and \; \sum_i \alpha_i y_i = 0 \quad (4)$$

where C denotes the penalization coefficient of data points on hyper plane. Based on C value to set the width of margin between data points in the middle of the hyper plane. In order to maximize the performance, we have set the values for the parameter C = 128.

5 Fusion Approach

Four fusion rules were applied in the hybrid model fusion approach. Table 1 shows formula of four fusion rules namely sum, weighted sum, product and maximum. Hybrid model have two matcher of SVM and GPDF whose output range is 0 to 1, so score normalization is not necessary before fetching to next process of fusion. Fusion helps to combine the significant information of SVM and GPDF, so it could increase the overall performance. Reason to employ fusion method to improve the performance significantly. In this research, we propose fusion to hybrid model that is fusing between SVM and GPDF scores to produce a final score. At last, fusion score will decide the user is genuine or imposter.

6 Experimental Results and Discussions

6.1 Experimental Setup

Our experiments were performed with fixed phrase text of users keystroke data. Collected the raw data of 15 samples from 100 users. Extracted four different keystroke features (PR, PP, RP, and RR) from 100 users raw data. Then, template could be generated based on extracted four keystroke features with calculated their mean and standard deviation for each and every character of the user typed. Each user data consists of four different templates. Testing purpose, randomly divide fifteen samples of each user into five and ten whereas five samples are converted to templates named as training samples and ten samples reserved for testing purpose

Table 1 Various fusion rules

Fusion rule	Formula
Sum	$Score_{SUM} = \frac{Score_{SVM}+Score_{GPDF}}{2}$
Weighted sum	$\text{Score}_{\text{Wsum}} = \text{W}_1\text{Score}_{\text{SVM}} + \text{W}_2\text{Score}_{\text{GPDF}}$
Product	$Score_{product} = \frac{Score_{SVM}Score_{GPDF}}{2}$
Max	$Score_{Max} = MAX(Score_{SVM}, Score_{GPDF})$

named as testing samples. Experiment was carried on all sets of users' templates with five training samples versus ten testing samples. Error rates could be calculated as false rejection rate and false acceptance rate. The false rejection rate (FRR) is the ratio of genuine user rejected and the total number of user samples attempted. The false acceptance rate (FAR) is the ratio of approved imposters as genuine users and the total number of user samples attempted. The experiment was carried by comparing the test data sample score against threshold value within the range of 0 to 1 (interval of 0.01), calculate FAR and FRR. Repeated the experiment with increase the interval each time 0.01, calculated the FAR, FRR values. After tabulation of FAR and FRR values, equal error rate (EER) is calculated when FAR is near to FRR value. Tested fifteen different combinations with five training data and ten testing data. For each combination of sample data, we have obtained final results could be the average of EER. Experimental results discussed for the next section could be described with the average value of EER, FAR and FRR.

7 Results

7.1 Keystroke Features Without Fusion

This approach, each keystroke features (PR, PP, RP, and RR) have been applied on matcher SVM and GPDF without using any fusion approaches. Observing the performance of four keystroke features on SVM and GPDF in Fig. 3 we notice that feature PR is obtained better result compared to other keystroke features (PP, RP, RR). Observing the EER % of four keystroke features without fusion in Table 2 we notice that PR feature lead the best result of 3.8214 EER % while using SVM. SVM results of all four keystroke features are better than GPDF results. Apart from that we performed this experiment with 100 user samples even though the result remains consistent.

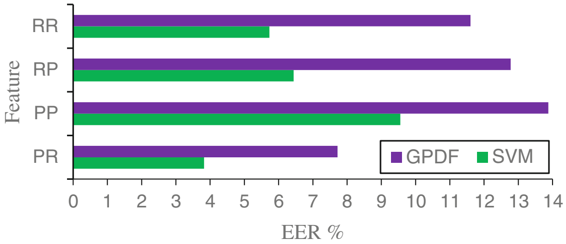

Fig. 3 Performance comparison of four keystroke features without fusion

Table 2 EER % of four features on SVM and GPDF without fusion

Method	PR	PP	RP	RR
SVM	3.8214	9.5531	6.4372	5.7315
GPDF	7.7199	13.875	12.776	11.602

7.2 Hybrid Model with Fusion Approach

We proposed, hybrid model using combination of two keystroke features with four fusion approach. Initially, two keystroke features have been applied on two matcher SVM and GPDF, output scores of each matcher named partial score. Then partial score fused with four fusion rules namely sum, weighted sum, product and maximum. Each fusion rules were applied separately to partial score and analyzed the output score shown in Fig. 4. This testing was repeated with all possible combination of two keystroke features and also repeated with different fusion rules. Eventually fused output score is compared with a predefined threshold before making a final decision. The final decision should be accepted if the score is greater than threshold value or else rejected. Experiment results shown in Table 3 we noticed that PR+RP feature combination with weighted sum fusion rule produced the best result of 1.612 % EER among other feature combination. PR feature combination with any other three features provided better results compared to without PR of remaining feature combination. Noticing that the performance improvement on fusion approach than the without fusion approach on individual feature. Observed the better results of two combination features than single keystroke feature used in without fusion

