Adaptive Biometric Strategy using Doddington Zoo Classification of User's Keystroke Dynamics

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

Adaptive Biometric Strategy using Doddington Zoo Classification of User's Keystroke Dynamics

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*—Securing personal, professional and even official data is a very critical issue nowadays, giving that these informations are safeguarded in different devices (mobile, computer) and various accounts (social networks, e-mails). To protect them from unauthorized acess, users generally are asked to use passwords. But using only these authentication solutions is no longer efficient against hacker attacks. Keystroke dynamics is a biometric promising modality that guarantees the recognition of the user's characteristics; his typing manner on the keyboard. Regarding that the typing rythm of the user changes over time, adaptive biometric solutions help to take into consideration these variations. In this paper we classify user into multiple categories according to Doddonghton Zoo classification. Afterwards, we apply an adaptive strategy specific to each category of users. The achived experiments demonstrate that an update strategy specific to the user class has improved significantly the obtained performances.**

***Index Terms*—Authentication; Password security; Keystroke dynamics; Adaptive strategy; Doddonghton Zoo; Users classification.**

I. Introduction

Industrialists as well as researchers in the field of Information Technology (IT) are more and more interested to the security of IT Services. Thus, different authentication mechanisms has been proposed and used to ensure the needed security. It is generally based on what the user knows like passwords and passcodes, or what the user has like cards [1].

Biometric modalities are becoming more widespread as a solution to enhance the authentication solutions such as the fingerprint (*e.g.*, fingerprint scanner [2], Touch ID [3], etc.), the face and the iris modalities that are used based on video cameras on mobile devices [4]. Keystroke dynamics is a behavioral modality non intusive, inexpensive and weakly constrained for the user [5], [6]. It consists in combining the verification of the syntactic password accuracy with the confirmity of the typing manner of the user which is usually described with latencies latencies [7]. The latter are obtained by calculating the time difference between pressure and release instants corresponding to two or three successive keys.

The major drawback of this modality is that it suffer from large intra-class variation [8], [9]. In fact, the keystroke dynamics of the user varies as time elapses according to different situations. This variability may be due to the familiarity with the password after a time span, the user's humor and activennes and the changing of the keyboard (AZERTY or QWERTY, virtual or physical).

Adaptive strategies [10], [11] also known as template update strategies are an interesting solution to overcome the intra-class variability. It consistsin updating the user's reference during the use of the system. Different adaptive mechanisms has been proposed to update the reference of the user. We quote the additive mechanisms [12] and the replacement mechanisms [13], [14]. The Growing window mechanism [15] is one of the additive mechnaisms which adds each accepted query to the user's reference . The sliding window mechanism [15] is a replacemet adaptation mechanism that replaces the oldest sample in the user's reference with the newly accepted query whereas the least frequently used mechanism [14], [13] replaces sample in the reference which is the least frequently used in the verification system.

Communly, one of these mechanisms is applied to all users of the authetication system. While, a biometric system's performance is subject dependent[16]. That is why, we decided to use an update strategy for each category of users in ths work. For that, we are interested in the users' classification based on the Doddington Zoo [17]. It is a commonly used theory for user classification [18], [19] but, to our knowledge, it has not been mixed with adaptive strategies for keystroke dynamics modality. The common users' classes are :

- sheeps: users who can easily be recognised;
- goats: users who are particularly difficult to recognise;
- lambs: users who are easy to imitate;
- wolves: users who can easily imitate others.

Several methodologies have been proposed to distinguish between this variety of users. Doddington et al considered his classification based on the mean of the user's genuine or impostor scores. Users classified as Goats increase the False Reject Rate (FRR) of the recognition system whereas wolves and lambs increment its False Acceptance Rate (FAR).

Others [20] proposed personal entropy and relative entropy for biometric menagerie of online signatures verification. Personal entropy is computed using only genuine data. It serves to differentiate between sheep and goat class of users. Relative entropy is calculated with both genuine and impostor data. It helps to distinguish lambs class.

This paper investigates an authentication method based on an only one sample of the user's keystroke dynamics in the enrollement phase. During the use of the authentication system, the reference is enriched thanks to the chosen adaptive strategy. Users classification into Doddington Zoo categories is firstly based on the evolution of the user's reference size over time. Once the maximum size of the refence is reached, the users categorization is ensured with the personal and the relative entropy claculation.

In the next section we introduce the proposed adaptive strategy specific to each category of users. Section III describe the experimental protocol and the obtained results. Finally, conclusions and perspectives are drawn in section IV.

