

# BehavePassDB: Benchmarking Mobile Behavioral Biometrics

Giuseppe Stragapede, Ruben Vera-Rodriguez, Ruben Tolosana, Aythami Morales

*Biometrics and Data Pattern Analytics,*

Universidad Autonoma de Madrid

Madrid, Spain

Email: giuseppe.stragapede@uam.es, ruben.vera@uam.es, ruben.tolosana@uam.es, aythami.morales@uam.es

**Abstract**—Mobile behavioral biometrics have become a popular topic of research, reaching promising results in terms of authentication, exploiting a multimodal combination of touchscreen and background sensor data. However, there is no way of knowing whether state-of-the-art classifiers in the literature can distinguish between the notion of user and device. In this article, we present a new database, BehavePassDB, structured into separate acquisition sessions and tasks to mimic the most common aspects of mobile Human-Computer Interaction (HCI). BehavePassDB is acquired through a dedicated mobile app installed on the subjects’ devices, also including the case of different users on the same device for evaluation. We propose a standard experimental protocol and benchmark for the research community to perform a fair comparison of novel approaches with the state of the art<sup>1</sup>. We propose and evaluate a system based on Long-Short Term Memory (LSTM) architecture with triplet loss and modality fusion at score level.

**Index Terms**—mobile authentication, continuous authentication, behavioral biometrics, BehavePassDB, device bias

## I. INTRODUCTION

Mobile biometric authentication currently relies mostly on physiological biometrics such as fingerprint or face [1]. These biometric systems, however, are prone to physical presentation attacks (spoofing) [2] and digital manipulations [3] and, just as well as knowledge-based systems (PIN codes, passwords, and lock patterns [4]), they are designed for *entry-point* authentication and not suited for offering prolonged protection. In such case, mobile users would have to keep interrupting their activity to carry out the authentication process, for instance by placing their fingertip on the dedicated scanner. Frequent face verification also seems infeasible due to hardware constraints, such as the computational overload, memory overhead and battery consumption of the acquisition and processing of images. Considering such limitations of the currently deployed authentication systems, if an intruder gains access to the device, they can stay authenticated as long as the device remains active, being granted a considerable amount of time to obtain private information [5].

In this scenario, in contrast to physiological biometrics,

behavioral biometrics<sup>2</sup> allow for Continuous Authentication (CA), a paradigm based on constantly verifying the biometric features of the user in a *passive* way, in other words, without having them to carry out any specific authentication task [6], [7]. In CA systems, biometric samples are continuously acquired and processed, and the user will be redirected to an *entry-point* authentication mechanism in case that the matching with pre-acquired enrolment samples returns a negative response. To this end, behavioral biometrics traits are suitable as mobile devices are equipped with several sensors, such as touchscreen, motion sensors, etc., able to continuously acquire low-dimensional temporal signals concerning the user activity, that can reveal a significant amount of information about the user [8]. In addition, other aspects such as the application usage, GPS position, and network connections are included in the behavioral category as they capture users’ personal habits and routines. As a result, behavioral biometrics offer strong security and high usability in this mobile scenario.

### A. Description of the Problem

Although systems based on behavioral biometrics do not usually achieve the same authentication performance as their *physiological* counterparts, Behavioral Biometrics for Continuous Authentication (BBCA) [6] is an appealing area for the biometrics research community, either as:

- (i) A form of complementary technology or second factor in a 2-factor authentication (2FA) [4]; for instance, in a remote security-wise critical service, BBBCA could be used on top of existing security protocols. **In this case, every user would be using their own mobile device.**
- (ii) The primary security technology in the real-world scenario of a theft, in which the **impostor and the genuine user data originate from the same device** [9].

The difference in between the two scenarios consists in the authentication technology being able to differentiate between the notion of “device” and “user”. This is mainly related to two data collection approaches, as subjects are typically asked to use their own mobile device for data collection without

<sup>2</sup>In the context of biometrics, a well-known dichotomy is given by the nature of the traits: all biological characteristics that allow to identify an individual are defined as *physiological* (face, fingerprint, iris, etc.), whereas all the means that allow or help in discriminating among individuals based on the way activities are performed, such as gait, typing, scrolling, signature, etc., are labelled as *behavioral*.

<sup>1</sup>[https://github.com/BiDALab/MobileB2C\\_BehavePassDB/](https://github.com/BiDALab/MobileB2C_BehavePassDB/)

