User Dependent Template Update for Keystroke Dynamics Recognition

Abir Mhenni, Estelle Cherrier, Christophe Rosenberger, Najoua Essoukri Ben Amara

User Dependent Template Update for Keystroke Dynamics Recognition

Abir Mhenni*†‡, Estelle Cherrier†, Christophe Rosenberger† and Najoua Essoukri Ben Amara‡
*ENIT, University of Tunis El Manar, BP 94 Rommana 1068 Tunis, Tunisia
Email: abirmhenni@gmail.com
†Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France
Email: estelle.cherrier@ensicaen.fr
Email: christophe.rosenberger@ensicaen.fr
‡LATIS- Laboratory of Advanced Technology and Intelligent Systems, ENISo
University of Sousse, BP 526 4002 Sousse, Tunisia
Email: najoua.benamara@eniso.rnu.tn

***Abstract*—Regarding the fact that individuals have different interactions with biometric authentication systems, several techniques have been developed in the literature to model different users categories. Doddington Zoo is a concept of categorizing users behaviors into animal groups to reflect their characteristics with respect to biometric systems. This concept was developed for different biometric modalities including keystroke dynamics. The present study extends this biometric classification, by proposing a novel adaptive strategy based on the Doddinghton Zoo, for the recognition of the user's keystroke dynamics. The obtained results demonstrate competitive performances on significant keystroke dynamics datasets.**

***Keywords*-Authentication; Password security; Keystroke dynamics; Adaptive strategy; Doddington Zoo; Users classification.**

I. Introduction

The security of password based applications is one of major concerns nowadays regarding the proliferation of web and mobile applications. Moreover, these applications are the target of various hackers attacks according to the recent statistics achieved by Hackmageddon [1]. Keystroke dynamics is an emerging solution to reinforce logical access control. It is a behavioral modality that verifies the typing manner of the user in addition to the verification of the syntactic conformity of the password [2], [3]. The main disadvantage of the keystroke dynamics modality is the variability of the typing manner of users over time [4], [5]. In fact, it changes according to several factors like the user's emotional state, their activeness, the password mastery; etc.

Adaptive strategies, are one of the most interesting solutions to remedy to the intra-class variations [6], [7] for behavioral biometric systems. They consist in updating the biometric reference template describing the typing rhythm of the user at each access verification. These strategies depend generally on five parameters [8]:

- Reference modeling : which defines the representation of the user's model. It can be represented by a single sample, a gallery or a cluster;
- Adaptation criterion : which decides to launch the adaptation process;
- Adaptation mode : which can be supervised or semi-supervised;
- Adaptation periodicity : which can be online or offline;
- Adaptation mechanism : which determines how to apply the modifications to the reference. It can be an additional, replacement or combined mechanism.

These adaptation strategies are promising solutions to intra-class variations for behavioral biometric modality among them the keystroke dynamics one, which we consider in this paper. But, applying the same adaptation mechanism to all users is not the best solution, as the users behaviors are generally different. Doddington Zoo is a concept that ensures users analogy with animal groups [9]. It consists in grouping users according to their behavioral specificities when dealing with the authentication process. For that purpose, we propose a novel adaptation method that is appropriate to the user's typing rhythm. The main contribution of this paper is to propose a user dependent template update strategy based on the Doddington zoo classification. To the best of our knowledge, none work has been done to apply the Doddington zoo concept for updating the reference template of keystroke dynamics data. This methodology is applied on real data coming from two well known datasets in the literature.

The reminder of this paper is organized as follows. In the next section, we present some related works concerning Doddington Zoo categorization. In section III, the proposed adaptive strategy specific to the keystroke dynamics of each user's category is described. Section IV details the experiments and the obtained results. Finally, conclusions

and perspectives are drawn in section V.

II. Related work

Doddington et al. [9] proposed an animal zoo grouping four animals categories, to model users behaviors:

- Sheep: corresponds to users who are easily recognized;
- Goats: describes users who are particularly difficult to recognize;
- Lambs: represents users who are easily imitated;
- Wolves: depicts users who are capable to imitate others easily.

