Keystroke Dynamics based User Authentication using Deep Learning Neural Networks

Yris Brice Wandji Piugie, Joël Di Manno, Christophe Rosenberger, Christophe Charrier

Keystroke Dynamics based User Authentication using Deep Learning Neural Networks

Yris Brice Wandji Piugie*†, Joël Di Manno*, Christophe Rosenberger† and Christophe Charrier†
*FIME EMEA, 14000 Caen, France
brice.wandji@fime.com, joel.dimanno@fime.com
†Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France
christophe.rosenberger@ensicaen.fr, christophe.charrier@unicaen.fr

***Abstract*—Keystroke dynamics is one solution to enhance the security of password authentication without adding any disruptive handling for users. Industries are looking for more security without impacting too much user experience. Considered as a friction-less solution, keystroke dynamics is a powerful solution to increase trust during user authentication without adding charge to the user. In this paper, we address the problem of user authentication considering the keystroke dynamics modality. We proposed a new approach based on the conversion of behavioral biometrics data (time series) into a 3D image. This transformation process keeps all the characteristics of the behavioral signal. The time series do not receive any filtering operation with this transformation and the method is bijective. This transformation allows us to train images based on convolutional neural networks. We evaluate the performance of the authentication system in terms of Equal Error Rate (EER) on a significant dataset and we show the efficiency of the proposed approach on a multi-instance system.**

***Index Terms*—Behavioral biometrics, keystroke dynamics, user authentication, security, convolutional neural networks.**

I. Introduction

The development of Information and Communication Technologies (ICT), as well as improvements in ambient intelligent technologies, such as sensors and smart phones, have led to the rapid development of smart environments [1], [2]. Considerable resources can be saved if sensors can help staff record and monitor users or automatically report any abnormal behavior [2], [3]. For example, in payment systems, in order to ensure the application of strong customer authentication, it is necessary to require adequate security features[1] based on authentication factors such as knowledge, possession, inherent or biometric factors [4]. Knowledge factors rely on information that the user knows such as a password, PIN, or shared secret. Possession factors are based on an element, an object that the user possesses such as a smart card, a USB key, a smartphone, a security token. Inherent or biometric factors are the only factors that are directly related to the user. These factors are useful in reducing the risk that elements such as algorithm specifications, key length, and information entropy will be discovered, disclosed, and used by unauthorized parties [5]. When Multi Factor Authentication (MFA) is requested, using Seamless biometrics, as behavioral, improve the security without decreasing the User Experience (UX). Increasing performance of such biometrics is a high need of current industrials.

Biometrics is now a common solution for user authentication for logical access control, as for example when browsing the Internet on a laptop [5]. There are two main biometrics modalities namely morphological and behavioral. Behavioral biometrics is the process of measuring user's behavioral tendencies resulting from both psychological and physiological differences between individuals. Behavioral methods include keystroke dynamics, mouse dynamics, voice recognition, gait, signature verification and Graphical User Interface (GUI) usage analysis [2]. Due to the variability of the human body and mind, the adoption of this type of biometrics has lagged behind physiological biometrics [6].

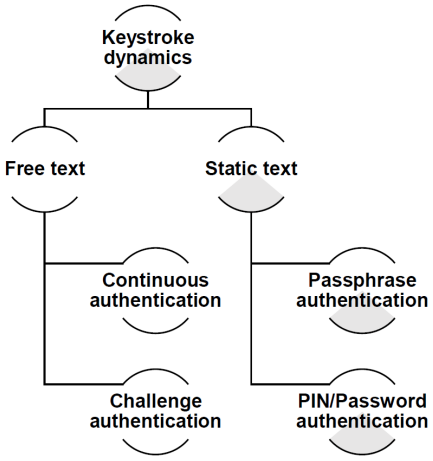

Figure 1: Overview of the different use cases of keystroke dynamics systems.

Keystroke dynamics is a behavioral biometric modality consisting in analyzing the way a user types on a keyboard [7]. Figure 1 gives the different use cases of keystroke dynamics. In this work, we focus on passphrase authentication where all users type the same password. The authentication is realized by only analyzing the way of typing. This approach is convenient for users as no password has to be remembered but is more challenging for research in term of performance.

[1]http://data.europa.eu/eli/reg_del/2018/389/oj

The proposed method is to implement an authentication system using a behavioral biometric modality : keystroke dynamics.

We assume that by extracting only the keystroke characteristics of each user, it is possible to apply a promising and low cost authentication system compared to many others biometric systems, as it does not require any additional sensor and is easy for the user to perform [8]. Keystroke dynamics as a behavior biometric modality is described by the way of typing on a keyboard (on a laptop) *i.e.*, times computed for key events on the keyboard. Since keystroke dynamics allows to profile users by the way they type on a keyboard, the use of characteristics such as typing behaviours shows that it is possible to identify or authenticate a person knowing his/her typing style [5] . Besides, research has been conducted in recent years to find the best algorithm to perform the authentication task. In this paper, we intend to answer how well deep learning approaches could perform for passphrase user authentication by using keystroke dynamics data. In this work, an image transformation is applied to keystroke dynamics considered as time series, before applying deep learning architectures.

We propose a proof of concept implementation and we study the performance of different deep learning architectures.

