

# Recognizing Online Digital Signatures Using Kernel Based Classification Techniques

Ravi Chakravarthi (✉ [ravichakravarthipapers123@gmail.com](mailto:ravichakravarthipapers123@gmail.com))

Al Musanna College of Technology: University of Technology and Applied Sciences - Al Musannah

Anna Palagan C

Teegala Krishna Reddy College of Engineering and Technology

Ravindra Ratilal Dharamshi

University of Nizwa

Anand J Dhas

Rohini College of Engineering and Technology

Shrikant Taware

Al Musanna College of Technology

Ahilan Appathurai

PSN College of Engineering and Technology

---

## Research Article

**Keywords:** Project Registration System (PRS), online digital signature, authentication, classification techniques.

**Posted Date:** October 21st, 2021

**DOI:** <https://doi.org/10.21203/rs.3.rs-945090/v1>

**License:**   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

---

# Abstract

In recent education system, project submission is crucial for college students to complete their respective studies. The understudies needed to propose their undertaking before finishing the pre-last year. One of the critical assessment forms like course Project Registration System (PRS) helps the students and their education board to enhance the knowledge and skill level required for competitive world. PRS is the efficient methods to authenticate the proposal utilizing the online digital signature recognition criteria. During project submission, authentication is important to prevent the unauthorized submission of proposal and contrast the signature utilizing classification techniques such as Kernel Based Artificial Neural Network (K-ANN), Kernel Based K-Nearest Neighbor (K-KNN), Kernel Based Self Organizing Map (K-SOM) and Kernel based Support Vector Machine (K-SVM). The prime objectives of this research work was to recognize the genuine online digital signatures from the assortment of genuine, skilled, unskilled and random types of forged signatures by using the dynamic features like pen pressure, altitude, velocity, azimuth and duration taken by the legitimate person for signing using the proposed K-SVM classification techniques. The data collection based on online digital signature with various students and the proposed classification techniques gives better performance and accuracy compared with other techniques.

## 1 Introduction

Now-a-days, online digital signature recognition was being considered as one of the authenticating criteria to evaluate the e-documents [1]. Also, in present education system, there exist a number of student's evaluation criteria [2]. Computerized marks are frequently used to actualize electronic signatures, a more extensive term that alludes to any electronic information that conveys the goal of a mark, however not every single electronic mark utilize advanced marks [3]. One of the majority important valuation processes such as PRS that helps the students to increase their knowledge based skills [4]. The benefits of utilizing such a validation procedures are signatures are broadly acknowledged by society as a type of recognizable proof and check [5]. Data required isn't delicate. In light of this instructive framework, the vast majority of the last year students need to enroll [6] and complete their examinations with course-ventures. The understudies needed to propose their undertaking before finishing the pre-last year [7]. These are the current issues in the current instructive framework. Along these lines, PRS was utilized to take care of the issues at the period [7] of apportioning the ventures [8]. This framework empowers the understudies to enroll him or [8] her in course venture and present their proposition for assessment [9]. In addition, PRS is utilized to approve and verify the activities by assessing the understudies' proposition and its originator.

Among the approaches, PRS is used to authentic the project proposal and identifying the genuine signatures from the forged signatures. A few literatures have been proposed in the literature survey for online digital signature is classified based on four classification techniques such as K-ANN, K-KNN, K-SOM and K-SVM. This section describes the signature prediction with threshold value and finds the genuine signatures with the given efficient techniques.

## 2 Literature Review

Heckerth, Jonathan et al 2017 [10] had proposed the distinction among credible and mimicked electronic signatures were assessed the capacity of Forensic Handwriting Examiners (FHEs). They analyzed the genuineness of electronic signatures caught with programming by signotec on a Smartphone Galaxy Note 4 by Samsung and marks made with a ballpoint pen on paper for sixty-six expert FHEs. At long last, the investigation results could have been impacted because of the altering of test marks, which two gatherings of FHEs got for looking at addressed normal simulations.

Houmani, Nesma et al 2012 [11] had introduced the primary consequence of Biosecure Signature Evaluation Campaign (BSEC'2009). It is utilized to assess different online signature algorithms on two undertakings, examining the impact of procurement conditions frameworks, contemplating the effect of data content in marks on frameworks' execution. The consequences of the 12 frameworks associated with this assessment battle are accounted for and examined in detail in this paper. Trial results uncovered that the strategy gives the better outcomes with Better Error Rate (BER).

Signature Verification System is the one having diverse biometric method which helps in close to home recognizable proof was proposed by (Ganorkar, P. N. et al 2014) [12]. This technique is to confirm whether the given mark done by the computerized pen is genuine or falsification. For recognizing different parameters like precision and coordinating level of two marks, this part displays slant strategy to distinguish the mark. Results demonstrated that the given strategy gives the better precision of the signature.

The creator (Rashidi, Saeid et al 2013) [13] had proposed 40 useful highlights of perspective characterization mistake and consistency for removing the best subset once a lot of highlights gives maximal segregation capacity between genuine. An adjusted separation of the DTW calculation is proposed to enhance execution of the check stage. The proposed framework is assessed on the general population SVC2004 signature database. The proposed Dynamic Time Wrapping (DTW) calculation gives the base Equal Error Rate (EER). The diverse classifier with a skilled forgery demonstrates that the best outcome has a superior EER utilizing the Parzen window classifier.

Galbally, Javier et al 2017 [14] had examined a novel methodology that exploits the execution enhancing that can be come to through the combination of on-line and disconnected marks. They propose a strategy for the age of upgraded engineered static examples from on-line information. Such engineered disconnected marks are utilized on another on-line signature acknowledgment design dependent on the blend of the two kinds of information: genuine on-line tests and fake disconnected marks combined from the genuine information.

## 3. Proposed Methodology

The proposed methodology describes to register the student project details via online registration form. In this every student put the signature during the submission of the proposal using online digital signature

method. Here, PRS is the efficient methods to authenticate the proposal utilizing the online digital signature recognition criteria. Here, the authentication as well as signature identification is the most important role during the project submission to prevent the unauthorized submission of the proposal by the student. Moreover, they contrast the genuine signature from the types of forged signature and it is classified based on proposed classification technique such as K-ANN, K-SOM, K-KNN, and K-SVM. The kernel based SVM classification technique gives better accuracy and performance compared to existing techniques.

## **3.1 Design and development of PRS**

PRS was structured and produced for the understudies and the staff members of ACT who wanted to manage the process with utmost security. It proposes the understudies' course venture and get it endorsed by the directors. Kinds of performers like understudies and managers are associated with this PRS. This current understudies' PRS is an online framework for accommodation of ventures and its endorsement by the pre-last year understudies. This PRS includes numerous procedures like login, expansion of qualified understudies for venture, accommodation of task recommendations by qualified understudies and its endorsement from the managers. Amid the online accommodation of proposition, every understudy needed to put their computerized marks utilizing the advanced tablet and its pen. This PRS serves to perceive the authentic marks of understudies from the sorts of manufactured marks like Random, Skilled and Unskilled, in this way keeping the accommodation of unapproved venture proposition.

Figure 2 speaks to the utilization case design for this proposed PRS. Each qualified pre last year students in the school needed to get ready and present their project proposal online with their authentic advanced signatures. At that point the project council examines the submitted proposal forms and relying upon its authenticity of data, the project is either acknowledged or rejected and allotted to each colleague.

## **4. Classification Techniques**

Here, some of the kernel based classification methods is used to analyze the signature and identifying the genuine from the forged one. Various classification methods like kernel based weight, ranking, similarity, regressions are analyzed. Based on this each feature was weighed and threshold was used for identifying the signatures efficiently.