These users classes were differentiated by calculating the False Rejection Rate (FRR) and the False Acceptance Rate (FAR) of each user according to [9]. Referring to Doddingtons menagerie, sheep are characterized by high genuine (similarity) matching scores whereas goats are characterized by low genuine matching scores. Lambs have similar matching problems as goats, by having high impostor matching scores (FAR).

Besides, sheep generally dominate the population of the zoo, goats as well as lambs constitute only a small fraction of the population. However, the wolves category constitutes a large portion of false rejection and acceptance rates.

Further, Yager and Dunstone [10] distinguished four other animal categories of users by considering simultaneously both the genuine and impostor matching scores, for each claimed identity:

- Chameleons: corresponds to users who are easy to recognize and easy to attack. They are a sub-category of goats and lambs;
- Phantoms: depicts the users characterized by rejections of genuine and impostor queries. They are a sub-category of goats class;
- Doves: represents the best users because they are easy to recognize and difficult to attack. Doves are a sub-category of sheep class;
- Worms: regroup the worst users as they are difficult to recognize and easy to attack. Worms are a sub-category of goats and lambs.

Otherwise, in [11], the authors distinguished between the users' classes using the personal entropy and relative entropy for biometric menagerie of online signature verification. Personal entropy is computed using only genuine data. It serves to differentiate between sheeps and goats class of users. Relative entropy is calculated with both genuine and impostor data. It helps to distinguish lambs class. Once these three groups are specified, it is easy to recognize the other groups, as depicted in Figure 1.

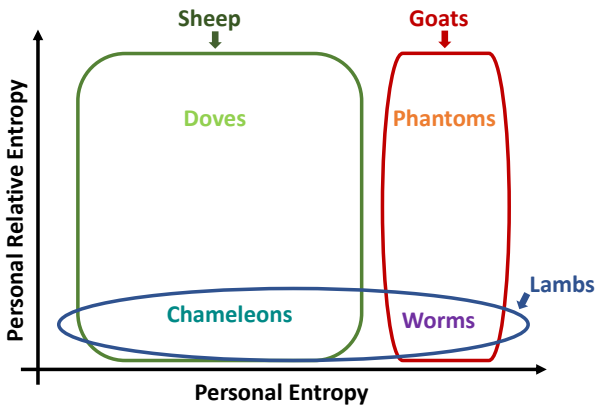


Figure 1: Entropy based classification of the Doddington ZOO animals according to [11].

In this paper, except the wolves group, we consider all of the zoo groups. The wolves group is eliminated because we are not interested in modeling impostors.

III. User dependent adaptation strategy

This paper investigates a novel adaptive strategy that takes into account the specificities of each user to remedy to its intra-class-variations. Figure 2 depicts the proposed authentication process based on the keystroke dynamics modality.

A. Enrollment phase

Two samples are considered initially to register the typing manner of the user. Indeed, for all password-based applications, users are usually asked to type their password and to confirm it when creating an account.

B. Verification phase

During the authentication process, the verification is performed by the K Nearest Neighbor (KNN) classifier based on Hamming, Euclidean, Statistical and Manhattan distances. Afterwards, a vote is ensured by a Genetic Algorithm (GA) to calculate the final score. These distances are chosen because they demonstrated the best performances when compared to other distances as detailed in [12].

C. Adaptation phase

We detail here the different components of the adaption strategy.

1) Reference modeling : At the beginning, the reference template is composed of two samples to remedy to the tedious learning phase while aligning with the account creation process for web and mobile applications. After that, each novel query considered in the adaptation phase is added to the user's reference. Then, we obtain a gallery of samples describing the typing rhythm of the user which

