BIOMETRIC TECHNOLOGIES FOR ONLINE STUDENT AUTHENTICATION

Aythami Morales, Julian Fierrez, Ruben Vera-Rodriguez, Javier Ortega-Garcia

Departamento de Tecnologia Electronica y de las Comunicaciones, EPS, Universidad Autonoma de Madrid (SPAIN)

Abstract

In this work we present: i) an analysis of biometric technologies for online student authentication; ii) a case study on keystroke dynamics authentication applied to a real operational environment. Concisely, this work studies the biometric technologies and their advantages/disadvantages for online student authentication services. The analysis is made on the basis of three main pillars: performance, usability and legal concerns. Our study provides new insights on the deployment of these technologies in educational environments with special attention to keystroke dynamics systems. Keystroke dynamic authentication has attracted much interest from industry and researchers during the last decade. Keystroke dynamics authentication is interesting for online authentication because it is: i) transparent (it runs in the background without requiring explicit user interaction); ii) continuous (authentication can be performed over all the user activity, not only based on an initial access to the platform). This work includes a case study on keystroke dynamic authentication over the typing patterns of 64 students answering questions in 3 online exams over a semester. We analyze the performance of four keystroke biometric systems and the results obtained show a promising performance with a correct student authentication over 90%. This work encourages to further explore in authentication services based on biometric technologies for online courses.

Keywords: authentication, biometrics, MOOCs, POOCs.

1 INTRODUCTION

Online education is changing the world-wide education scenario (e.g. Massive Open Online Courses and Participatory Open Online Courses). Online courses break with the barriers associated to traditional lessons and provide a new widely accessible education over the internet. A new education emerges on the basis of open, free, distributed and participatory courses. This new approach does not attempt to replace the traditional education and it must be seen as a complementary proposal to overcome limitations and take advantage of new technologies. However, there is a discussion among all the academic sectors about this new educational scenario. Among the topics under discussion, how to certificate the successful completion of courses is one of the most controversial. How can we certify courses without classroom attendance? Is it possible a reliable authentication of the students? How can we avoid/detect fraudulent users? The widely and accessible nature of online courses complicates the individualization of the education and student authentication is part of this individualization. The aim is not to criminalize the students but reliable authentication is critical for the future of online education and solutions should be balanced between security and user's privacy. Therefore, researchers and instructors have made efforts to propose authentication approaches which comply with the characteristics of these courses.

Among all the technologies proposed, biometric authentication is one of the most attractive approaches. Biometric recognition technologies allow to authenticate users based on "something that we are" instead of traditional authentication based on "something that we know" such as passwords or PINs. The biometric technologies have become popular during last years (e.g. Apple Iphone Fingerprint sensor) and nowadays they can be considered an important actor in consumer technology market. The biometric recognition technologies can be divided in physical traits (face, fingerprint, iris, DNA ...) and behavioural traits (signature, voice, gait, keystroking,...). There is no a technology which overcomes the rest and depending of the application we can opt for several solutions.

In this context, the keystroke dynamics authentication systems have attracted the interest of both researchers and industry [1][2][3]. The keystroke dynamics are proposed to improve the security of traditional authentication services based on passwords or PIN numbers. Biometric recognition is commonly related with "something that users are" instead of "something that users have" such as passwords. In the case of keystroke dynamics, the typical approaches based on fixed password

authentication combine complex passwords and our keystroke dynamic biometrics. The password acts as a primary security level and the user access is not allowed until the correct password is inserted. The role of the biometric system is a secondary security level which try to detect intruders who are spoofing the identity of the legitimate user. Keystroke dynamics authentication is interesting for online authentication because it is: i) transparent (it runs in the background without requiring explicit user interaction); ii) continuous (authentication can be performed over all the user activity, not only based on an initial access to the platform); iii) it arises low privacy concerns; iv) it is easy to integrate in existing platforms.

This work analyses biometric technologies for online student authentication services. We include an end-to-end approach which covers most of the authentication steps: design, acquisition, modelling and decision. Concisely, this work studies the biometric technologies on the basis of three main pillars: performance, usability and legal concerns. Our study provides new insights on the deployment of these technologies in educational environments with special attention to keystroke dynamics systems. This work includes a case study on keystroke dynamic authentication over the typing patterns of 64 students answering questions in 3 online exams over a semester. We analyze the performance of four keystroke biometric systems and the results obtained show promising accuracy with a correct student authentication over 90%. This work encourages to further explore in authentication services based on biometric technologies for online courses.