II. Proposal of an adaptive strategy specific to the user's category

This section presents an adaptive strategy based on Doddington Zoo classification. The main idea consists in grouping users according to their performance evolution over time. Then, we put forword an adaptive strategy specific to each category of users to ensure the usability of the keystroke dynamics modality. In the present work, three categories among the animal based categories are considered: sheeps, goats and lambs. Wolves class has been eliminated because we are not interested in modeling hackers.

For the enrollement phase an only one sample is considered to store the typing manner characteristics of each user. Afterwards, during the use of the authentication systems, the presented queries are classified based on the K Nearest Neighbor (KNN) classifier with multiple distances. Before making the acceptance decision, a vote is ensured to reckon with all obtained scores. If the query is classified as geninuine, it is used to update the user's reference. This process is achieved in an online way according to the algorithm 1.

Three adaptive mechanisms are considered for our process. The growing window mechanism is firstly considered when the maximum size of the reference is not reached. Once the size of the user's reference is equal to the fixed maximum size, the sliding window mechanism is lunched. Otherwise, the least frequently mechanism is used when the size of the user's reference is higher then the fixed maximum size. This is the case where the user migrates from the class of goats to that of sheeps. The least frequently mechanism is used to decrease the size of the reference from 15 to 10. Thus, the 5 least frequently used samples of the reference are deleted.

Some parameters and choises of the strategy need to be redefined and updated during the system's operation. So we divided the process into sessions. Each session consists in presentation of 8 new queries: 5 geniune queries and 3 impostor ones.

Algorithm 1: Template update strategy for user j during an adaptation session.

```
Require:
    $ref_{j(t)}, \mathcal{A} = \{\mathbf{q}\}, \theta_j^{adapt} = \{label^p, maxSize(ref_{j(t)})\}$
Ensure: $ref_{j(t+1)}$
    nq ← 0    Number of accepted queries during the session
    $N \leftarrow size(ref_{j(t)})$
    $score1 \leftarrow similarityScore(KNN_{Hamming}(ref_{j(t)}), \mathbf{q})$
    $score2 \leftarrow similarityScore(KNN_{Euclidean}(ref_{j(t)}), \mathbf{q})$
    $score3 \leftarrow similarityScore(KNN_{Statistical}(ref_{j(t)}), \mathbf{q})$
    $score4 \leftarrow similarityScore(KNN_{Manhattan}(ref_{j(t)}), \mathbf{q})$
    $Score_j = \alpha \times score3 + \beta \times score1 + \gamma \times score2 + \delta \times score4$
    if ( $Score_j < adaptatedThreshold$ ) then
        nq ← nq + 1
        if ( $N < maxSize(ref_{j(t)})$ ) then
            $ref_{j(t+1)} \leftarrow adaptGrowingWindow(ref_{j(t)}, \mathbf{q})$
        else if ( $N == maxSize(ref_{j(t)})$ ) then
            $ref_{j(t+1)} \leftarrow adaptSlidingWindow(ref_{j(t)}, \mathbf{q})$
        else
            $ref_{j(t+1)} \leftarrow adaptLeastFreqUsed(ref_{j(t)}, \mathbf{q})$
        end if
    end if
```

At the end of each session, a parameters' adjustment is performed to optimize performance and ensure smooth operation:

• *Users are assigned to one of the three defined categories according to their characteristics:* During the growing window phase, the size of the reference is an important indicator regarding the category of the user. Indeed, if the size of the reference of the user remains small, this means that the number of accepted queries is very small. These users belong to the category of **goats** which are known as being difficult to recognize. The other part of the users, can be considered belonging to the **sheep** category since they are easily recognized.

However, during the sliding window phase, the distinction of the user's categories is based on the Entropy measure. First, the Personal Entropy is measured by means of local density estimation according to equation (1).

$$PersonalEntropy_j = -\sum_{i=1}^{N} ref_{j(t)}(i)\ \log\left(ref_{j(t)}(i)\right) \quad (1)$$

If the Personal Entropy is under 0.2, then the user is classified as a **sheep**. Otherwise the user is considered as a **goat**. Additionally, the objective of this work requires assessing the vulnerability of a user to attacks. For this reason, we propose another quality measure, namely Relative Entropy, which allows a user to be characterized not only in terms of keystroke dynamics variability, as Personal Entropy does, but also in terms of how difficult it is to attack such a typing manner. In fact, Relative Entropy defined in Equation (2), aims to recognise users belonging to **lambs** class. If the value of this entropy is low, the user is more vulnerable to attacks.

Thereby, if the user's Relative Entropy is under 6, is classified as a lamb.