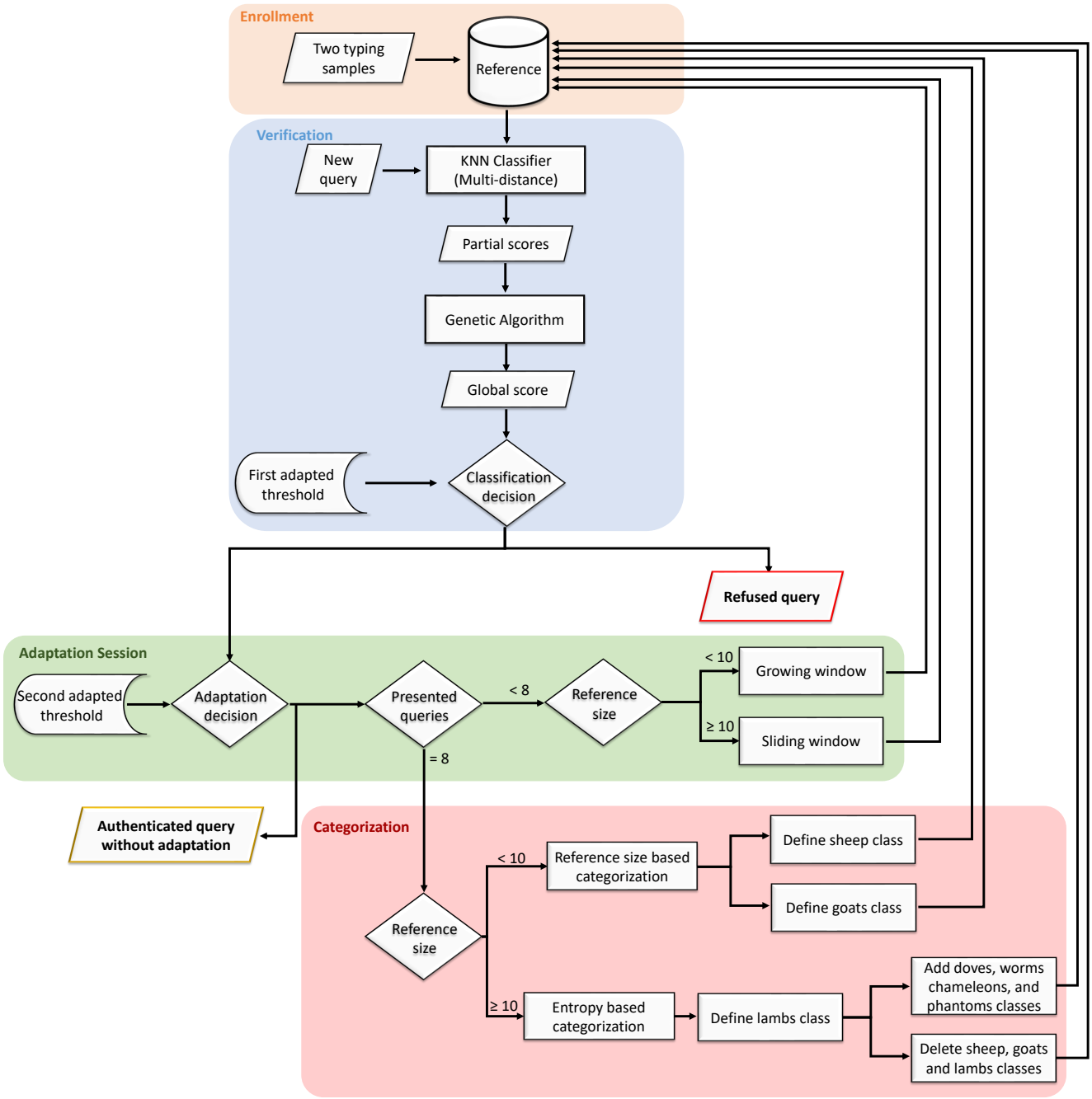


Figure 2: Description of the keystroke authentication process

maximum size is initially set to 10.

2) Adaptation criterion: Different adaptation criteria were proposed in the literature [13], [14], [15]. We are interested in the adapted thresholds criterion that has been proposed in [16]. It has the advantage to use the double threshold verification [13] while maintaining the thresholds user dependent and adapted as time elapses. The adapted thresholds are managed by equation (1).

$$T_j^{i+1} = T_j^i - e^{-\frac{\mu_j}{\sigma_j}} \tag{1}$$

where μ_j is the average of the mean vector of the reference of the user j, σ_j is the standard deviation of the standard deviation vector of the reference of the user j and T_j^i is the threshold value specific to user j during session i.