The rest of the paper is organized as follows: Section 2 describes the main concepts related with the authentication of users for e-learning platforms; Section 3 deals with the keystroke dynamics authentication and the experimental framework included in this work; results are reported in Sections 4. Finally Section 5 draws some conclusions.

2 AUTHENTICATION OF USERS FOR E-LEARNING

The authentication of users for web-services is a must in a global society. The necessity to authenticate students in online courses is an example of this necessity. The research community, industry and educational institutions are studying new technologies/solutions to provide reliable authentication for e-learning platforms [4]. As a service, the user's authentication must to comply with requirements related with the performance, usability and legal concerns. The service must be secure, not affect the user activity and respect the laws:

- **Performance:** the performance of the system is related with a variety of topics: i) robustness of the system to detect attacks (False Positives); ii) the system ability to detect the genuine users; iii) the scalability of the system from tens of users to millions. The performance of the authentication system is important and it varies depending of the biometric traits used. The performance of keystroke dynamics is far from other popular biometric technologies such as fingerprint or iris. However, keystroke dynamics can provide attack detection rates up to 50% with a minimum cost (no need new sensors) in comparison with other biometrics (which need specific sensors).
- **Usability:** the user experience is important for any kind of service and authentication systems need to be as transparent as possible. The normal use of the service (the educational platform) must be guaranteed and the authentication service cannot be seen as a barrier. This is probably the main attraction of keystroke dynamics technologies which allow a transparent authentication. The authentication is made during the normal activity (typing is needed in a web environment) and users do not have to perceive the process running in the background. The Universality is also a key concerns in platforms with a widespread use as new massive educational environments. Can we consider keystroke dynamics as universal? The use of the authentication service must be guarantee for a high percentage of the population and keystroke dynamics could be considered universal for most of the users of educational web-platforms.