### **4.1 Kernel based Artificial Neural Network (K-ANN)**

KANN algorithm utilizing the kernel logic and the datasets were converted into grid features. There is a change from the first signatories were converted into grid space. The advantage of using linear kernel helped to enhance the performance when mapping of data compared to other kernel functions. Weights were utilized for weighing the dynamic features. Each feature was weighed by the system and was

ordered from - 1 to 1. Based on the order, the genuine signatures were selected using the threshold criteria.

## **4.2 Kernel based K-Nearest Neighbours (K-KNN)**

This algorithm derived the operation of the kernel and ranking was used for identifying the signatures from the signature space. In the previous algorithm, KANN, weights were utilized to find genuine signatures from the signature space. But some genuine signatures were left from the signature space. So the genuine signature was identified using the weighted ranking voting and threshold value was utilized to identify the genuine signatures. It is utilized to optimize the output predictions. The objective of this approach was useful to find the genuine signatures using the dynamic features.

## **4.3 Kernel based Self-Organizing Map (K-SOM)**

It was proposed for identifying the similarity between the features and find genuine signatures. The difference between the previous and KSOM algorithm was obtained using similarity measure and weights. The similarity of the features was identified using the distance between the original and forged one. Employing the weights leads to recognizing the various dynamic features of the signature.

## **4.4 Kernel based Support Vector Machine (K-SVM)**

KSVM algorithm was specially developed for finding the genuine signature from the feature space. This approach was that genuine signatures were obtained using weight and regression. The signatures were selected based on the weight from the signature space. The threshold value was used to find the dynamic features and the same datasets were used for experimenting with the proposed algorithms. The approximation was employed for finding the features and also leads to minimize the error at the time of recognizing the signature.

### **4.4.1 Best threshold value**

Based on the above classification technique, it stated as efficiently predicted the signature result from the original signature dataset. Moreover, the best threshold value is obtained and it is used identify the genuine signatures.

## **5. Result And Discussion**

In this part, signature dataset is taken from college. Moreover, the signature is analyzed by using various classification techniques such that the accuracy and performance is explained with below charts and tables.

### **5.1 Dataset Preparation**

In Al-Musanna College of Technology (ACT), presently 6000 students are studying in various levels and specializations. Out of total number of students, 1000 of them are eligible to register and study their

course project in the pre-final year. In this research work the mix of forged and genuine online digital signatures from 750 students of ACT were collected on the basis of 75 students in one day for a period of 10 days with the digital tablet and stored as ACT dataset. The genuine signatures obtained in every day was exchanged with the other set of 75 students for a period of 10 days to prepare the types of random, skilled and unskilled forged signatures.

## 5.1.1 Performance of PRS

In the below Figs explains the various performance of PRS. Here, how to login the page and how to add the students detail are explained in below

The user inputs valid User Name and Password for accessing this PRS with the assistance of login page given in Fig. 3. New users must register and Sign up their details. In case the user does not remember their password, they can use Forgot Password option to get their new password in their email. The students can view the list of project proposals and their detailed status after successful login.

Figure 4 explains to help the staff or the administrator to add students' details and group them according to their specialization. In the add students page there are female, level and specifications. Only the new student's details are entered, the old student's accounts can also be deleted if it is not used for longer time. If, all the details are given, then logout the given page for unauthorized person open the considered page.

Figure 5 explains admin statistics page was used by the admin to get the statistical information and manage the student project allocation and their group members based on their level of study and specialization. Here, the number of projects by which the students is registered, and how many male and female are registered in the corresponding admin statistics page.

Figure 6 represents each student group leader must fill in their project proposal details in the online form and inform their other team members to make their digital signatures and finally submit to the project approval committee. This committee then evaluates the student's project proposal and identifies the genuine signer's signature by employing the proposed kernel based classifiers for recognizing the online digital signature, before approving the student's project.

**Table: 1** Accuracy analysis for various classification techniques

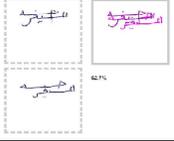
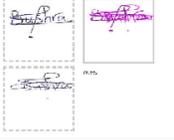
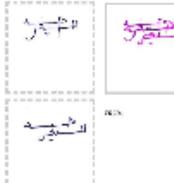
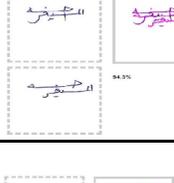
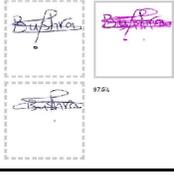
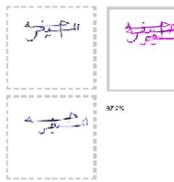
Classification techniques	Training and testing	Online digital signature of student	Accuracy
K-ANN	Training		65.8%
	Testing		62.7%
K-KNN	Training		75.6%
	Testing		75.3%
K-SOM	Training		94.1%
	Testing		94.3%
K-SVM	Training		97.5%
	Testing		97.2%

Table 1 explains the training and testing results in the ACT dataset for online digital signature recognition. Here, it is verified by the various classifications techniques for analyzing the performance and accuracy for signatures. The data sets were divided, into training 80% and test sets 20%. The various classification techniques are K-ANN, K-KNN, K-SOM and K-SVM. Each and every technique gives the different accuracy and performance during training and testing. For training, the signature using K-ANN

technique the accuracy is 65.8%, and for testing the accuracy is 62.7%. For training, the signature using K-KNN technique the accuracy is 75.6%, and for testing the accuracy is 75.3%. For training, the signature using K-SOM technique the accuracy is 94.1%, and for testing the accuracy is 94.3%. Finally, for K-SVM the accuracy is 97.5% during training and achieves 97.2% during testing. Compared to all other techniques K-SVM gives the better performance and accuracy for various digital signatures.

Performance analysis: The accuracies of these four models and its sampling were represented and studied in the form of True Positive Rate (TPR), False Positive Rate (FPR) and Equal Error Rate (EER).

True Positive Rate (TPR): It measures the proportion of actual positives that are correctly identified the genuine signatures.

$$TPR = TP / (TP + FN)$$

False Positive Rate (FPR): It is the probability of falsely rejecting the null hypothesis for a particular test.

$$FPR = FP / (FP + TN)$$

Equal Error Rate (EER): EER is a biometric security system algorithm used to predetermine the threshold values for its false acceptance rate and its false rejection rate. When the rates are equal, the common value is referred to as the equal error rate.

## 5.2 Comparative analysis

In this comparative analysis was tested in two ways, modeling and sampling selection performance based on two datasets such as ACT and ICDAR. Based on this it is noticed as plot the accuracy graph with various epochs.

### 5.3 Model selection performance in ACT dataset

Figure 7 (a) explains the accuracy analysis of various epochs. Here, x-axis represents the epochs and y-axis explains the accuracy in (%). When the epoch is at 20, the accuracy value is 0.26 for K-ANN, for K-KNN the obtained accuracy value is 0.30, for K-SOM the obtained accuracy value is 0.33 and for K-SVM the accuracy value is 0.41. Similarly, for all other techniques it obtained the different accuracy values. The K-SVM gives the higher accuracy values compared to all other techniques.

### 5.4 Model selection performance in ICDAR dataset

Figure 7 (b) explains the modeling selection performance in ICDAR dataset. Here, the accuracy analysis is performed for ICDAR dataset. The model selection is performed with various classification techniques. The epoch is at 20, the accuracy attained for K-ANN is 0.18, at 40, the accuracy is 0.21, at 60, accuracy is 0.26, at 80, the accuracy is 0.31, at 100, the accuracy is 0.38, similarly for all other epoch have the different accuracy values. Beyond 180 epochs, the training was halted due to the over-fitting problem which is still an unsolved issue in machine learning area, leading to lower performance. Epoch at 180, gives the maximum accuracy for K-SVM and this classification method gives the better accuracy values.