3) Adaptation mode: The adaptation is ensured in a semi-supervised mode thanks to the KNN classifier combined with the GA. If the global score is lower than the adapted thresholds, the query is used to update the reference.

4) Adaptation periodicity: The adaptation is executed online, immediately after the query acceptation.

5) Adaptation mechanism: Concerning the adopted mechanism, we combine two existing approaches: the growing window and the sliding window mechanisms [17]. These mechanisms are frequently used for keystroke dynamics modality [18], [19]. The growing window mechanism is used to enlarge the size of the reference until the maximum size is reached. The sliding window is afterward considered to maintain a fixed reference size. Hence, the nomenclature is called "double serial mechanism".

D. User classification

During the two first update sessions, we start to classify users into two groups: sheep and goats. We are first interested to only these two groups because we focus on the most representative groups of the Doddington zoo.

Thereby, over the growing window phase, we assume that users, whose number of accepted queries has not overcome 3 samples during the update session, are not easily recognized. So, they are classified as goats. The rest of the users, those whose number of accepted queries is greater than 3, are classified as sheep, as they are easy to recognize.

For the sliding window mechanism, the size of the reference is no more significant as the maximum size of the reference is reached. So, we considered the Entropy measure to distinguish between the considered users groups. In fact, it was demonstrated in [11], [20] that the higher the user's entropy is, the more the error rates increase. Thereby, both Personal and Relative Entropy are calculated according to equations (2) and (3) respectively. For this fact, the Personal Entropy of the reference ref_j containing N samples of the user j is measured according to equation (2):

$$Entropy_j = -\sum_{i=1}^{N} ref_{j_{(t)}}(i) \ \log\left(ref_{j_{(t)}}(i)\right) \qquad (2)$$

The Relative Entropy is equally calculated according to equation (3), where $attaq_j$ is a matrix containing N samples of the keystroke dynamics of multiple users other than the user j:

$$RelativeEntropy_j = \frac{1}{2}\ (\sum_{i=1}^{N} ref_{j_{(t)}}(i) \log(\frac{ref_{j_{(t)}}(i)}{attaq_j(i)}) + \sum_{i=1}^{N} attaq_j(i) \log(\frac{attaq_j(i)}{ref_{j_{(t)}}(i)})\ ) \qquad (3)$$

Therefore, starting from session 4, we use the Entropy to classify users. We initially distinguish the lambs class. Once users of this class are defined, we determine during the following sessions the remaining classes of the zoo. Once session 6 starts, classes of worms, doves, chameleons and phantoms take place and classes of sheep, goats, and lambs disappear.

For each class, we use specific adaptation parameters. Concerning goats and worms classes, which are characterized by a high intra-class variation according to the different conducted experiments, we increased the maximum size of the reference to 15 in order to enrich the description of the keystroke dynamics of the users. The maximum size of phantoms class should be higher because this class is difficult to describe. Regarding the lambs, worms, chameleons and phantoms classes, stricter thresholds are needed to minimize the acceptance of the impostor attacks. These thresholds are generated based on equation (4).

$$T_j^{i+1} = T_j^i - e^{-\frac{\mu_j}{2*\sigma_j}} \qquad (4)$$

The fixed parameters for each user category are detailed in Table I.