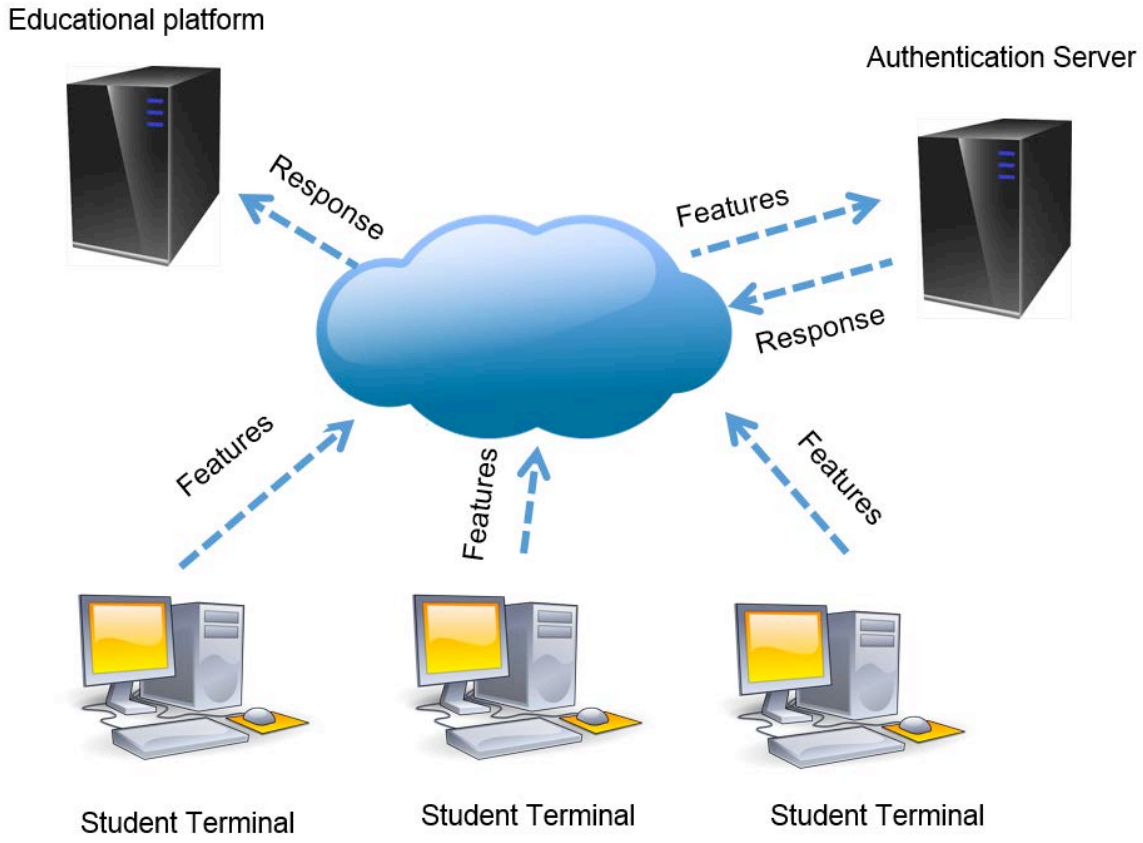

Figure 1. Student authentication process for e-learning platforms

- **Legal concerns:** the system must respect the laws associate to the services provided. The use and store of biometric data raise important privacy concerns. It is important to comply with standards (e.g. ISO/IEC 19794-2, ANSI/INCITS 378) and legality of the countries in which the services is provided. However, due to the worldwide dimension of new educational platforms (MOOCs, POOCs) it is not trivial to fully comply with all legal concerns. Keystroke dynamics can be considered a noninvasive biometric trait in comparison with other technologies such as fingerprint or face but the use of key listener (programs which provide the typing information) imply several privacy issues.

2.1 Architecture of a Biometric Authentication Service for e-learning

The architecture of biometric authentication systems can be adapted depending of the characteristics of the service. The security of the system depends of the architecture and its vulnerabilities. The storage of biometric data is critical and speed of the service must be quick enough to do not affect the use of the educational platform. The authentication can be performed:

- **Offline:** the comparison of the biometric data is made on the user terminal.
- **Online:** the data are acquired in the user terminal and then are sent to the authentication server where the comparison is made.

In this work we propose a traditional user authentication service based on cloud computing, see Fig. 1. First the keystroke dynamics are acquired in the student terminal. The biometric information is extracted locally (at student terminal) and encoded. It is recommendable avoid to send the raw data because of privacy and security concerns. Secondly, the authentication server receive the codified features and decode it to perform the authentication (online authentication). Once the authentication is done, the response/identity is sent to the educational platform which can accept or denied the access to the services.

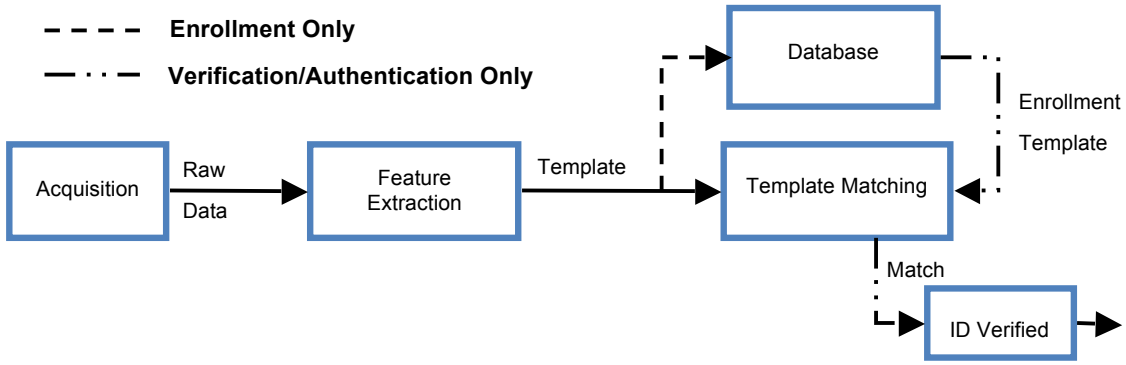

Figure 2. Block diagram of biometric authentication systems

The next sections focus on the biometric authentication process to be performed in the authentication servers.