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

where $attaq_j$ is a matrix containing N samples of the keystroke dynamics of multiple users other than the user j.

Algorithm 2: Assign users to specific classes at the end of the session.

```
Require: $ref_{j_{(t)}}, attaq_j$
Ensure: $goatsClass, sheepsClass, lambsClass$
  if $N < maxSize(ref_{j_{(t)}})$ then
    if nq $< 3$ then
      $goatsClass \leftarrow goatsClass \cup \{user_j\}$
    else
      $sheepsClass \leftarrow sheepClass \cup \{user_j\}$
    end if
  else
    $personalEntropy_j \leftarrow Entropy(ref_{j_{(t)}})$
    if $personalEntropy_j < 0.2$ then
      $sheepsClass \leftarrow sheepClass \cup \{user_j\}$
    else
      $goatsClass \leftarrow goatsClass \cup \{user_j\}$
    end if
    $RelativeEntropy_j \leftarrow RelativeEntropy(ref_{j_{(t)}}, attaq_j)$
    if $RelativeEntropy_j < 6$ then
      $lambsClass \leftarrow lambsClass \cup \{user_j\}$
    end if
  end if
```

- *The vote parameters are controlled:* The parameters $(\alpha, \beta, \gamma, \delta)$ are generated by the Genetic Algorithm (GA) based on its parameters detailed in TABLE I. At the end of the first update session, after the creation of the three categories of users, these parameters are generated to each category of users separately. At the end of each session, the vote parameters are updated thanks to the GA to fit the variation of each category population.

TABLE I: Parameters of the Genetic Algorithm

Parameter	Value
Population size	50 (numberOfVariables ≤ 5)
Crossover Fraction	0.8
Generation	400 (100*numberOfVariables)
Elite count	2.5 (0.05*PopulationSize)
Fitness Function	Minimizing the False Rejection Rate (FRR) and the False Acceptance Rate (FAR)
Selection Function	Stochastic uniform
Crossover Function	Crossover Scattered
Mutation Function	Gaussian

- *The used thresholds are updated:* The thresholds of acceptance and adaptation decision are adapted according to Equation (3). These thresholds are individual and adapted from one update session to another [6].

$$T_j^{i+1} = T_j^i - e^{-\frac{\mu_j}{\sigma_j}} \tag{3}$$

For all categories of the treated user, we applied the double serial adaptive mechanism. Nevertheless, according to the class to which the user belongs, there are differences in the update strategie which are summerised in TABLE II.

- For the **sheep** class standard settings are specified. The maximum size of the reference is fixed to 10, and the thresholds are adapted according to Equation (3).
- For the **goats** which are known with the high intra-class variability, the description of its typing manner needs to be richer than that of other categories. For that, we have increased the maximum size of the reference of this user class to 15.
- Concerning the **lambs**, which are the most susceptible to attacks as they are easy to imitate, stricter thresholds for the selection of new queries is the appropriate strategie. Thus, the thresholds of acceptance and update decision are updated according to Equation (4).

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

TABLE II: Specific parameters according to user's category

User category	Reference size	Thresholds
Sheep	10	Adapted thresholds
Goats	15	Adapted thresholds
Lambs	10	Stricter thresholds

III. Experiments and results

The proposed approach is validated in two public datasets. The WEBGREYC [21], 45 user participated in five sessions of the database, typed the same password ”SÉSAME” and provided 60 patterns. The CMU [22]: This database includes data of 30 users that typed the same password 400 times during eight acquisition sessions. The defined password is ”.tie5Roanl”. Thus we obtained 12 adaptation sessions for the WEBGREYC database (60/5) and 80 adaptation sessions for the CMU database (400/5).

To evaluate the performances of the proposed methos we used the the Error Equal Rate (EER) and the Area Under Curve (AUC) metrics. The Receiver Operating Characteristic (ROC) curves for the two considered databases are deicted in Fig. 1 and Fig. 2. The achieved performances are promissing as the EER of the last adaptation session of the WEBGREYC, CMU database is equal to 0.8%, 0.3% respectively.

Furthermore, we illustrated the variation of the size of users' references during the use of the system in Fig. 3 andFig. 4. It is an indicator of the users' categories during the adaptation sessions.