Table I: Specific parameters according to user's category

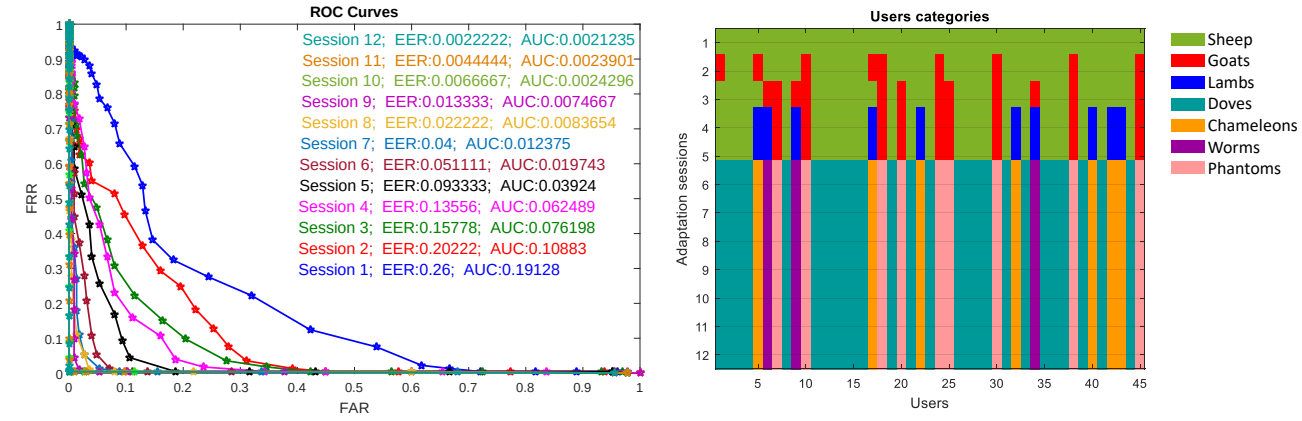
User category	Reference size	Thresholds
Sheep	10	Adapted thresholds
Goats	15	Adapted thresholds
Lambs	10	Stricter thresholds
Worms	15	Stricter thresholds
Chameleons	10	Stricter thresholds
Doves	10	Adapted thresholds
Phantoms	20	Stricter thresholds

IV. Experiments and Results

The proposed approach was tested on two public databases: WEBGREYC and CMU. WEBGREYC [21] database, contains 60 samples from 45 users. The CMU database [22] includes 400 biometric samples of 50 users.

A. Data stream generation

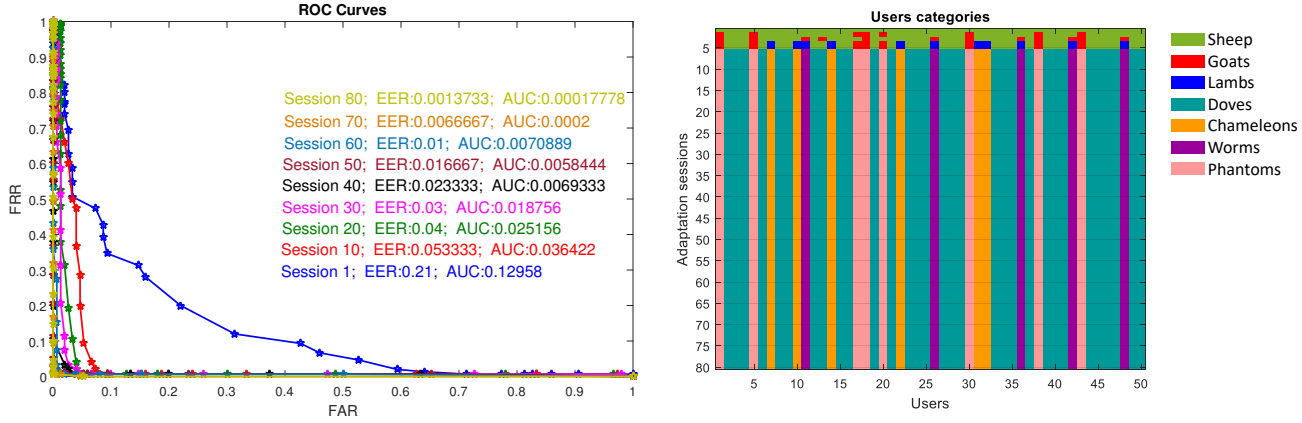
We managed user samples during the adaptation sessions as follows. Two samples of each user are considered during the enrollment phase in order to create the reference. For



(a) Roc curves

(b) Distribution of user classes

Figure 3: Obtained performances and the distribution of users classes for WEBGREYC database.