The paper is organized as follows. Section II contains related work on authentication from keystroke dynamics systems. Section III presents the proposed method and the different deep learning models with the specifications and the impact of different parameters on our evaluation system. Section IV draws the experimental protocol. Section V details the experiments on benchmark datasets and the results we obtained. Section VI gives the conclusions of this work and some perspectives.

II. Related work

In the literature, most of works are based on conventional machine learning for user authentication (based on behavioral biometric modality). Although the proposed algorithms are excellent, the results can be improved. Therefore, this research proposed an image architecture (for a chosen behavioral biometric modality) and a deep learning authentication process using neural networks for user authentication based on a passphrase.

A. Authentication factors

Keystroke dynamics can be used for different goals (identification, authentication, soft biometrics) in different cases (free text, fixed text, same-text) [2], [16]. Like any biometric solution, keystroke dynamics systems require sets of prior knowledge (references) that are used to verify the newly acquired data (sample). For identification and authentication, a reference describes the typing style of a specific user, while for soft biometrics, a reference describes the typing style of a set of users (e.g., male, female, left/right handed). The references are then used to retrieve, or verify, the identity of the user who typed from a sample [17].

B. Keystroke dynamics

Keystroke typing dynamics allows to profile users (identification, authentication, gender recognition, profiling) by analyzing the way a user is typing on a keyboard as for example when surfing on the Internet. Keystroke dynamics was first used in 1975 [18] and the basic idea was to use a keyboard to automatically identify individuals. In the preliminary report dressed by Gaines et al. [19], seven secretaries typed several paragraphs of text and the researchers showed that it was possible to differentiate users by their typing habits [20].
Keystroke dynamics can be a multi-factor authentication scheme as we combine the knowledge of a password and the way of typing. In case of attack, it can be revoked by changing the password. Nevertheless, some studies showed it is possible to profile users on Internet (gender recognition, age category) [21] without the consent or awareness of the users [2], [20]. Many studies have shown that it is possible to authenticate an individual by typing on a mobile device or keyboard. Table I lists the main works undertaken by researchers to develop neural network based authentication systems. We can note that these works are tested on small databases. In this work, we want to study how recent deep learning methods can improve these results on a representative dataset. We detailed the proposed approach in the next section.

III. Proposed architecture

We describe the proposed system based on keystroke dynamics in Figure 2. It is composed of different steps namely data collection (signal-to-image transformation), features extraction and verification process. We detail in the following sections these steps.

A. Signal processing : matrix representation

Time series analysis in the frequency domain plays an essential role in signal processing. The same is true for image analysis in the frequency domain, which plays a key role in computer vision and was even part of the standard pipeline in the early days of deep learning [22]. In this paper, we propose a new method by transforming the time series (behavioral biometric signal) into an image, *i.e.*, we convert a keystroke dynamics vector of size $1 \times m$, into a matrix of size $n \times n$ such that: $m = n \times (n-1)/2$. This is done though *squareform()* [2] function in MatLab.
One of the properties of the *squareform()* function is to convert a distance vector into a distance matrix, and vice versa.

Conversely, the squareform of matrix V is vector x. The *squareform()* function is bijective.

[2]https://fr.mathworks.com/help/stats/squareform.html

Table I: Overview of keystroke dynamics for user authentication-related work using neural networks

Study	Features	Classification	Testing type	Env.	#Users	Samples	EER
Andrean *et al.* [9]	Latency, Trigraph/N-graph	MLP	Static, Dynamic	Controlled	51	400	16.14%
Lu *et al.* [10]	Latency, Trigraph/N-graph	CNN+RNN	-	Controlled	260	-	05.97%
Çeker *et al.* [11]	-	CNN	Static, Dynamic	Controlled	133	-	06.50%
Alpar [12]	Trigraph/N-graph	Gauss-newton based neural network	-	-	13	780	05.10%
Roth *et al.* [13]	Digraph/N-graph	Digraph Static	Static, Dynamic	Controlled	50	-	11.00%
Harun *et al.* [14]	Latency	NN, dist. classifier	Static	Controlled	15	150	22.90%
Revett *et al.* [15]	Latency, Trigraph/N-graph	Specht Probabilistic NN	Static	Controlled	50	10000	05.70%

In a database sample composed of 110 users, time series composed of 378 features is represented by a matrix of size 28 $\times$ 28. The matrix is displayed with *imagesc()* [3] function in MatLab which display image with scaled colors. We finally have a 3D image on RGB format. Figure 3 shows the step-by-step instructions when computing the time series into an 3D matrix image. The transformation is done on each sub-database separately and on the fusion of sub-databases in order to build a new database of images.

70% of the obtained images were used for training (enrollment)and the remaining 30% were used for validation (verification) both on deep models used for user classification and feature extraction. The matrix representation for user's behavioral typing time series transformation is illustrated in Figure 3. This signal to image transformation allow us to use the 2D convolutional networks to build feature vectors. This will allow us to compare these feature vectors to the reference template vectors to compute the performance metric.

B. Deep learning architectures

Deep learning algorithms have been used in recent years in several fields and are becoming more and more widespread [23], [24].

In this work, we used six deep networks namely ResNet-101, DarkNet-53, GoogleNet, ShuffleNet, DenseNet-201 and SqueezeNet that are models pretrained on a subset of the ImageNet database[4]. In the literature, these are the most recent successful deep learning architectures for image classification [25] since authentication is the result of a classification problem. Table II gives the architecture and the optimization hyper-parameters for the six used deep networks where the network depth is defined as the largest number of sequential convolutional or fully connected layers on a path from the input layer to the output layer. The inputs networks take RGB images format. We used these convolutional networks to build a features vector as output, which is then compared to the reference/test model.