## 5.5 Sampling performance in ACT dataset

Figure 8 (a) explains the sampling performance in ACT dataset. The epoch is varied from 0 to 180 and the accuracy value is varied from 0 to 1. The epoch is increased correspondingly the accuracy value is increased. Here, epoch at 20, the obtained accuracy value is 0.22 for K-ANN, for K-KNN the obtained accuracy is 0.28, for KSOM the obtained accuracy is 0.35 and for K-SVM the obtained accuracy is 0.43. Compared to all other techniques K-SVM gives the maximum accuracy for all epochs.

## 5.6 Sampling performance in ICDAR dataset

Figure 8 (b) represents the sampling performance in ICDAR dataset. Here, the sampling is performed with four classification techniques such as K-ANN, K-KNN, K-SOM and K-SVM. By using this method, it attained different accuracy values with varying epochs. The epoch is repeated until it gets the maximum accuracy values. At epoch 20, the accuracy obtained for K-ANN is 0.19, 0.25 for K-KNN, 0.30 for K-SOM, 0.41 for K-SVM. Here, also K-SVM gives the highest accuracy for all other epochs.

## 5.7 Model selection performance in ACT dataset

Figure 9. (a) Explains the EER analysis of ACT dataset. EER is calculating based on different iterations. The compared algorithms are K-ANN, K-KNN, K-SOM and K-SVM. The graph is plotted based on model selection performance with the given dataset. From the graph, it clearly shows that K-SVM gives the minimum EER compared to all other techniques.

## 5.8 Model selection performance in ICDAR dataset

Figure 9. (b). explains the EER analysis of ACT dataset. EER is calculating based on different iterations. The compared algorithms are K-ANN, K-KNN, K-SOM and K-SVM. The graph is plotted based on model selection performance with the given dataset. From the graph, it clearly shows that K-SVM gives the minimum EER compared to all other techniques.

## 5.8 Sampling performance in ACT dataset

Figure 10 (a) explains the sampling performance in ACT dataset for EER analysis. Here, in the above graph all the techniques give the different error rate results. At epoch 20, K-ANN gives the error values 0.76, for K-KNN the value is 0.65, for K-SOM the value is 0.56 and the K-SVM gives error values at 0.36. Similarly, all the techniques give the various error values. K-SVM gives the minimum EER with best results.

## 5.9 Sampling performance in ICDAR dataset

Figure 10. (b)., explains the EER analysis for sampling performance in ICDAR dataset. Here, x-axis represents the epoch and y-axis represents the EER. The minimum EER value was obtained for K-SVM techniques. This technique gives the overall best results with repeating the iterations. At epoch 180, the technique gives the better EER.

Figure 11, explains the time analysis with various classification techniques. Here, for various signatures iterations have been repeated the iteration, to get the time calculated. The minimum time for K-SVM has been achieved and hence the proposed algorithm gives the better results compared to other techniques.

## 6. Conclusion

The paper presented an online digital signature in PRS for project proposal identified by using student signature. PRS is used to authenticate the student's project proposal and to prevent the unauthorized submission of proposal. The prime objectives of this research work was to recognize the genuine online digital signatures from the assortment of genuine, skilled, unskilled and random types of forged signatures by using the dynamic features like pen pressure, altitude, velocity, azimuth and duration taken by the legitimate person for signing using the proposed K-SVM classification techniques. The genuine signature is recognized by using proposed techniques with better accuracy with 97% and better performance. The growth in the signatures sample size in numerous datasets and the choice of various dynamic features other than pen pressure, velocity, altitude, azimuth, and time taken for signing could be the open issues for the future research work in this arena of enriching the performance and accuracy of recognizing the online digital.

## Declarations

### Funding

The authors received no specific funding for this study.

### Conflict of interest/Competing interests

This paper has no conflict of interest for publishing

### Ethics approval

The Research guide reviewed and ethically approved this manuscript for publishing in Wireless Personal Communication journal.

### Consent to participate

The participants are Dr. R. Ravi Chakravarthi, Dr.C. Anna Palagan,

Mr. Ravindra Ratilal Dharamshi, Dr. Anand J Dhas, Mr. Shrikant Taware and Dr. Ahilan Appathurai

### Consent for publication

The author was agreed to publish this research work in Wireless Personal Communication journal.

### Availability of data and materials

Not applicable

Code availability

Not applicable

Authors' contributions

Conceptualization, investigation: Dr. R. Ravi Chakravarthi, Dr.C. Anna Palagan, Mr. Ravindra Ratilal Dharamshi, Dr. Anand J Dhas,Mr. Shrikant Taware and Dr. Ahilan Appathurai

Writing—original draft preparation: Dr. R. Ravi Chakravarthi

Writing—review and editing: Dr.C. Anna Palagan,

Mr. Ravindra Ratilal Dharamshi, Dr. Anand J Dhas,Mr. Shrikant Taware and Dr. Ahilan Appathurai

All authors have read and agreed to the published version of the manuscript.

## References

1. Shankar, T. N., Gadadhar Sahoo, and S. Niranjana.: Using the digital signature of a fingerprint by an elliptic curve cryptosystem for enhanced authentication. *Info Sec Jour: A Global Perspective*.5: 243-255, (2012). <https://doi.org/10.1080/19393555.2012.694978>
2. Ibrahim, M. T., Khan, M. A., Alimgeer, K. S., Khan, M. K., Taj, I. A., & Guan, L.: Velocity and pressure-based partitions of horizontal and vertical trajectories for on-line signature verification. *Pattern Recgn*, 43(8), 2817-2832, (2010). <https://doi.org/10.1016/j.patcog.2010.02.011>
3. Sae-Bae .N, Memon .N, Sooraksa .: Distinctiveness, complexity, and repeatability of online signature templates. *Pattern Recgn*. 1;84:332-44, (2018), <https://doi.org/10.1016/j.patcog.2018.07.024>
4. RabotkaV, Mannan M.: An evaluation of recent secure deduplication proposals. *Jour Info Sec App..* 1;27:3-18, (2016), <https://doi.org/10.1016/j.jisa.2015.08.001>
5. Velez J, Sanchez A, Moreno B, Esteban J.: Fuzzy shape-memory snakes for the automatic off-line signature verification problem. *Fuzzy Sets Sys*. 16;160(2):182-97, (2009) <https://doi.org/10.1016/j.fss.2008.05.021>
6. Batista L, Granger E, Sabourin R.: Dynamic selection of generative–discriminative ensembles for off-line signature verification. *Pattern Recognition*.45(4):132640. (2012), <https://doi.org/10.1016/j.patcog.2011.10.011>
7. Yasuda K, Muramatsu D, Shirato S, Matsumoto T.: Visual-based online signature verification using features extracted from video. *Network andComp* ;33(3):333-41(2010) <https://doi.org/10.1016/j.jnca.2009.12.010>
8. Cpałka K, Zalasiński M.: On-line signature verification using vertical signature partitioning. *Expert Sys. with App*.1;41(9):4170-80 (2014 ). <https://doi.org/10.1016/j.eswa.2013.12.047>