## BehavePassDB

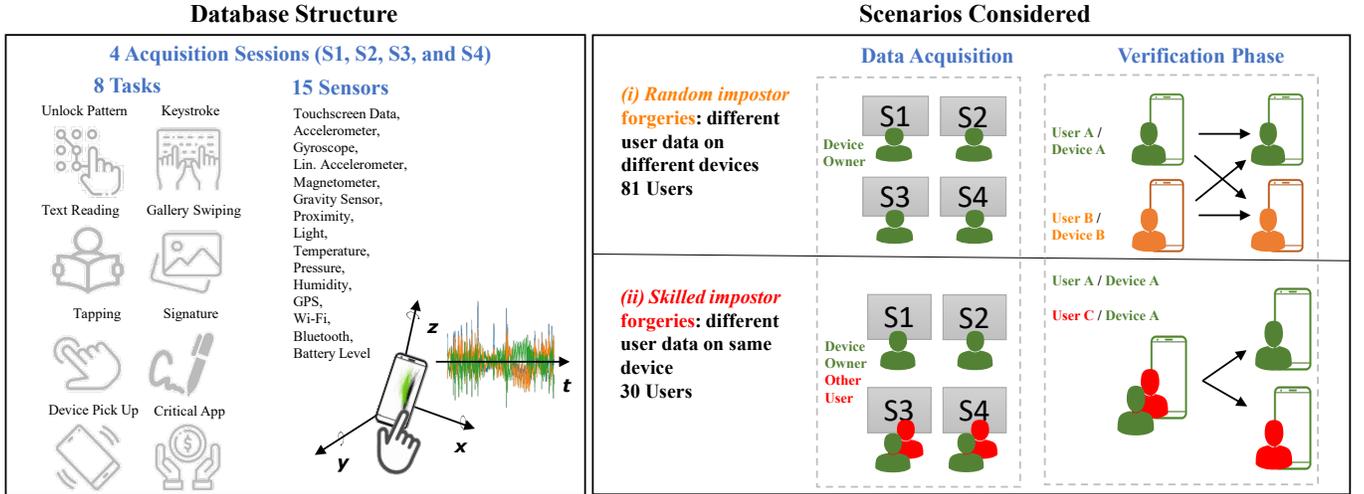


Fig. 1. In BehavePassDB, each of the 4 acquisition sessions contains 8 tasks. During each task, data are acquired from 15 different sources (modalities), including touchscreen information and background sensors. Two impostor scenarios are allowed for user verification: (i) *random impostor forgeries*, in which every user data are acquired from their own mobile device, and the user data cross comparisons entail different devices; (ii) *skilled impostor forgeries*, in which the last two acquisition sessions are performed also by a different user on the same device, allowing user data cross comparisons from the same device.

hard requirements in terms of the devices used, as long as it is the same one for the entire data acquisition process [10]–[13], or they are asked to use only one or few dedicated acquisition devices [14]–[17]. Consequently, in the first case, the user extracted features of user might in reality be related to their mobile device, and it is not possible to assert with certainty that they are, indeed, biometric. A potential learning bias could be in fact introduced due to sensor differences and calibration imperfections across devices [13], [18]. The source of such possible bias is avoided or reduced in the second case. Nevertheless, the performance of the developed authentication system could be highly affected if evaluated on a different device. The proposed BehavePassDB considers a hybrid approach, in the attempt to quantify a possible difference in the performance of a system developed in the first setting, which allows a simpler, large-scale data collection, and evaluated in both scenarios. We define the above-described case (i) impostor data as *random forgeries*, as the genuine and impostor data are acquired by two different devices, whereas case (ii) is addressed as *skilled impostor forgeries*, since the genuine and impostor data are related by the fact that the acquisition device is exactly the same and the impostor users were instructed to imitate the device owner, leading to a more challenging scenario (Fig. 1).

### B. Contributions

In the present article, we aim to address the above mentioned aspects, contributing to the development of large-scale real-world of BBCA systems, as follows:

- We collect a multimodal behavioral biometrics database, BehavePassDB, involving 81 users, structured into separate acquisition sessions, in which the user is asked to carry out a series of tasks designed to mimic the most salient traits of mobile Human-Computer Interaction (HCI). The collected data also includes two dedicated

sessions to be completed by another person (impostor) on the same exact device. In this way, we attempt to shed some light on the ability of the learned models to decorrelate user from device recognition in the learned data representation for background sensors.

- We consider several mobile behavioral biometric sources (touchscreen data, and background sensors such as accelerometer, gyroscope, magnetometer, lin. accelerometer, etc.). For each individual modality, we implement a popular Deep Learning (DL) architecture with the triplet loss function, and compare the biometric performance of individual modalities and their fusion at score level.
- The DL models are developed considering user data collected from different devices, and evaluated on user data collected in a similar scenario, and from the same exact device by an impostor user. Thus, we evaluate both *random* and *skilled forgeries* scenarios.
- We propose a standard experimental protocol publicly available to the research community in order to perform a fair comparison of novel approaches with the state of the art. This way we provide an easily reproducible framework. BehavePassDB<sup>3</sup> and the experimental protocol followed in this paper are used to organize the MobileB2C<sup>4</sup> competition at the International Joint Conference of Biometrics<sup>5</sup> (IJCB) 2022. This competition will be made an ongoing competition, so the current work will serve as a benchmark that researchers working in this field will be able to compare to.

<sup>3</sup>[https://github.com/BiDALab/MobileB2C\\_BehavePassDB/](https://github.com/BiDALab/MobileB2C_BehavePassDB/)

<sup>4</sup><https://sites.google.com/view/mobileb2c/>

<sup>5</sup><http://www.ijcb2022.org/>

## II. RELATED WORK

### A. BBCA Systems

Given their suitability for continuous authentication on mobile devices, behavioral biometric traits have received the attention of the biometric research community since the launch of the first smartphone models. Over the years, different biometric systems have been developed and applied for BBCA, especially with the rise of DL. In the remainder of this section, some of the most recent and promising related studies up-to-date will be presented.