[3]https://fr.mathworks.com/help/matlab/ref/imagesc.html

[4]https://image-net.org

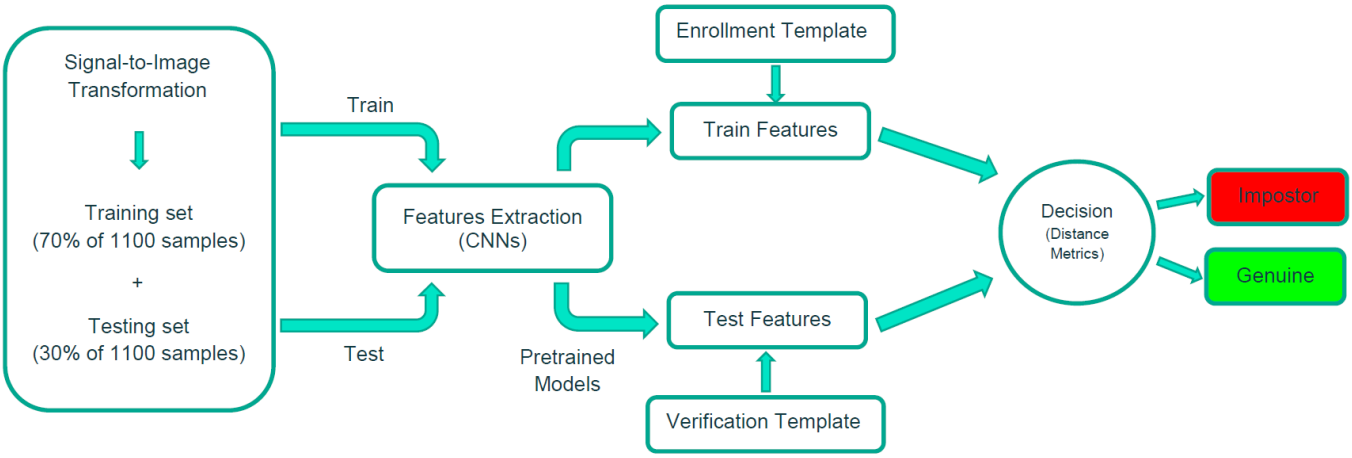

Figure 2: Architecture of our proposed keystroke dynamics based authentication system.