9. Doroz R, Kudlacik P, Porwik P. Online signature verification modeled by stability oriented reference signatures. *Info*1;460:151-71(2018).<https://doi.org/10.1016/j.ins.2018.05.049>
10. Heckerroth J, Boywitt C.: Examining authenticity: an initial exploration of the suitability of handwritten electronic signatures. *Forensic sci international*1;275:144-54(2017). <https://doi.org/10.1016/j.forsciint.2017.02.019>
11. Houmani N, Mayoue A, Garcia-Salicetti S, Dorizzi B, Khalil M.I., Moustafa M.N., Abbas H, Muramatsu D, Yanikoglu B, Kholmatov A, Martinez-Diaz M.: BioSecure signature evaluation campaign (BSEC'2009): Evaluating online signature algorithms depending on the quality of signatures. *Pattern Rec.*;45(3):9931003(2012). <https://doi.org/10.1016/j.patcog.2011.08.008>
12. Ganorkar P.N., Pendke K.: Design Of Digital Signature Verification Algorithm Using Relative Slope Method. *International Journal for Research Eng & Tech.* (2014).
13. Rashidi S, Fallah A, Towhidkhah F.: Similarity evaluation of online signatures based on modified dynamic time warping. *Applied Artificial Intelli.* 9;27(7):599-617(2013).<https://doi.org/10.1080/08839514.2013.813187>
14. Galbally J, Diaz-Cabrera M, Ferrer M.A., Gomez-Barrero M, Morales A, Fierrez J.:On-line signature recognition through the combination of real dynamic data and synthetically generated static data. *Pattern Rec.* ;48(9):2921-34(2015).<https://doi.org/10.1016/j.patcog.2015.03.019>
15. Appathurai A, Sundarasekar R, Raja C, Alex EJ, Palagan CA, Nithya A. An efficient optimal neural network-based moving vehicle detection in traffic video surveillance system. *Circuits, Systems, and Signal Processing.* 9(2):734-56(2020)
16. Appathurai A, Manogaran G, Chilamkurti N. Trusted FPGA-based transport traffic inject, impersonate (I 2) attacks beaconing in the Internet of Vehicles. *IET Networks.* 2019 Jun 10;8(3):169-78..