(a) Roc curves

(b) Distribution of user classes

Figure 4: Achieved performances and the distribution of users classes for CMU database.

each adaptation session, 8 new queries are introduced to the authentication system. These queries are divided into 5 genuine samples and 3 impostor ones. Thus, we considered 12 adaptation sessions for the WEBGREYC database and 80 adaptation sessions for the CMU database.

B. Results and Comparisons

To evaluate the performance of the proposed approach, we consider two evaluation metrics : the Error Equal Rate (EER) and the Area Under Curve (AUC).

The obtained results show an improvement in the performance of the strategy as demonstrated in Figures 3a and 4a. Adding doves, phantoms, chameleons and worms classes, improved the EER performances by 0.6% for the WEBGREYC database and by 0.2% for the CMU database. Furthermore, when compared to the same adaptation approach without biometric menagerie, the user specific adaptation approach ensures an improved EER performance of more then 2% for CMU database and 5% for WEBGREYC database.

We also depict the distribution of users categories among all adaptation sessions for the two considered databases. The sheep class includes the majority of users as shown in Figures 3b and 4b.

To illustrate the benefits of the consideration of 7 classes of the Doddington zoo in the proposed approach, we compared it to the same adaptation approach without biometric menagerie and with the consideration of only 3 classes conducted in [23], namely sheep, goats and lambs. As demonstrated in Tables II and III, the proposed approach show improved performances as it proposes an adaptive strategy that is the most appropriate to the user's specificities. In fact, the considered users' categories encompass a

wider variety of users. Hence, the adaptation method acts according to each user's particularities.

Table II: Comparison of the proposed adaptation strategy for WEBGREYC database

Adaptation strategy	EER	AUC
Without Doddington menagerie	5.3%	0.02
Biometric menagerie based on 3 classes	0.8 %	0.003
Biometric menagerie based on 7 classes	0.2%	0.002

Table III: Comparison of the proposed adaptation strategy for CMU database

Adaptation strategy	EER	AUC
Without Doddington menagerie	2.3%	0.004
Biometric menagerie based on 3 classes	0.3%	0.001
Biometric menagerie based on 7 classes	0.1%	0.0001

V. Conclusion

In this paper, we put forward a user specific adaptation strategy based on the Doddington Zoo concept. It consists in applying an adaptive strategy related to each user class. So, regarding users who suffer from a large intra-class variation, we enlarge the reference size to capture more variabilities. Moreover, for users that are more vulnerable to impostor attacks, we apply stricter thresholds to eliminate as much as possible the false accepted queries in our system.

The Doddington zoo is a biometric menagerie that applies an analogy between users and animals characteristics, and it was efficient for discrimination between users. A large number of the zoo classes is considered in this work, thus demonstrating enhanced performances. Besides, the proposed approach has the advantage of being conform to the web and mobile applications that generally consider only two password acquisitions (the second is to confirm the firts typed one) when creating a new account. So, we consider only these two samples to create the user's reference.

As perspectives to this work, we aim to apply and model impostor attacks to reinforce the security of our authentication system.

References

[1] P. Passeri, "Information security timelines and statistics," *hackmageddon.com*, 2018.

[2] M. Rybnicek, C. Lang-Muhr, and D. Haslinger, "A roadmap to continuous biometric authentication on mobile devices," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2014 International*. IEEE, 2014, pp. 122–127.

[3] R. S. Gaines, W. Lisowski, S. J. Press, and N. Shapiro, "Authentication by keystroke timing: Some preliminary results," DTIC Document, Tech. Rep., 1980.

[4] C. Epp, M. Lippold, and R. L. Mandryk, "Identifying emotional states using keystroke dynamics," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '11. New York, NY, USA: ACM, 2011, pp. 715–724.