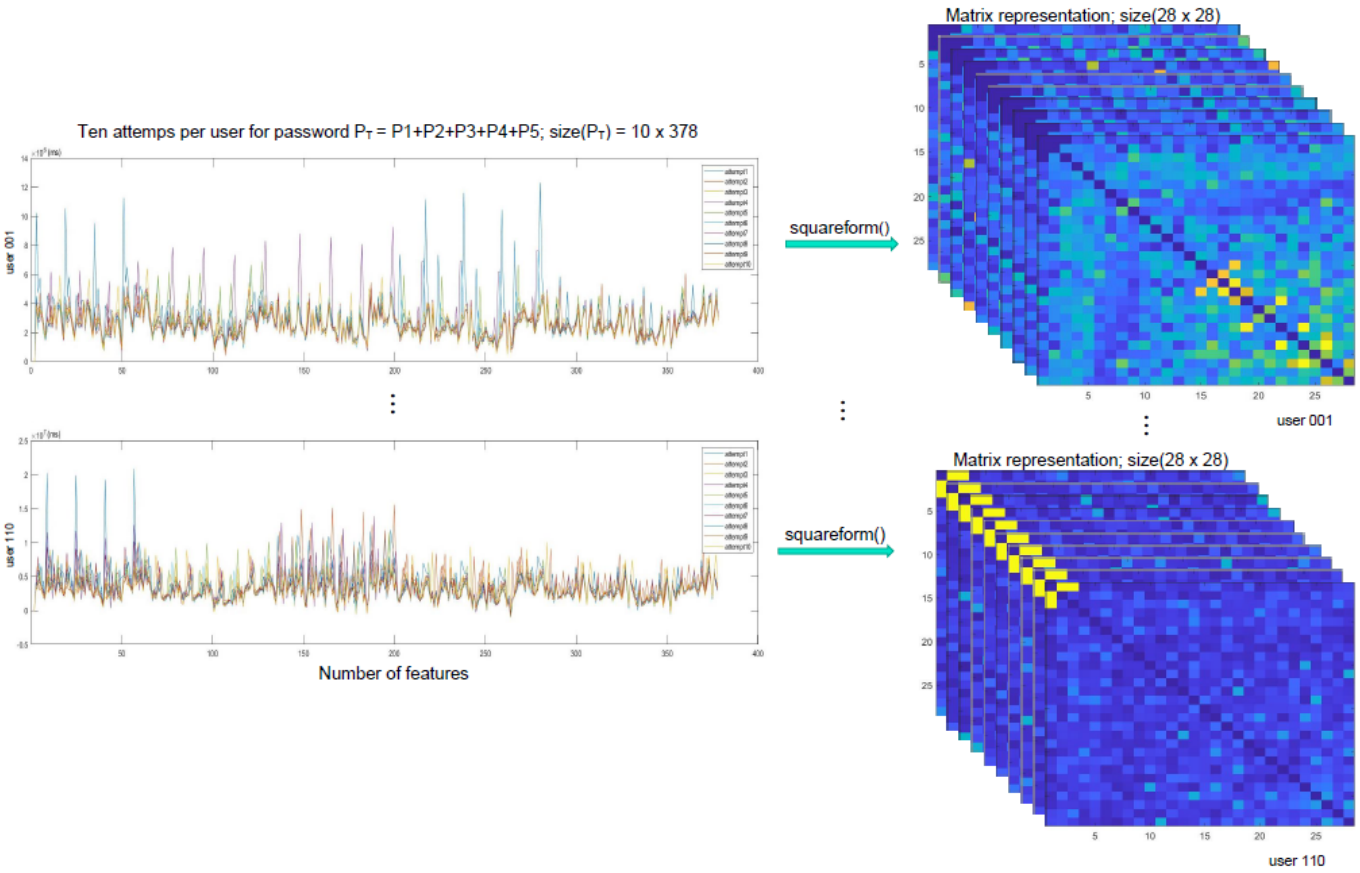

Figure 3: Graphic illustration process of time series transformation into matrix.

Table III: Description of passphrases used in the GREYC-NISLAB database. Note : $P_T = (P1+P2+P3+P4+P5)$

Password	Description	Size	Features
P1	leonardo dicaprio	17-char	64
P2	the rolling stones	18-char	68
P3	michael schumacher	18-char	68
P4	red hot chilli peppers	22-char	84
P5	united states of america	24-char	92
P_T	fusion of features	99-char	376

C. Scoring algorithms

Deep architectures as explained previously generate feature vectors that can be used as reference/test templates. We need a matching algorithm to compare and make the authentication decision. Many distance metrics can be used to compute a distance score [5] from a reference (x_s) and a sample (x_t) such as:

- Minkowski distance

$$d = \sum_{j=1}^{n} |x_{sj} - x'_{tj}| \tag{1}$$

- Euclidean distance

$$d^2 = (x_s - x_t)(x_s - x_t)' \tag{2}$$

- Cosine distance

$$d = 1 - \frac{x_s x'_t}{\sqrt{(x_s x'_s)(x_t x'_t)}} \tag{3}$$

Once we obtain a biometric score, we decide if the user is authenticated by a simple thresholding approach (accept when the score is upper a set threshold).

Table II: Architectures and optimizations hyper-parameters for the deep learning approaches

Models	#Layers	#Depth	Image Input Size	Activate	Normalize	Algorithm	Loss	#Epochs	#Batch	#Learning rate
ResNet-101	347	101	224-by-224	ReLU	Batch	SGDM	cross-entropy	500	10	0.001
ShuffleNet	172	50	224-by-224	ReLU	Batch	SGDM	cross-entropy	500	10	0.001
GoogleNet	144	22	224-by-224	ReLU	Batch	SGDM	cross-entropy	500	10	0.001
DarkNet-53	184	53	256-by-256	ReLU	Batch	SGDM	cross-entropy	500	10	0.001
DenseNet-201	708	201	224-by-224	ReLU	Batch	SGDM	cross-entropy	500	10	0.001
SqueezeNet	68	18	227-by-227	ReLU	Batch	SGDM	cross-entropy	500	10	0.001

IV. Experimental protocol

We draw in this part the experimental protocol we follow in this work. We detail the used biometric datasets and the performance metrics.

A. GREYC-NISLAB

The GREYC-NISLAB database [26] for keystroke dynamics is constituted of five passwords entered by 110 users. There were 10 samples per password per user for each way of typing. The best password is a sentence according to experts. We have in total 5500 data samples which correspond to $110 \times 10 \times 5$ keystroke dynamics samples proposed in our benchmark database.

For this modality, 5 passphrases were presented to users as shown in Table III, which are between 17 and 24 characters (including spaces) long, chosen from some of the well-known or popular names or artists (known both in France and Norway), denoted P1 to P5. The GREYC Keystroke software has been used to capture biometrics data. P_T denotes the fusion of the 5 passwords (fusion of features) [2]. Representative keystroke dynamics databases are very heavy to realize. One of the biggest advantages of using the GREYC-NISLAB database is that we have several passwords for the same users. To the best of our knowledge, such transformation (Signal-to-Image) approach on keystroke dynamics database does not exist in the literature up to now.

Among the transformed signal-to-image samples of each user, 7 out of 10 samples are used for training and testing data.

B. Performance metrics

In the authentication/verification stage, the raw data is acquired and processed to extract the biometric template. This biometric template is then compared with the existing reference templates in the database. A matching algorithm is then used to determine how closely the biometric matches with an existing template in the database. We compute the inter and intra class score according to the extract features. Using the distance metrics (*Minkowski*, *Euclidean* and *Cosine*), we evaluate the degree of similarity between the password entry between each user.

Two important error rates are used to determine the performance of a biometric authentication system according to ISO19795 [27]: False Match Rate (FMR) and False Non-Match Rate (FNMR).

- FMR is the proportion of a specified set of completed non-mated comparison trials that result in a comparison decision of *match*.
- FNMR is the proportion of completed mated comparison trials that result in a comparison decision of *non-match*.