## Figures

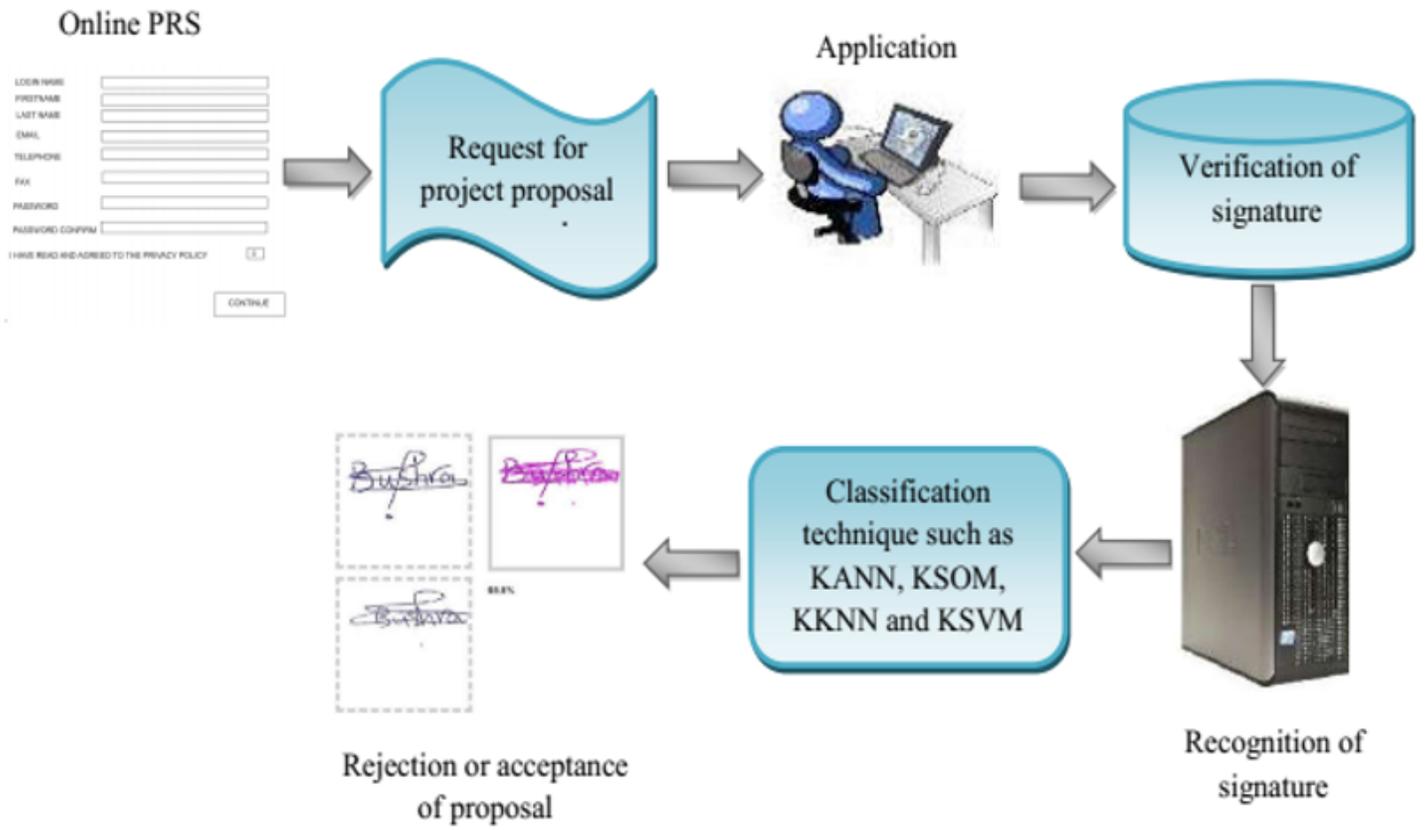


Figure 1

Overview of PRS

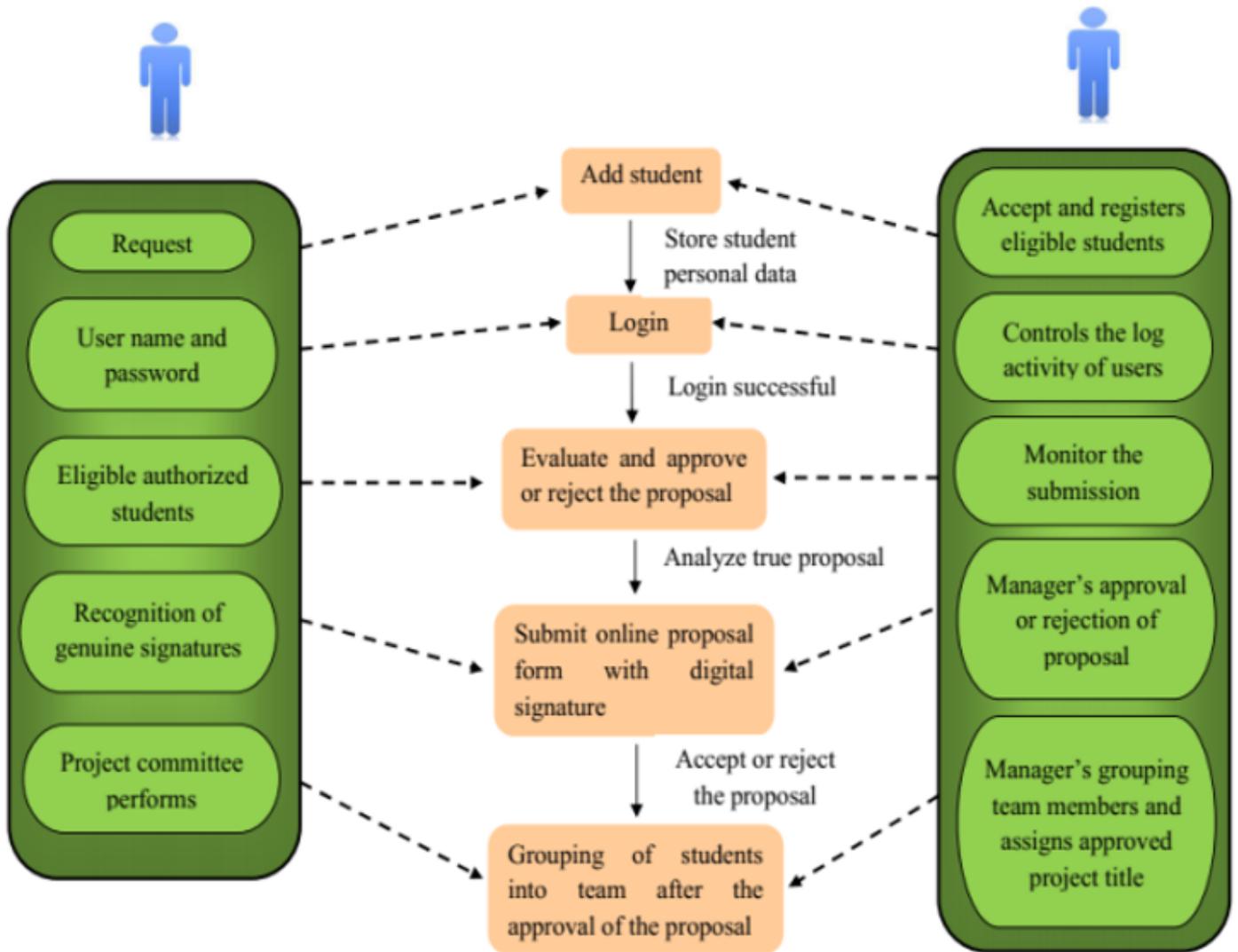
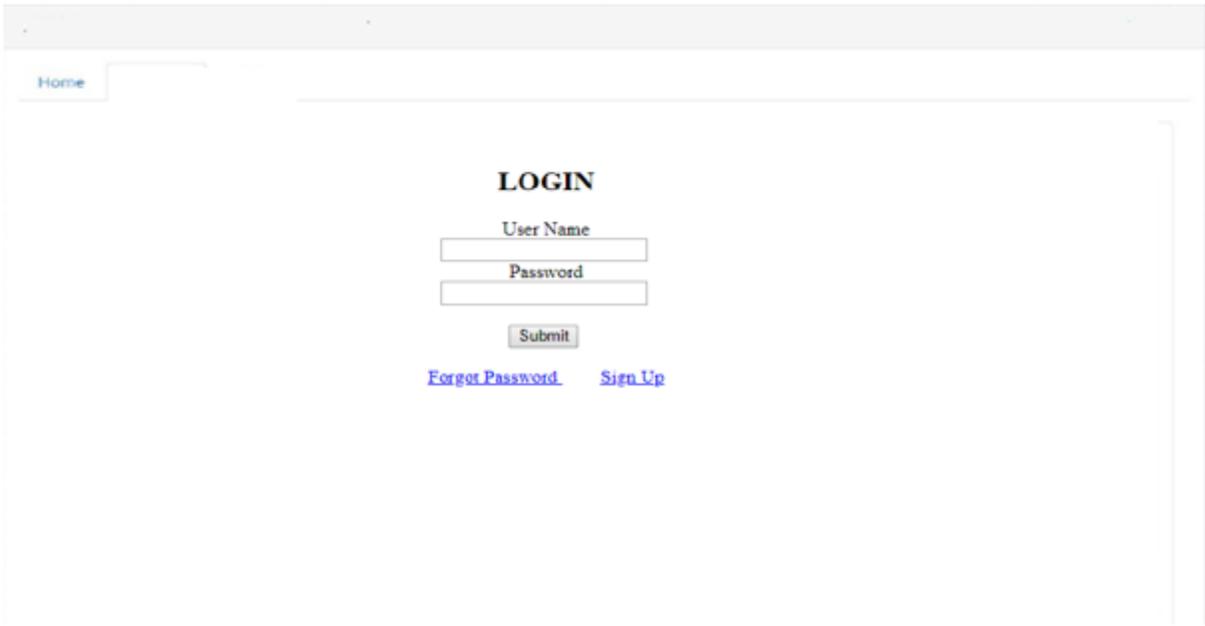


Figure 2

PRS design



**Figure 3**

User login Page

ADMIN Logout

Home Manage Groups

[Add Student](#)

[Delete Accounts](#)