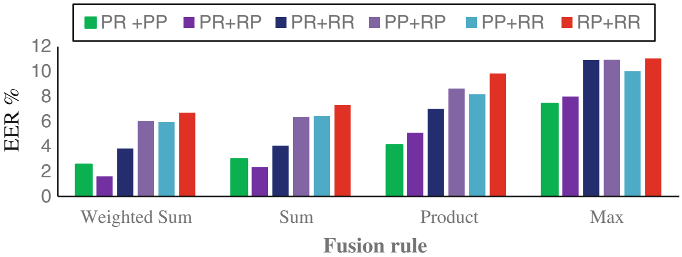

Fig. 4 Performance comparison of hybrid model with four fusion rules

Table 3 EER % of four fusion rules

EER %						
Fusion rule	PR+PP	PR+RP	PR+RR	PP+RP	PP+RR	RP+RR
Weighted sum	2.57	1.612	3.842	6.043	5.961	6.714
Sum	3.015	2.36	4.074	6.341	6.432	7.315
Product	4.124	5.112	7.031	8.64	8.184	9.842
Max	7.443	8.004	10.921	10.944	10.03	11.054

approach. Among the combination of features used in hybrid model with various fusion rule, weighted sum rule shown better results than the other fusion rule. Among the four fusion rules, weighted sum rule results are better and worst results obtained on max rule. Analyzed the major performance difference between weighted sum and max rule, scenario of max rule final output is the maximum probability output between two matchers that is best among the two matcher scores and discard the even small point difference score value of one matcher but weighted sum rule utilize both matcher scores with weighted value. Therefore, weighted sum rule have imposter acceptance is very less, so overall performance is high. Best equal error rate obtained among all four fusion rule is weighted sum rule at 1.612 %. At the experimental stage, weighted sum fusion rule was tested with bias weight of $W_{1ScoreSVM}$ and $\mathrm{W}_{\mathrm{1ScoreGPDF}}$ in the range starting from 0 with step size 0.1 till 1 value, observed the best result obtained at bias value of $\mathrm{W}_{\mathrm{1ScoreSVM}} = 0.73$ and $\mathrm{W}_{\mathrm{2ScoreGPDF}} = 0.27$. Weighted sum rule performs better than sum and product rule due to the setting of bias weight. Overall observation, two keystroke feature combination enhance the performance using weighted fusion rules on hybrid model than individual features used on without fusion method.

8 Conclusions

In light of the current need for enhanced authentication mechanisms, keystroke dynamics shows as a promising alternative. We discussed a promising method for the performance enhancement of keystroke dynamic authentication using hybrid model with four fusion approach. We showed the two keystroke features using hybrid model with four fusion approach to improve the efficiency of a keystroke dynamic authentication system. We described that hybrid model by fusing the scores from two matchers of SVM and GPDF, the result can be improved significantly than using them individually. We showed in our experiment that using two keystroke features combination is able to provide best result than individual keystroke features. The experimental results showed that proposed hybrid model with weighted sum rule using two keystroke feature combination is able to obtain better result of 1.612 % of EER, due to fusion approach helps to increase the performance.

References

1. Hosseinzadeh, D., Krishnan, S.: Gaussian mixture modeling of keystroke patterns for biometric applications. IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. **38**(6), 816–826 (2008)
2. Peacock, A., Ke, X., Wilkerson, M.: Typing patterns: A key to user identification. IEEE Secur. Priv. **2**(5), 40–47 (2004)
3. Sasse, M., Brostoff, S., Weirich, D.: Transforming the ‘weakest link’ a human/computer interaction approach to usable and effective security. BT Technol. J. **19**(3), 122–131 (2001)

4. Hosseinzadeh, D., Krishnan, S., Khademi, A.: Keystroke identification based on Gaussian mixture models. In: Proceedings IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), vol. 3, pp. 1144–1147 (2006)
5. Sang, Y., Shen, H., Fan, P.: Novel impostors' detection in keystroke dynamics by support vector machine. In: Parallel and Distributed Computing: Applications and Technologies, pp. 666–669. Springer (2005)
6. Rodrigues, R.N., Yared, G.F.G.: Biometric access control through numerical keyboards based on keystroke dynamics. In: Zhang, D., Jain, A.K. (eds.) International Conference of Biometrics (ICB 2006), LNCS 3832, pp. 640–646 (2005)
7. Guven, O., Akyokus, S., Uysal, M., Guven, A.: Enhanced password authentication through keystroke typing characteristics. In: Proceedings of 25th IASTED international multi-conference: artificial intelligence and applications, Innsbruck, Austria, pp. 317–322 (2007)
8. Azevedo, G., Cavalcanti, G., Filho, E.C.: Hybrid solution for the feature selection in personal identification problems through keystroke dynamics. In: International Joint Conference on Neural Networks, pp. 1947–1952 (2007)
9. Giot, R., El-Abed, M., Rosenberger, C.: GREYC keystroke: a benchmark for keystroke dynamics biometric systems. In: IEEE 3rd International Conference on Biometrics, pp. 1–6 (2009)
10. Ramu, T., Arivoli, T.: A Framework of secure biometric based online exam authentication: an alternative to traditional exam. IJSER **4**(11), 52–60 (2013)
11. Archambeau, C., Valle, M., Assenza, A., Verleysen, M.: Assessment of probability density estimation methods: Parzen window and finite gaussian mixtures. ISCAS, pp. 3245–3248 (2006)
12. Parzen, E.: On estimation of a probability density function and mode. Ann. Math. Stat. **33**, 1065–1076 (1962)
13. Tax, D.M.J., Duin, R.P.W.: Support vector data description. Mach. Learn. **54**, 45–66 (2004)