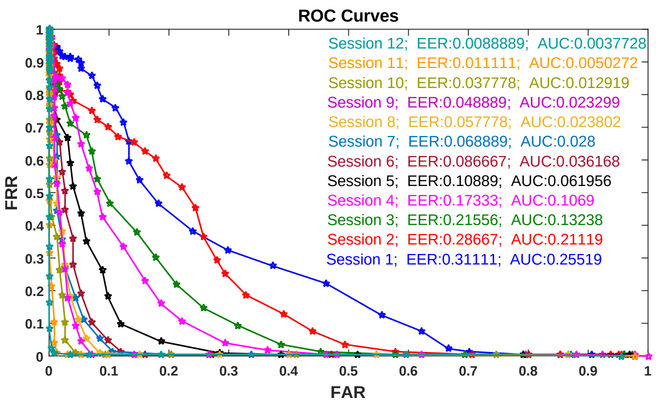

Fig. 1: Illustration of ROC curves and the associated EER and AUC performances of each adaptation session for WEBGREYC database.

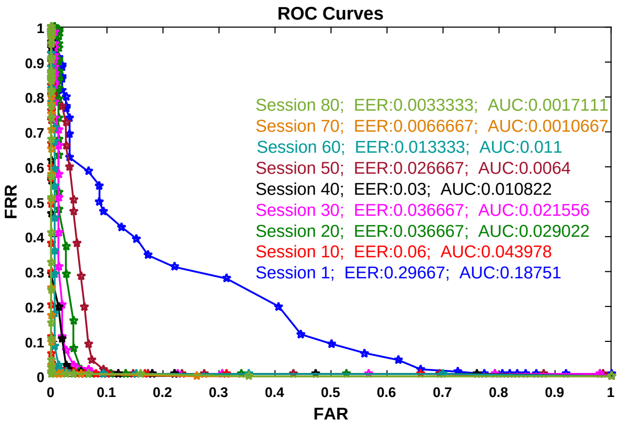

Fig. 2: Illustration of ROC curves and the associated EER and AUC performances of each adaptation session for CMU database.

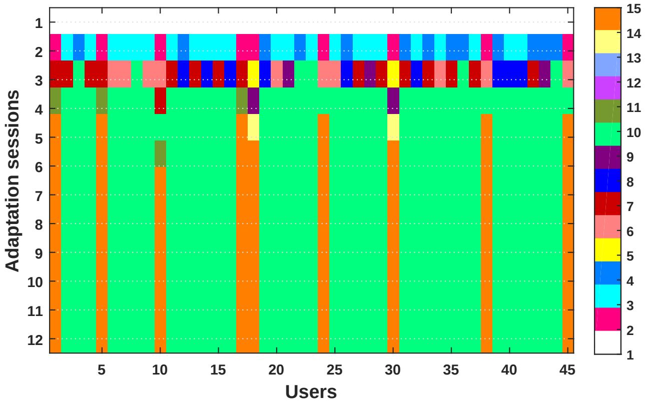

Fig. 3: Size variations of users' galleries during all adaptation session for WEBGREYC database.

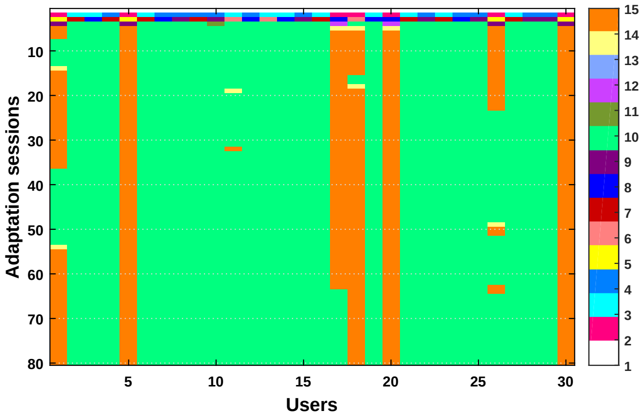

Fig. 4: Size variations of users' galleries during all adaptation session for CMU database.

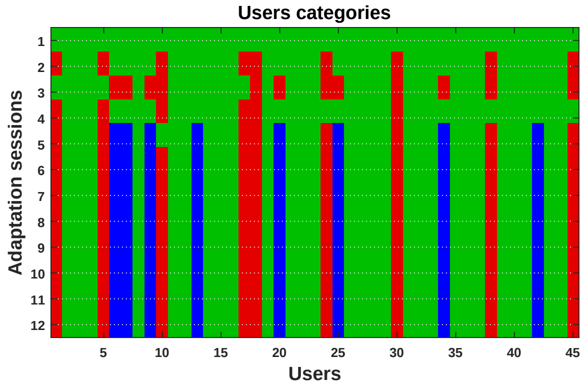

Fig. 5: Distribution of users categories during all adaptation session for WEBGREYC database. The green color illustrates the sheeps class, the red color illustrates the goats class and the blue color illustrates the lambs class.