2.2 Block Diagram of the Biometric Recognition System

The scheme of a keystroke dynamics biometric system is similar to traditional biometric recognition systems based on other traits such as fingerprint, face or iris, see Fig. 2. The differences lie in the data and algorithm used to recognize the users. The system works on two modes: i) in the enrollment stage, the system acquires the data from the user and stores it in memory for a posterior ii) recognition or authentication stage, in which from new data, the system compares with the data in the memory to ascertain the identity of the user. The modules involved in both stages are similar with the exception of the matching module which is only necessary during the recognition/authentication stage. Therefore, the system comprises the next modules:

- **Acquisition**: the timestamps of the keyboard events are acquired using a key-listener or similar programs.
- **Feature extraction:** the keystroke dynamics are extracted from the raw data (timestamps) to provide distinctive patterns (templates) which characterize the users. These templates are stored in a database during the enrollment phase.
- **Template matching:** to verify the identity related with a new sequence of key events, the template obtained is compared with the identities stored in the database. This task is traditionally named as classification and the result is a similarity score. The user identity is authenticated if the score exceeds a threshold.

Other important sub-modules such as image preprocessing or decision module can be added to the basic scheme or can be considered as part of one of the principal modules.

3 KEYSTROKE DYNAMICS BIOMETRIC AUTHENTICATION

Keystroke dynamics include distinctive patterns which can be used for a reliable authentication in web-environments. In this section we will explain the main steps for the development of a user authentication algorithm based on keystroke dynamics.

3.1 Feature Extraction Methods

The keystroke dynamics extracted from a sequence of N keys consist on a vector $\mathbf{t}$ which contains the time stamp of every key-press ($\mathbf{t}^p$) and key-release ($\mathbf{t}^r$) event. These time stamps can be used to model the way a subject type but it is necessary to process the data to normalize the features with respect a reference. This normalization on time can be achieved considering intervals between consecutive key events instead absolute time stamps, see Fig. 3. The most popular features used to characterize the keystroke patterns [5] are:

- **Hold Time:** it is the differences between the time of pressure and release of the *i*th key:

$$H_i = t_i^r - t_i^p \qquad i = 1, \dots, N$$

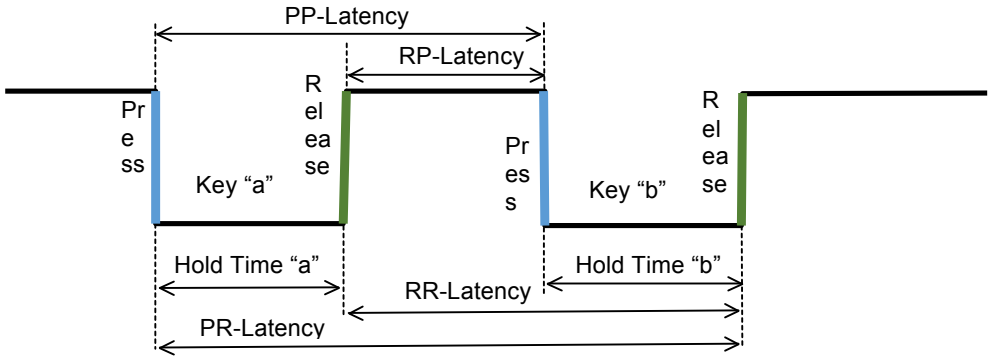

Figure 3. Keystroke dynamics features for a generic digraph “ab”

- **Release-Press latency (RP-latency):** is the difference between the time of pressure of the (*i+1*)th key and the release of the *i*th key:

$$L_i^{rp} = t_{i+1}^{p} - t_i^{r} \qquad i = 1, \dots, N-1$$

- **Press-Press latency (PP-latency):** is the difference between the time of pressure of (*i*+1)th key and the pressure of the *i*th key:

$$L_i^{pp} = t_{i+1}^{p} - t_i^{p} \qquad i = 1, \dots, N-1$$

- **Release-Release latency (RR-latency):** is the difference between the time of pressure of (*i*+1)th key and the pressure of the *i*th key:

$$L_i^{rr} = t_{i+1}^{r} - t_i^{r} \qquad i = 1, \dots, N-1$$

- **Press-Release latency (PR-latency):** is the difference between the time of release of the (*i*+1)th key and the pressure of the *i*th key:

$$L_i^{pr} = t_{i+1}^{r} - t_i^{p} \qquad i = 1, \dots, N-1$$

Fig. 3 shows the features extracted from a generic digraph composed by two keys ”a, b”. In our experiments we chose the Hold Time and RP-Latency. The combination of the features is made by a simple concatenation of the values $\{H_i, L_i^{rp}\}$.