The Equal Error Rate (EER) is when the FMR is equal to the FNMR as depicted in Figure 4. It can be seen as a compromise of usability and security. The goal of a matcher is to minimize this value. The lower the value of EER, the better the performance of the authentication system is. This error rate is the most commonly used in the literature to illustrate the performance of biometric systems. In this work, we evaluate the proposed architecture in terms of EER.

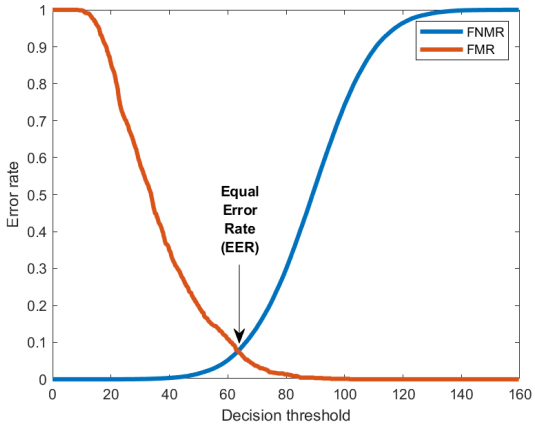

Figure 4: Relationship between FMR, FNMR and EER

V. Results and Discussion

In this section, we present the experimental results we obtained. We tried to structure them by answering some questions concerning the performance of the proposed method.

A. *Which performance can we obtain on each dataset?*

First, we consider a single password, i.e. we take each database separately to generate results. We used 1100 samples in total (110 users * 10 entries) taking 70% for the learning phase and 30% for the testing one. We illustrate the six architectures (namely ResNet-101, ShuffleNet, DarkNet, GoogleNet DarkNet-53, DenseNet-201 and SqueezeNet) and we draw the model and the metric that offer the best performances on each database separately. This is illustrated by Figure 5.

We observe that GoogleNet offers the best performance with an EER value equal to 18.43% (P1), 14.20% (P3) and 14.80% (P5). Sometimes, ResNet-101 performs well with a EER value to 14.23% (P2) and 15.70% (P4). We can also note that we do not have the same performance from one password to another. So using 7 samples for a user as reference template generation does not provide very good results (with an EER value between 14% to 18%). Obviously, if we had much more data, we could expect to obtain a better performance.

B. *Which performance can we obtain on a larger dataset?*

In this section, we merge all the sub-databases (**fusion of features**) to create a new dataset called P_T (concatenation of P1, P2, P3, P4 and P5). We took 70% of data for the learning phase and 30% for the testing one. Figure 5 draws the obtained results for a verification on P_T .

A comparative analysis of the six architectures on P_T database allows us to identify the best performance for a static authentication. Its given by ResNet-101 ($EER = 07.55\%$) and GoogleNet ($EER = 07.45\%$) architectures.

Performance is largely improved because we used more data that is general requested for deep learning techniques. This

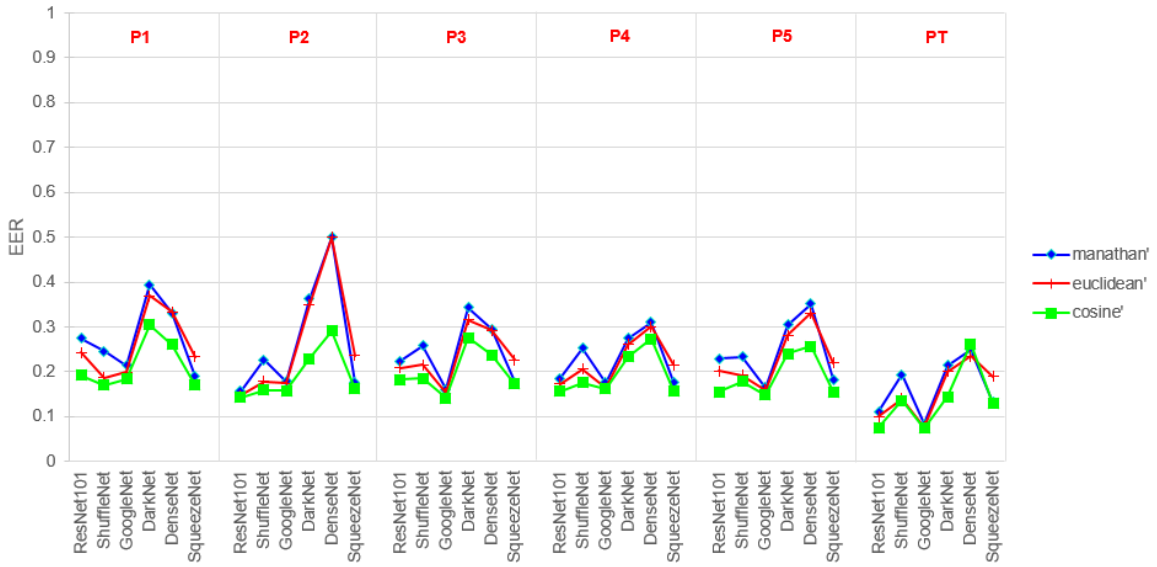

Figure 5: EER ($\times 100$) rate on deep architectures for P1, P2, P3, P4, P5 and PT sub-databases

.

illustrates the need of large keystroke dynamics (in terms of users and samples per user) to optimize the performance of deep learning methods on this biometric modality.
Figure 5 shows that the Cosine distance metric provides the best EER scores compared to the Minkowsky distance and the Euclidean distance, regardless of the architecture and sub-databases used, except for DenseNet-201 on the P_T case. We keep the Cosine distance in the rest of this work.