**Figure 4**

ADD students page

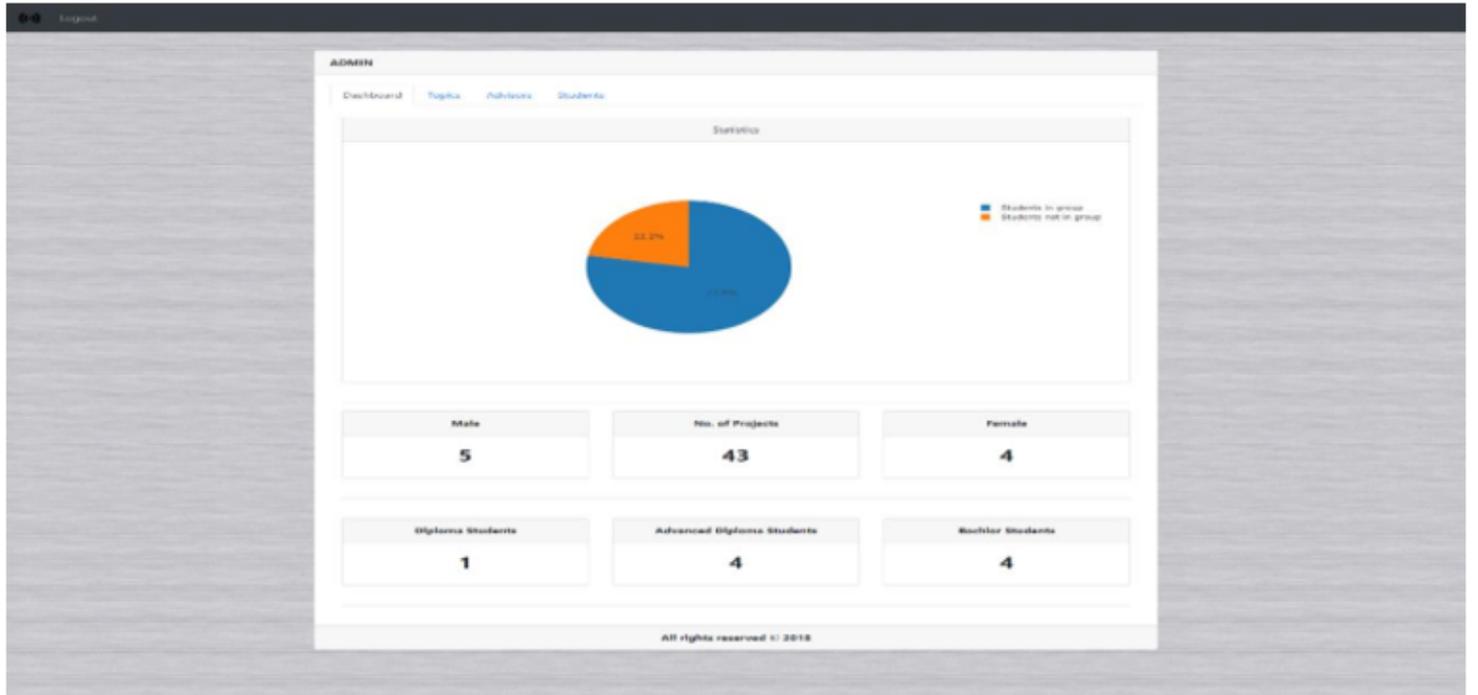


Figure 5

Admin Statistics page

**Project Proposal Submission Form**

**Project Title**

**Project Objectives and Strength  
(What I hope to achieve?)**

**Procedures (How I plan to  
accomplish my goal)**

**Resources ( Things I plan to use to  
reach my goal)**

**Exhibition(What I plan to produce  
and present)**