3.2 Classifiers

This work evaluates two different classification algorithms for keystroke dynamic authentication. Assume $\mathbf{f} = \{f_1, f_2, \dots, f_M\}$ as the feature vector (with M features) of a given test sample and $\mathbf{g^k} = \{g_1^k, g_2^k, \dots, g_M^k\}\ k \in 1, \dots T$ as an enrollment set with T samples. The four keystroke dynamics classifiers included in the benchmark are:

- **Mahalannobis + Nearest Neighbor:** this classifier, based on the Mahalanobis distance, was proposed by Cho et al. [6]. The distance between a test sample $\mathbf{f}$ and each of the enrollment samples $\mathbf{g^k}$ is calculated as:

$$d_1{}^k = \left(\mathbf{f} - \mathbf{g^k}\right) S^{-1} \left(\mathbf{f} - \mathbf{g^k}\right)^T \qquad (1)$$

  where the covariance matrix of the gallery set, S, is introduced to increase the impact of those features with a smaller variance. The final distance d_2 is obtained as the k closest distance.

- **Modified Scaled Manhattan distance:** this is a modification of the scaled manhattan distance classifier [7]. The distance between a feature vector of the test sample $\mathbf{f}$ and the enrollment set $\mathbf{g}$ is calculated as:

$$d_1 = \|\mathbf{f} - \bar{\mathbf{g}}\|_1 / \boldsymbol{\sigma}' \qquad (2)$$

  where $\boldsymbol{\sigma}'$ is the modified average absolute deviation:

$$\sigma_i{}' = \begin{cases} \frac{0.2}{M}\sum_{k=1}^{M}\sigma_k & if\ \ \sigma_i < \frac{0.2}{M}\sum_{k=1}^{M}\sigma_k \\ \sigma_i & rest \end{cases} \quad (3)$$

This simple modification try to mitigate the effects of samples with very low variance during the normalization (low variance means high weight).

These algorithms were selected among some of the most competitive algorithms tested on the CMU benchmark dataset [8], see Table 1. As we can see, the performance achieved by the two distances is similar with average EER of all subjects ranked between 8.84% and 9.96%.

Table 1. Performance (EER) of the two classifiers using the CMU benchmark dataset. The table also shows the performance of other popular keystroke dynamics algorithms [8]

Classifier	Average EER
Mahalannobis + Nearest Neighbor (d_1)	**0.0996**
Modified Scaled Manhattan distance (d_2)	**0.0884**
z-score [8]	0.1022
SVM [8]	0.1025
Mahalanobis [8]	0.1101
Mahalanobis norm. [8]	0.1101

3.3 Database and experimental protocol

The experiments reported in this work are performed on OhKBIC dataset (available at http://biometric-competitions.com/ mod/competition/dataset.php?id=7). The database includes the responses of 64 students to 3 exams directly typed into the web-platform of the course which logged the keystroke pattern of each of the students (at least 500 keystrokes per exam). The database includes different scenarios depending of the hands used to type: i) typing with both hand; ii) typing only with right hand and iii) typing only with left hand. In our experiments we used the both hand subset as the most realistic scenario (the one hand scenarios simulate challenging conditions, see [5] for details). Therefore we consider here a:

- **Text independent authentication scenario:** the database includes more than 1500 keystroke samples per user. These keystroke samples are the responses to 3 different exams and the text typed depends of the different questions.
- **Multisession experiment:** the data acquisition comprises a semester and the time lapse between exams is approximately two months.