C. Which performance can we obtain if the user types more than one passphrase?

In this part, it is assumed that a person types more than one passphrase on the keyboard to authenticate himself/herself. We merge by summing the inter-class and intra-class scores (**fusion of score**) considering the number of typed passwords. We also took 70% of data for the learning phase and 30% for the testing one. Table IV shows the obtained results if we used the five typed passphrases (i.e. simulating a user typed the 5 passphrase to be authenticated). GoogleNet comes out as the best method with an EER score of 04.49% as presented in Table IV. GoogleNet is ahead of ResNet101 (06.70%) and ShuffleNet (07.34%).

Table IV: Performance evaluation on the multi-instance biometric system by fusion of features and scores level on P_T.

Models (EER_{cosine})	**Fusion of features**	**Fusion of scores**
ResNet-101	07.55%	06.70%
ShuffleNet	13.59%	07.34%
GoogleNet	**07.45%**	**04.89%**
DarkNet-53	14.96%	11.11%
DenseNet-201	26.18%	10.50%
SqueezeNet	12.87%	08.68%

To complete these results, we studied the obtained performance versus the number of passphrases typed by an user in a multi-instance context. Figure 6 highlights the EER value obtained for each case.

- In the most classical case, if we use 2 inputs (*i.e.* login + password), we obtain an EER value between $[9.17\% - 22.95\%]$ illustrated by block 2 in Figure 6.
- If we have 3 inputs (*i.e.* login + password + secret question), we have an EER value between $[6.89\% - 17.80\%]$ represented by block 3.
- If we use 4 inputs (*i.e.* login + 2 passwords + secret question), we have an EER value around $[5.95\% - 13.67\%]$ depicted by block 4.
- If we use 5 inputs, we get an EER value around $[4.89\% - 11.11\%]$ depicted by block 5. Even if this scenario is less realistic, it shows we can decrease easily the EER value for this kind of authentication.

We note that the EER value obtained when applying the fusion of score of sub-databases decreases for each architecture. It also appears from this work that the more information we have, the better the performance can be, that it is not surprising. Having a larger database, we could expect to get better results (*i.e.* with an EER value very close to 0%) increasing the number of samples per user.

D. Discussion

Keystroke authentication is totally based on the routines that the users have, since they probably entered the same password numerous times. In this case, their typing styles become so unique and hard to imitate, which is also the core of the keystroke recognition systems [12]. Neural networks have the

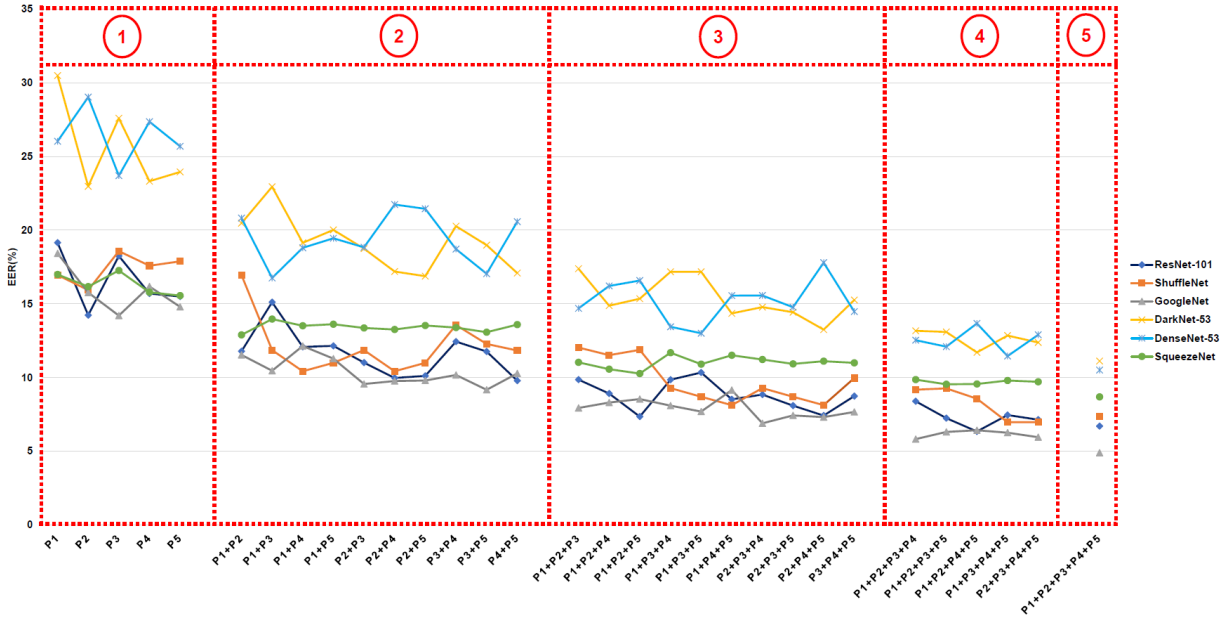

Figure 6: EER rate on deep architectures for the multi-instance biometric system. In block 1, we have P1, P2, P3, P4 and P5 sub-database. In block 2, we have the fusion of inter and intra class score from (P1+P2) to (P4+P5) sub-databases respectively. In block 3, (P1+P2+P3) to (P2+P3+P5). In block 4, (P1+P2+P3+P4) to (P2+P3+P4+P5) and in Block 5, (P1+P2+P3+P4+P5)

.