**Project Member 1 Signature**

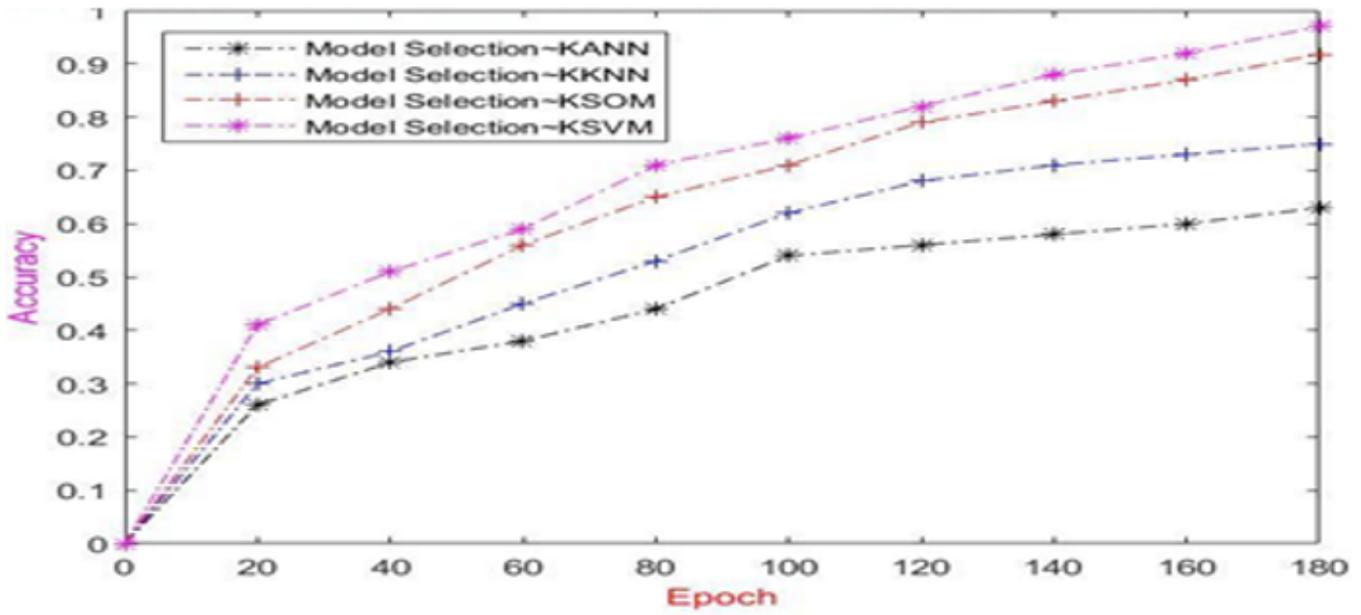
**Project Member 2 Signature**

**Project Member 3 Signature**

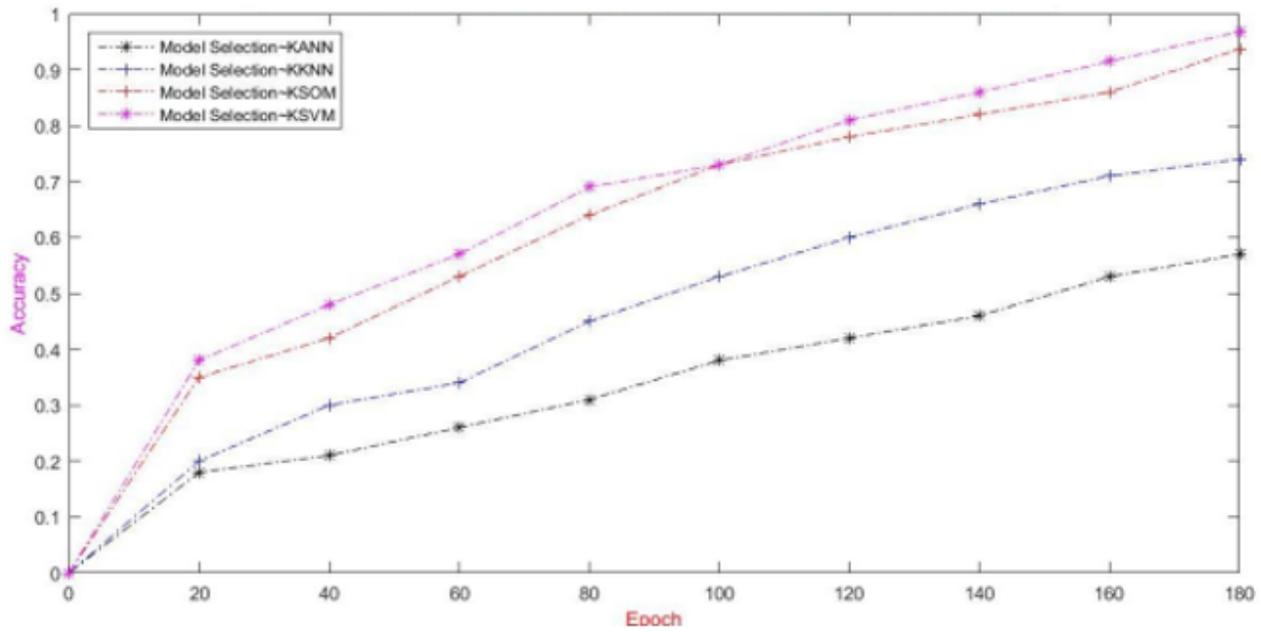
**Project Member 4 Signature**

**Figure 6**

Students Project Proposal page



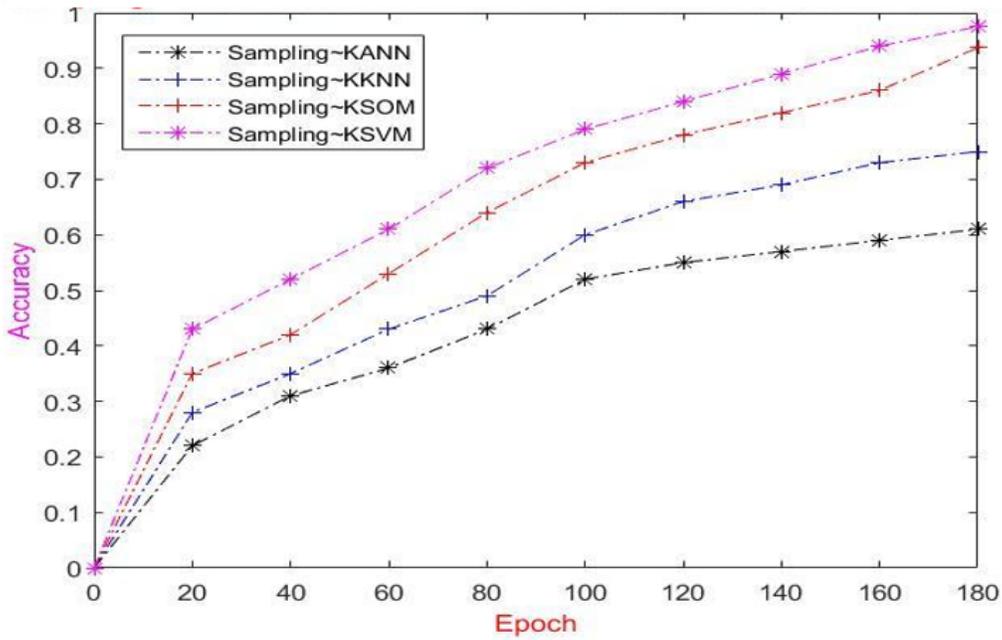
a



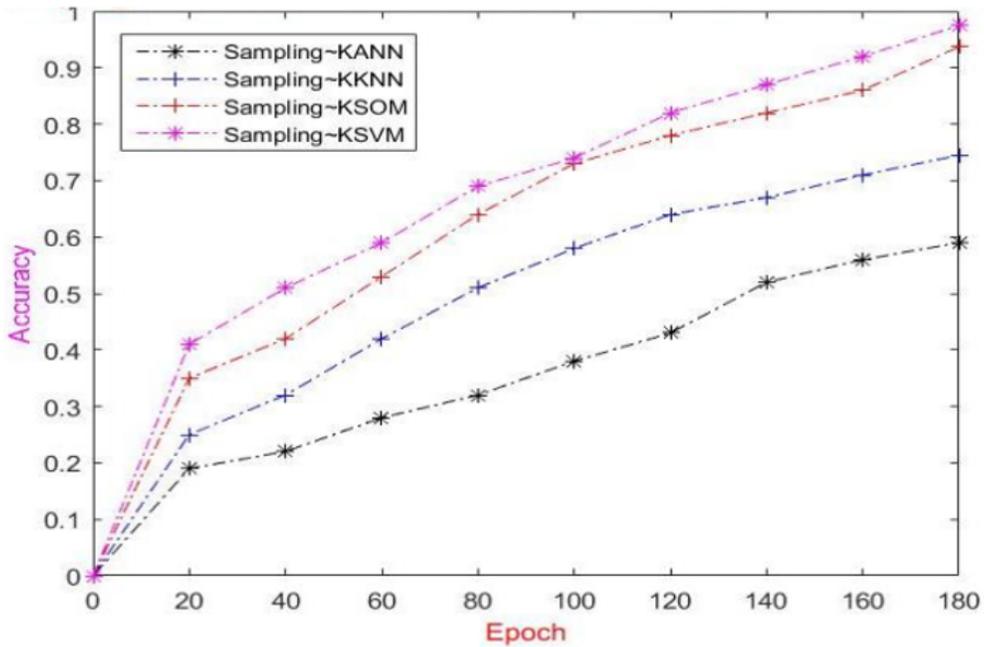
b

Figure 7

(a): Accuracy analysis (b): Accuracy analysis