[5] A. N. H. Nahin, J. M. Alam, H. Mahmud, and K. Hasan, "Identifying emotion by keystroke dynamics and text pattern analysis," *Behaviour & Information Technology*, vol. 33, no. 9, pp. 987–996, 2014.

[6] L. Didaci, G. L. Marcialis, and F. Roli, "Analysis of unsupervised template update in biometric recognition systems," *Pattern Recognition Letters*, vol. 37, pp. 151–160, 2014.

[7] N. Poh, A. Rattani, and F. Roli, "Critical analysis of adaptive biometric systems," *IET biometrics*, vol. 1, no. 4, pp. 179–187, 2012.

[8] A. Rattani, B. Freni, G. L. Marcialis, and F. Roli, "Template update methods in adaptive biometric systems: A critical review," in *International Conference on Biometrics*. Springer, 2009, pp. 847–856.

[9] G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds, "Sheep, goats, lambs and wolves: A statistical analysis of speaker performance in the nist 1998 speaker recognition evaluation," NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD, Tech. Rep., 1998.

[10] N. Yager and T. Dunstone, "Worms, chameleons, phantoms and doves: New additions to the biometric menagerie," in *IEEE Workshop on Automatic Identification Advanced Technologies*. IEEE, 2007, pp. 1–6.

[11] N. Houmani and S. Garcia-Salicetti, "On hunting animals of the biometric menagerie for online signature," *PloS one*, vol. 11, no. 4, p. e0151691, 2016.

[12] A. Mhenni, E. Cherrier, C. Rosenberger, and N. Essoukri Ben Amara, "Towards a secured authentication based on an online double serial adaptive mechanism of users' keystroke dynamics," in *International Conference on Digital Society and eGovernments (ICDS)*, 2018.

[13] A. Rattani, "Adaptive biometric system based on template update procedures," *Dept. of Elect. and Comp. Eng., University of Cagliari, PhD Thesis*, 2010.

[14] N. Poh, J. Kittler, S. Marcel, D. Matrouf, and J.-F. Bonastre, "Model and score adaptation for biometric systems: Coping with device interoperability and changing acquisition conditions," in *20th International Conference on Pattern Recognition (ICPR), 2010*. IEEE, 2010, pp. 1229–1232.

[15] C. Pagano, E. Granger, R. Sabourin, P. Tuveri, G. Marcialis, and F. Roli, "Context-sensitive self-updating for adaptive face recognition," in *Adaptive Biometric Systems*. Springer, 2015, pp. 9–34.

[16] A. Mhenni, C. Rosenberger, E. Cherrier, and N. Essoukri Ben Amara, "Keystroke template update with adapted thresholds," in *2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), 2016*. IEEE, 2016, pp. 483–488.

[17] P. Kang, S.-s. Hwang, and S. Cho, "Continual retraining of keystroke dynamics based authenticator," *Advances in biometrics*, pp. 1203–1211, 2007.

[18] R. Giot, C. Rosenberger, and B. Dorizzi, "Hybrid template update system for unimodal biometric systems," in *Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. IEEE, 2012, pp. 1–7.

[19] P. H. Pisani, A. C. Lorena, and A. C. de Carvalho, "Adaptive approaches for keystroke dynamics," in *International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2015, pp. 1–8.

[20] A. Morales, J. Fierrez, and J. Ortega-Garcia, "Towards predicting good users for biometric recognition based on keystroke dynamics," in *European Conference on Computer Vision*. Springer, 2014, pp. 711–724.

[21] R. Giot, M. El-Abed, and R. Christophe, "Web-based benchmark for keystroke dynamics biometric systems: A statistical analysis," in *Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*. IEEE, 2012, pp. 11–15.

[22] K. S. Killourhy and R. A. Maxion, "Comparing anomaly detectors for keystroke dynamics," in *Proc. of the 39th International Conference on on Dependable Systems and Networks*, pp. 125–134.

[23] A. Mhenni, E. Cherrier, C. Rosenberger, and N. Essoukri Ben Amara, "Adaptive biometric strategy using doddington zoo classification of user's keystroke dynamics," in *14th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2018.