Table V: Comparison with other published works in keystroke dynamics. EER values are reported (note some works have used non representative datasets). For each reported works, different biometric samples are merged.

Databases	Author/S (ref)	Years	Classifiers	EER
GREYC-NISLAB	**This Paper**	**2021**	**GoogleNet**	**04.89%**
GREYC-NISLAB	Idrus *et al.* [28]	2015	SVM	[08.45% – 10.63%]
Clarkson II	Li *et al.* [29]	2021	CNN & CNN-GRU	[07.55% – 07.74%]
Synthetic	Ayotte *et al.* [30]	2021	SVM & MLP	[04.90% – 05.46%]
GREYC 2009 vs WEB GREYC	Mhenni *et al.* . [31]	2018	kNN	[06.61% – 07.08%]
GREYC Keystroke	Zhong *et al.* [32]	2015	SVM	[08.45% – 10.65%]

advantage of being able to handle many parameters. However, they can be slow not only during training but also in the application phase. The purpose of this work is to analyze several information entered by a user in order to authenticate him/her.

To the best of our knowledge, the database resulting from the keystroke dynamics on a laptop used in this work (GREYC-NISLAB [26] database) is one of the most representative database that currently exist on this behavioral biometric modality despite the limited number of entries per user.

A complete list of available keystroke dynamics datasets has been listed by Monaco [33]. As it can be seen, most of datasets have less than 200 individuals and few samples are available for each user. The collection of such datasets is very time consuming, this is the main reason why there is not more very large datasets like for the face modality [17], [21] which is a crucial problem for the research in this area.

If we focus on research works that has been performed on the GREYC-NISLAB database, we can compare our results. Idrus *et al.* [28] obtained an EER value of 10.63% using a SVM-based method. They further improved the keystroke dynamics authentication accuracy from an EER value of 8.45%. Considering the same database, the proposed approach with GoogleNet performs better with an EER value of 04.89% (Table V).

To complete this comparison, we consider other works on different biometric databases. Of course, it is not possible to have a fair comparison but we give these values for illustration. When different keystroke dynamics samples are fused, Ayotte et al. [30] (2021) obtained an EER value of 04.90% with MLP method. They used a different database than the GREYC-NISLAB one (and is private). Both of these works are based on the content knowledge. This is not the case with our work because we place ourselves in an attack situation, that is to say that we consider that the attacker (passphrase situation) knows the password. We try to authenticate a person only by the way he/she types.

Multi-instance system consists of capturing samples of two or more different instances of the same biometric characteristics. Table IV shows that for a verification performed on keystroke dynamics, the best verification scores are obtained on the fusion of score as opposed to the fusion of feature when using

six different deep neural networks architectures.

VI. Conclusion and perspectives

In this paper, we have proposed a new keystroke dynamics system based in deep learning for user authentication. Keystroke dynamics on a laptop have been studied as behavioral biometrics because it has a number of advantages, it is low cost, there is no additional tool or constraint for the user, the user does not need to use and learn other tools to use the keyboard dynamics. This study answer how well deep learning approaches could perform for passphrase user authentication by using keystroke dynamics data and shows that keystroke dynamics is indeed an available method to enhance the security of PIN code based authentication on laptop or mobile devices for example. We also show that the new framework outperforms the state-of-the-art methods in terms of EER score.

For future research, we plan to add psychological features such as the user's emotions when entering passwords for the training and testing process to improve accuracy since emotional states could be identified from his or her input behavioral style. We intend also to improve (and expand) the keystroke dynamics datasets that are needed if we are to make further significant progress on this authentication problem.

Acknowledgment

Authors would like to thank FIME SAS, the "Normandy Region" and the ANRT for their financial support of this work.

References

[1] A. Visvizi, J. Jussila, M. D. Lytras, and M. Ijäs, "Tweeting and mining oecd-related microcontent in the post-truth era: a cloud-based app," *Computers in Human Behavior*, vol. 107, p. 105958, 2020.

[2] Y. B. W. Piugie, J. Manno, C. Rosenberger, and C. Charrier, "How artificial intelligence can be used for behavioral identification?" in *2021 International Conference on Cyberworlds (CW)*, 2021.

[3] Y. B. W. Piugie, D. Tchiotsop, A. N. K. Telem, and E. B. M. Ngouonkadi, "Denoising of electroencephalographic signals by canonical correlation analysis and by second-order blind source separation," in *2019 IEEE AFRICON*. IEEE, 2019, pp. 1–8.

[4] E. Cherrier, "Authentification biométrique: comment (ré) concilier sécurité, utilisabilité et respect de la vie privée?" Ph.D. dissertation, Normandie Université, 2021.

[5] D. Migdal, "Contributions to keystroke dynamics for privacy and security on the internet," Ph.D. dissertation, Normandie Université, 2019.

[6] K. O. Bailey, J. S. Okolica, and G. L. Peterson, "User identification and authentication using multi-modal behavioral biometrics," *Computers & Security*, vol. 43, pp. 77–89, 2014.

[7] B. Ayotte, M. K. Banavar, D. Hou, and S. Schuckers, "Study of intra-and inter-user variance in password keystroke dynamics." in *ICISSP*, 2021, pp. 467–474.