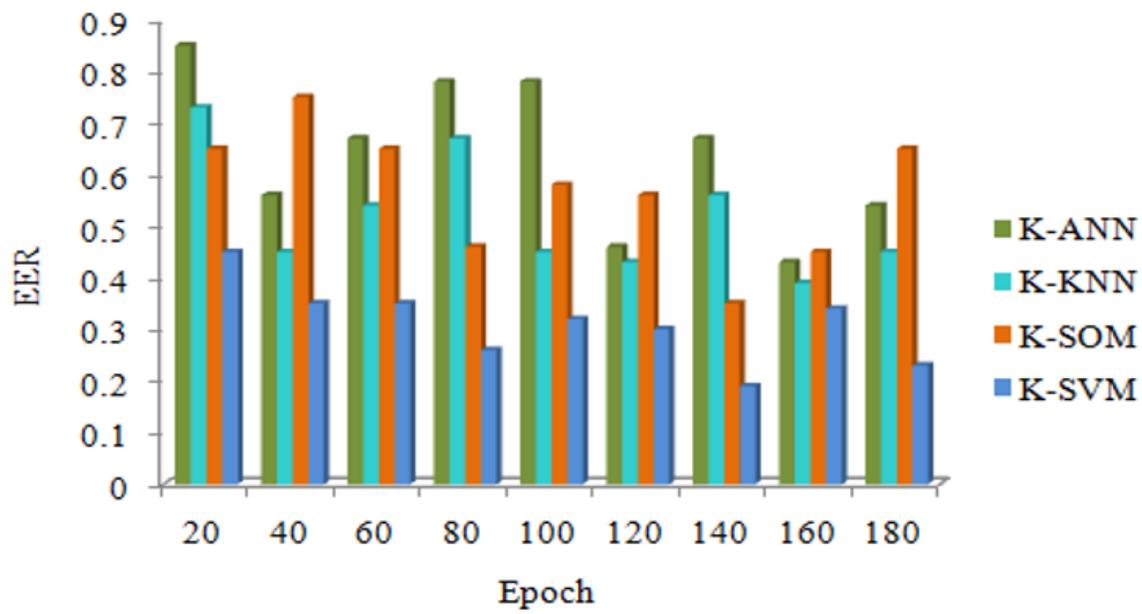
a



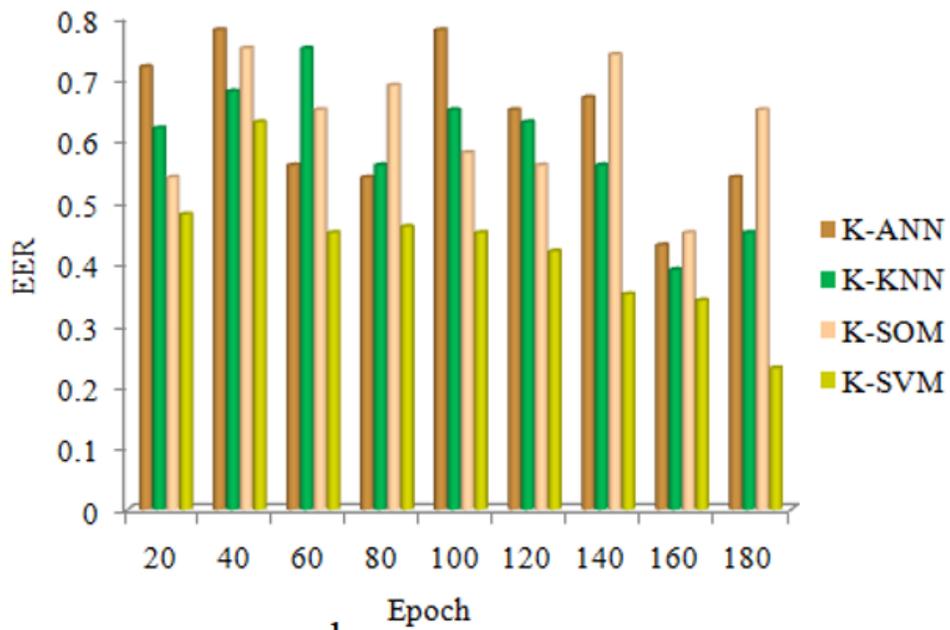
b

Figure 8

(a): Accuracy analysis (b): Accuracy analysis



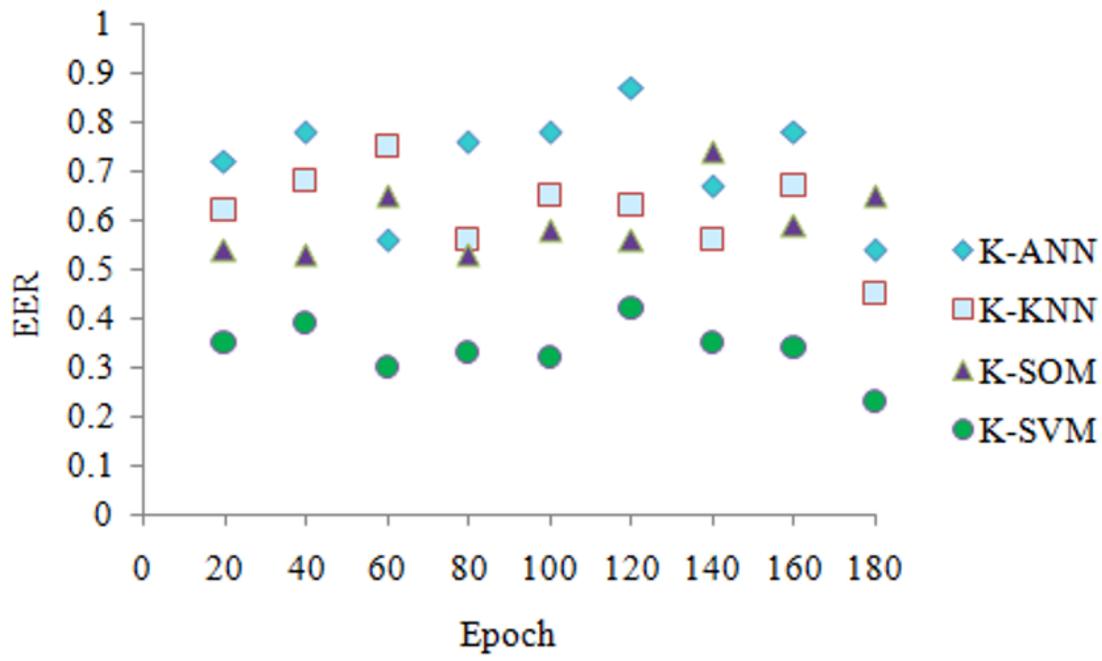
a



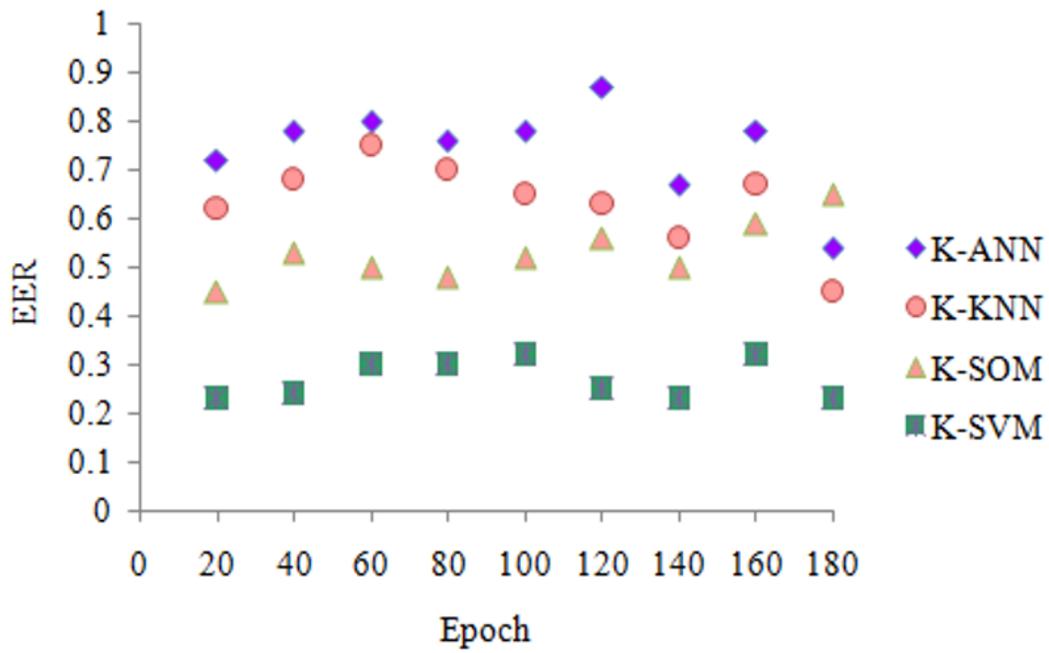
b

Figure 9

(a):EER analysis (b): EER analysis



a



b

Figure 10

(a): EER analysis (b): EER analysis

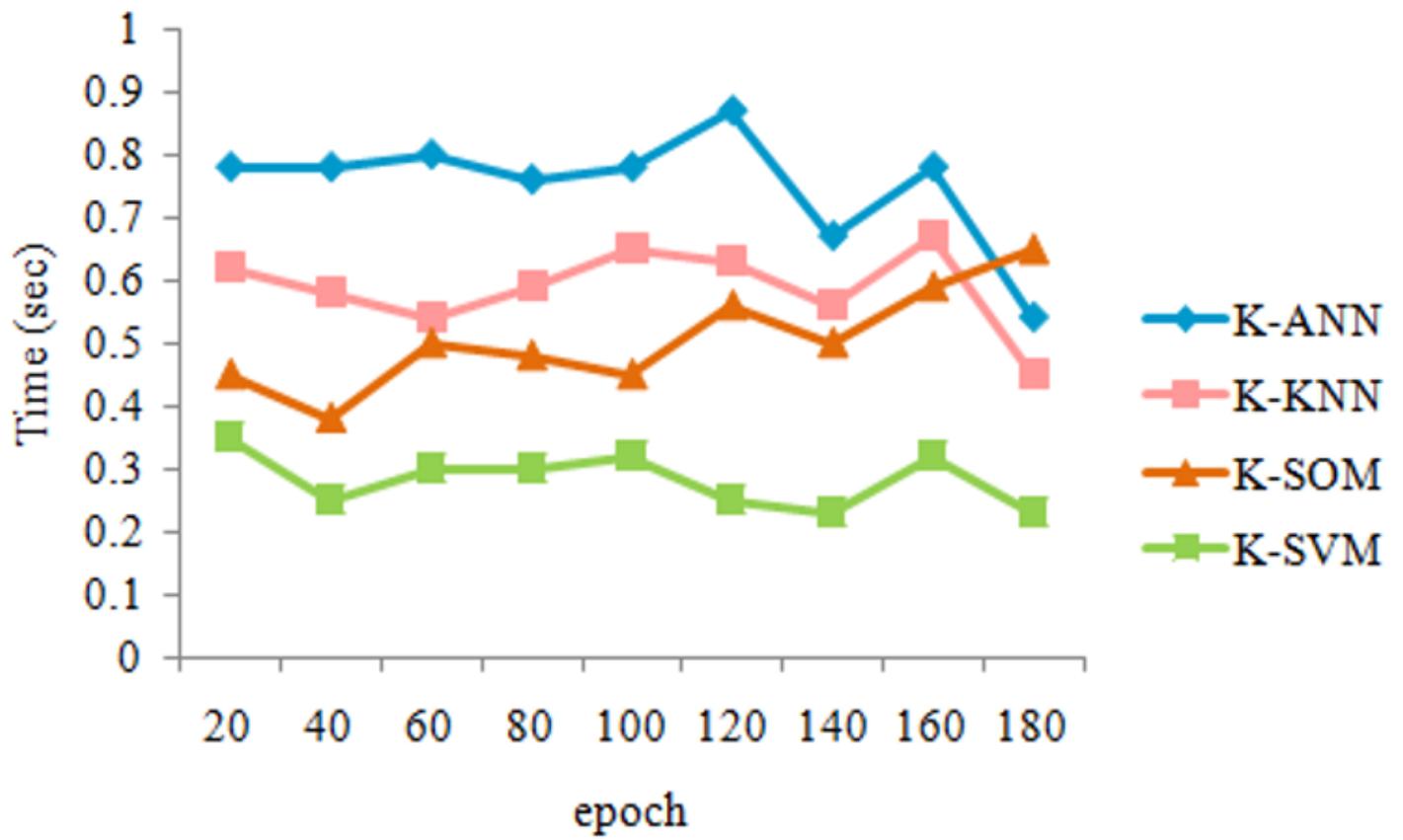


Figure 11

Time analysis