The aim of the experiment is to analyze the performance of keystroke dynamics among the different responses of the students. The experiments try to answer such a question: Can we authenticate the students using an initial subset of keystrokes and a new sequence of keystroke obtained from a different exam? The experimental protocol is summarized as:

- The database is divided into an enrollment set (500 keystroke per student) and evaluation set (203 samples of 500 keystrokes). These subset are provided with the database [5].
- We search for common digraphs and trigraphs (sequences of two and three characters respectively) between the enrollment and evaluation set.
- A cross-validation protocol is applied to measure the distance between the digraphs and trigrapgs from the enrollment and evaluation sets using the keystroke classifier analyzed in section 3.2.
- The final score is obtained as the mean of the best 40 distances (20 digraphs and 20 trigraphs);
- The performance of the overall experiment is provided according the average accuracy in authenticating each user (100-Equal Error Rate). The Equal Error Rate is the point where False Acceptance and False Rejection are equal.

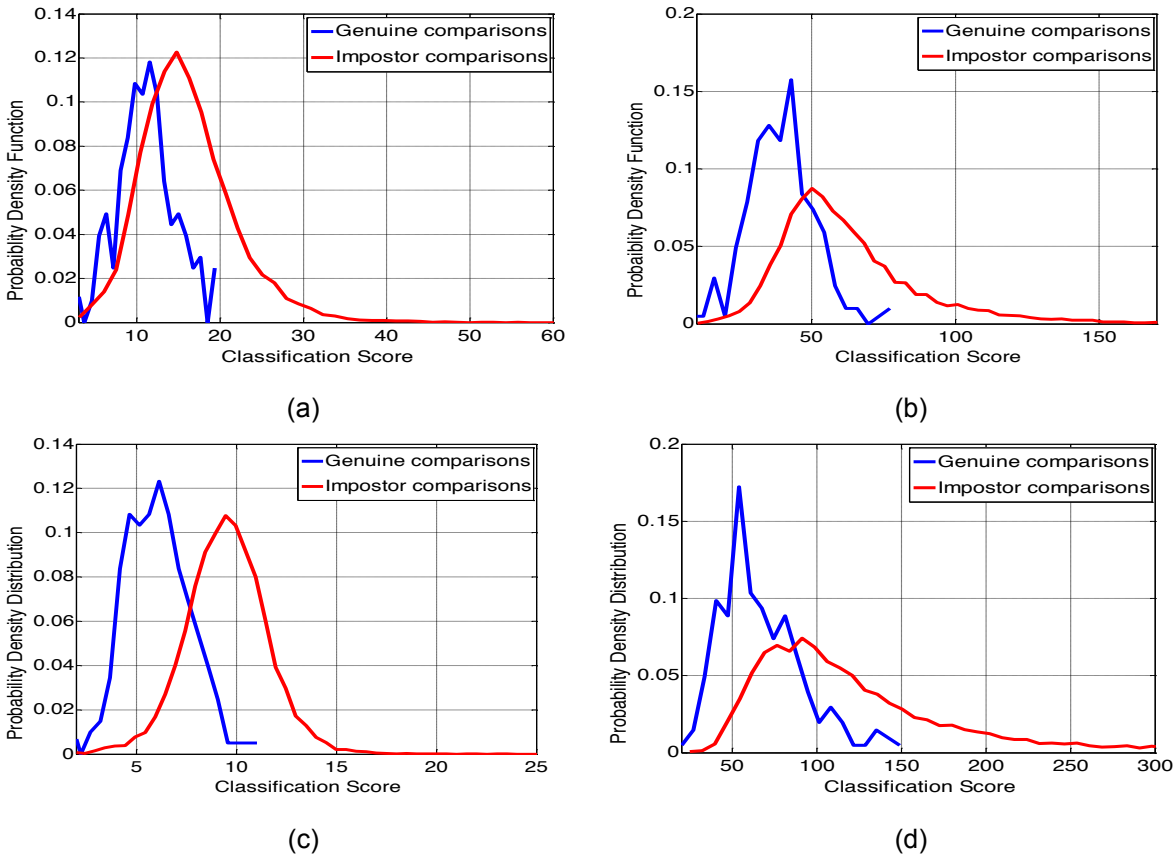

Figure 4. Probability Density Distribution for: digraphs and Modified Scaled Manhattan distance (a); digraphs and Mahalanobis-NN (b); trigraphs and Modified Scaled Manhattan distance (c); trigraphs and Mahalanobis-NN (d)

4 RESULTS

The experiments include the evaluation of two keystroke dynamics classifiers (see section 3.2) and features from keystroke events with two different lengths (digraph and trigraphs). There are two different types of comparisons:

- **Genuine comparisons:** the enrolment samples and the evaluation samples belong to the same student. These comparisons simulate normal access.
- **Impostor comparisons:** the enrolment samples and the evaluation samples belong to different students. These comparisons simulate spoofing attacks.