[8] R. Toosi and M. A. Akhaee, "Time–frequency analysis of keystroke dynamics for user authentication," *Future Generation Computer Systems*, vol. 115, pp. 438–447, 2021.

[9] A. Andrean, M. Jayabalan, and V. Thiruchelvam, "Keystroke dynamics based user authentication using deep multilayer perceptron," *International Journal of Machine Learning and Computing*, vol. 10, no. 1, pp. 134–139, 2020.

[10] X. Lu, S. Zhang, P. Hui, and P. Lio, "Continuous authentication by free-text keystroke based on cnn and rnn," *Computers & Security*, vol. 96, p. 101861, 2020.

[11] H. Çeker and S. Upadhyaya, "Sensitivity analysis in keystroke dynamics using convolutional neural networks," in *2017 IEEE Workshop on Information Forensics and Security (WIFS)*. IEEE, 2017, pp. 1–6.

[12] O. Alpar, "Frequency spectrograms for biometric keystroke authentication using neural network based classifier," *Knowledge-Based Systems*, vol. 116, pp. 163–171, 2017.

[13] J. Roth, X. Liu, A. Ross, and D. Metaxas, "Investigating the discriminative power of keystroke sound," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 333–345, 2014.

[14] N. Harun, W. L. Woo, and S. Dlay, "Performance of keystroke biometrics authentication system using artificial neural network (ann) and distance classifier method," in *International Conference on Computer and Communication Engineering (ICCCE'10)*. IEEE, 2010, pp. 1–6.

[15] K. Revett, F. Gorunescu, M. Gorunescu, M. Ene, S. Magalhaes, and H. Santos, "A machine learning approach to keystroke dynamics based user authentication," *International Journal of Electronic Security and Digital Forensics*, vol. 1, no. 1, pp. 55–70, 2007.

[16] Z. Chen, H. Cai, L. Jiang, W. Zou, W. Zhu, and X. Fei, "Keystroke dynamics based user authentication and its application in online examination," in *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. IEEE, 2021, pp. 649–654.

[17] D. Migdal, "Contributions to keystroke dynamics for privacy and security on the Internet," Theses, Normandie Université, Nov. 2019. [Online]. Available: https://tel.archives-ouvertes.fr/tel-02518436

[18] R. Spillane, "Keyboard apparatus for personal identification," *IBM Technical Disclosure Bulletin*, vol. 17, p. 3346, 1975.

[19] R. S. Gaines, W. Lisowski, S. J. Press, and N. Shapiro, "Authentication by keystroke timing: Some preliminary results," Rand Corp Santa Monica CA, Tech. Rep., 1980.

[20] D. Migdal and C. Rosenberger, "Statistical modeling of keystroke dynamics samples for the generation of synthetic datasets," *Future Generation Computer Systems*, vol. 100, pp. 907–920, 2019.

[21] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, and P. Bours, "Soft biometrics for keystroke dynamics: Profiling individuals while typing passwords," *Computers & Security*, vol. 45, pp. 147–155, 2014.

[22] C. Vasconcelos, H. Larochelle, V. Dumoulin, R. Romijnders, N. L. Roux, and R. Goroshin, "Impact of aliasing on generalization in deep convolutional networks," *arXiv preprint arXiv:2108.03489*, 2021.

[23] S. Maheshwary, S. Ganguly, and V. Pudi, "Deep secure: A fast and simple neural network based approach for user authentication and identification via keystroke dynamics," in *IWAISe: First International Workshop on Artificial Intelligence in Security*, vol. 59, 2017.

[24] L. Aversano, M. L. Bernardi, M. Cimitile, and R. Pecori, "Continuous authentication using deep neural networks ensemble on keystroke dynamics," *PeerJ Computer Science*, 2021.

[25] O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. Bernstein *et al.*, "Imagenet large scale visual recognition challenge," *International journal of computer vision*, vol. 115, no. 3, pp. 211–252, 2015.

[26] S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, and P. Bours, "Soft biometrics database: A benchmark for keystroke dynamics biometric systems," in *2013 International Conference of the BIOSIG Special Interest Group (BIOSIG)*, 2013, pp. 1–8.

[27] ISO, "Information technology — Biometric performance testing and reporting — part 1: Principles and framework," International Organization for Standardization, Geneva, CH, Standard ISO/IEC 19795-1:2021, 2021.

[28] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, S. Mondal, and P. Bours, "Keystroke dynamics performance enhancement with soft biometrics," in *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015)*. IEEE, 2015, pp. 1–7.

[29] J. Li, H.-C. Chang, and M. Stamp, "Free-text keystroke dynamics for user authentication," *arXiv preprint arXiv:2107.07009*, 2021.

[30] B. Ayotte, M. K. Banavar, D. Hou, and S. Schuckers, "Group leakage overestimates performance: A case study in keystroke dynamics," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2021, pp. 1410–1417.

[31] A. Mhenni, E. Cherrier, C. Rosenberger, and N. E. B. 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.

[32] Y. Zhong and Y. Deng, "A survey on keystroke dynamics biometrics: approaches, advances, and evaluations," in *Recent Advances in User Authentication Using Keystroke Dynamics Biometrics*. Science Gate Publishing, 2015, no. 1, pp. 1–22.

[33] V. Monaco, "Public keystroke dynamics datasets," 2018.