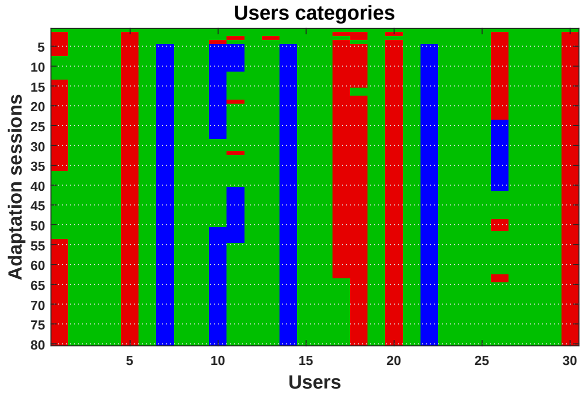

Fig. 6: Distribution of users categories during all adaptation session for CMU database. The green color illustrates the sheeps class, the red color illustrates the goats class and the blue color illustrates the lambs class.

The distribution of users categories among all adaptation sessions is also illustrated in Fig. 5 and Fig. 6. The sheep class represents the majority of users for both databases. Goats class represent approximately 0.2% for WEBGREYC AND CMU databases. Lams class represnt 0.15% for WEBGREYC database and 0.16% for CMU database.

IV. Conclusion and future work

In this work, we put forward a novel authentication method that helps to reinforce the security of IT services. Based on keystroke dynamics modality, the proposed method helps password based application to overcome hacking attacks. Indeed, the adaptive strategy specific to the user's category presnts many advantages. First, the recognition of the user category according to the animal based categories of the Doddington Zoo, helps to distinguish the user's specificities. Then an adaptive strategy that remedy the problems of the user class is adopted. So, three different adaptive mechanism are simultaneously used : the growing window mechanism, the sliding window mechanism and the least frequently used mechanism.

Another important benefit of the proposed method is the minimization of the size of the reference. As it is user dependent, a gain in memory used is ensured. Only users with a large intra-class variation (Goats), have a larger reference size. Moreover, users who are more vulnerable to hacker attacks (lambs), are given stricter decision thresholds. Despite this choice minimizes the capture of intra-class variation of these users, since only the most similar data are considered, but it protects them against attacks which are their weak point.

The accomplished results demonstrate competitive performances with an EER equal to 0.8% and 0.3% for the WEBGREYC and the CMU database respectively.

References

[1] A. Mansour, M. Sadik, E. Sabir, and M. Jebbar, "Ambas: An autonomous multimodal biometric authentication system," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International*. IEEE, 2017, pp. 2098–2104.

[2] B. Fernandez-Saavedra, R. Sanchez-Reillo, R. Ros-Gomez, and J. Liu-Jimenez, "Small fingerprint scanners used in mobile devices: the impact on biometric performance," *IET Biometrics*, vol. 5, no. 1, pp. 28–36, 2016.

[3] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, p. 28, 2015.

[4] D. F. Smith, A. Wiliem, and B. C. Lovell, "Face recognition on consumer devices: Reflections on replay attacks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 736–745, 2015.

[5] 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.

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

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

[8] 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.

[9] 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.

[10] 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.

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

[12] A. Rattani, G. L. Marcialis, and F. Roli, "Biometric system adaptation by self-update and graph-based techniques," *Journal of Visual Languages & Computing*, vol. 24, no. 1, pp. 1–9, 2013.

[13] B. Freni, G. L. Marcialis, and F. Roli, "Replacement algorithms for fingerprint template update," in *Image Analysis and Recognition*. Springer, 2008, pp. 884–893.

[14] T. Scheidat, A. Makrushin, and C. Vielhauer, "Automatic template update strategies for biometrics," *Otto-von-Guericke University of Magdeburg, Magdeburg, Germany*, 2007.

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

[16] N. Poh, J. Kittler, C.-H. Chan, and M. Pandit, "Algorithm to estimate biometric performance change over time," *IET Biometrics*, vol. 4, no. 4, pp. 236–245, 2015.

[17] 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.

[18] A. Ross, A. Rattani, and M. Tistarelli, "Exploiting the doddington zoo effect in biometric fusion," in *Biometrics: Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on*. IEEE, 2009, pp. 1–7.

[19] 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.

[20] 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.

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

[22] K. Killourhy and R. Maxion, "Why did my detector do that?!" in *International Workshop on Recent Advances in Intrusion Detection*. Springer, 2010, pp. 256–276.