Fig. 4 shows the probability density distribution of the classification scores obtained from the four experiments. The distributions show large overlap areas between genuine and impostor comparisons. The ideal scenario is when the overlap between distributions is zero which mean separable classes. However, the overlap obtained is different depending of the experiments and it is possible to see large differences between Modified Manhattan distance using digraphs (Fig. 4.a) or trigraphs (Fig. 4.c). The results showed in Table 2 confirm the performance of all 4 systems.

Table 2. Performance (EER) of the four systems for the OhKBIC dataset

Classifier	**Average EER**	
	Digraph	**Trigraph**
Mahalanobis + Nearest Neighbour (d_1)	**0.1543**	**0.1409**
Modified Scaled Manhattan distance (d_2)	**0.2512**	**0.0905**

According our results, the trigraphs clearly outperforms the digraphs and the Modified Scaled Manhattan distance shows the best performance with an EER equal to 9.905%. The superior performance of the trigraphs could be explained by its greater amount of information and the richer patterns obtained. The performance of the distances varies according the length of the key sequence. While the Modified Scaled Manhattan distance is the most competitive using trigraphs, the Mahalanobis + Nearest Neighbour show superior performance for digraphs.

5 CONCLUSIONS

This work analyses the biometric technology for student authentication services in e-learning platforms. We focus on keystroke dynamics technologies including an exhaustive study of the main steps involved in these authentication systems. We performed experiments with an operational databases including the responses of 64 students to 3 different exams over a semester. The results show a promising accuracy with correct authentication over the 90%. However there still room for improvements and it is necessary to increase the size of databases and number of experiments.

REFERENCES

[1] A. Peacock, X. Ke, and M. Wilkerson (2004). Typing patterns: A key to user identification. *IEEE Security and Privacy*, 2(5), pp. 40–47.

[2] D. Gunetti and C. Picardi (2005). Keystroke analysis of free text. *ACM Transactions on Information and System Security*, 8(3), pp. 312–347.

[3] A. Morales, J. Fierrez and J. Ortega-Garcia (2014). Towards predicting good users for biometric recognition based on keystroke dynamics. In *Proc. of European Conf. on Computer Vision Workshops*, Springer LNCS-8926, Zurich, Switzerland, pp. 711-724.

[4] Stanford, Education's digital future (2013). Coursera announces details for selling certificates and verifying identities. Available at: http://edf.stanford.edu/readings/coursera-announces-details-selling-certificates-and-verifying-identities.

[5] J. V. Monaco, G. Perez, C. C. Tappert, P. Bours, S. Mondal, S. Rajkumar, A. Morales, J. Fierrez and J. Ortega-Garcia (2015) . One-handed Keystroke Biometric Identification Competition. *In Proc. IEEE/IAPR Int. Conf. on Biometrics*, ICB, Phuket (Thailand), May 2015, pp. 1-7.

[6] S. Cho, C. Han, D. H. Han, and H. Kim (2000). Web-based keystroke dynamics identity verification using neural network. *Journal of Organizational Computing and Electronic Commerce*, 10(4), pp. 295–307.

[7] L. C. F. Araujo, L. H. R. Sucupira, M. G. Lizarraga, L. L. Ling, J. B. T. Yabu-uti (2005). User Authentication Through Typing Biometrics Features. *IEEE Trans. On Signal Processing*, 53(2), pp. 851-855.

[8] Kevin S. Killourhy and Roy A. Maxion (2009). Comparing Anomaly Detectors for Keystroke Dynamics. In *Proc. of the 39th Annual Int. Conf. on Dependable Systems and Networks (DSN-2009)*, Estoril, Lisbon, Portugal, June 29-July 2, 2009. IEEE Computer Society Press, Los Alamitos, California, pp. 125- 134.