A mobile wide-ranging multimodal system based on behavioral biometrics was introduced by Deb *et al.* [11]. Their approach was based on a contrastive loss-based Siamese Long Short-Term Memory (LSTM) Recurrent Neural Network (RNN) architecture, in order to verify the users' identity in a passive way, i.e., without any explicit authentication task. 8 different modalities were taken into account (keystroke, GPS location, accelerometer, gyroscope, magnetometer, linear accelerometer, gravity, and rotation sensors) and the individual scores were fused claiming results of 96.47% of True Acceptance Rate (TAR) at a False Acceptance Rate (FAR) of 0.1% considering 3-second time intervals for authentication. However, these results seem to be over-optimistic since they used a sampling frequency rate of 1Hz, i.e., 1 sample per second. They evaluated their system on a small self-collected dataset comprised of measurements from 30 smartphones for 37 subjects.

Following a similar method, Abuhamad *et al.* proposed a mobile DL-based BBCA system only based on different sets of background sensors [19]. In this case, the fusion of modalities took place at data level, exploiting different RNN LSTM architectures with triplet loss. In 1-second time intervals, they obtained 0.41% Equal Error Rate (EER) using three sensors (accelerometer, gyroscope, and magnetometer). The 84 participants in this study had to install a mobile application which transparently collected sensor information over time. Nonetheless, in both cases [11], [19], the time windows are extracted as long as the dedicated data acquisition app is running in the background, with loose restrictions in terms of sensor activity. A large amount of information is acquired per user, including many instances with little information content. Consequently, the average biometric distinctiveness of each single time window is allegedly less than in dense gesture-centered dedicated sessions, designed to mimic the most salient traits of mobile HCI. In light of this, it is difficult to assess how much of the authentication performance it to be attributed to the system identifying the device rather than the user.

Touchscreen data information was considered by Acien *et al.* First, in [20], the HuMidb public database [10] was used to examine swiping gestures. A final EER of 19% was achieved with a Siamese RNN by extracting 29 features. Then, the same authors adopted a LSTM RNN network for authentication based on keystroke dynamics in a free-text scenarios from the public Aalto database [21], employing a variety of loss functions (softmax, contrastive, and triplet loss), different amount of enrolment data, length of the typed sequences, and

device (physical vs touchscreen keyboard), achieving an EER of 9.2% for touchscreen information while typing [22].

In [7], [23], several experiments are performed over HuMidb, a separate RNN with triplet loss is implemented for each single modality with the weighted fusion of the different modalities is carried out at score level, leading to EER ranging from 4% to 9% depending on the modality combination in a 3-second interval.

### B. BBCA Databases

All machine learning-based systems thrive thanks to the availability of data, with no exception for the case of BBCA systems. The following aspects are important for a high-quality acquisition:

- Involving a large number of subjects, maximizing the amount of data per user. This two aspects are often in conflict.
- Collecting data from several biometric sources (*modalities*) in order to allow the development of multimodal systems, as such approach has proven to be beneficial in terms of robustness, immunity to noise, universality, and security, at a cost of increased complexity [6], [54], [55].
- Collecting data in an unconstrained scenario: this aspect is particularly sensitive with regard to behavioral biometrics for continuous authentication, given the ubiquity of mobile devices in the users' life and the diverse nature of such data. For instance, with respect to background sensors, an additional source of variability can be given by the user position or activity (sitting, standing, walking). Restricting the data acquisition scenario might affect the generality of the systems developed. Nevertheless, it is important to assess and avoid any possible learning bias due to users' position or activity.
- Number of acquisition devices: as well as the users' activity, also the usage of different acquisition devices can influence the ability of the systems to discriminate among human identities. Assessing this aspect rigorously is among the goals of the current study (see Sec. II-C).
- Public availability of the databases: assessing the performance of the different systems proposed in the literature is often a difficult task, given the different approaches, scopes, and the usage of self-collected non-public databases. Databases such as the Aalto database [21], the UMDAA-02 [49], the HuMidb [10], etc., represent an important tool for the scientific community to compare approaches and advance the state of the art.

In Table I, we report some of the most important mobile behavioral biometric databases up to date.

### C. Device Bias

Das *et al.* showed that under lab conditions a particular device could be identified by a response of its motion sensors to a given signal, developing a highly accurate fingerprinting mechanism that combines multiple motion sensors and makes use of (inaudible) audio stimulation to improve detection [18]. This happens due to imperfection in calibration of a sensor

TABLE I  
SUMMARY OF MOBILE BEHAVIORAL BIOMETRIC DATABASES.

ACRONYMS: A = ACCELEROMETER, AU = AUDIO, B = BLUETOOTH, BA = BATTERY LEVEL, C = CAMERA, °C = TEMPERATURE, CL = CALL LOGS, CT = CALL TOWER IDS, GR = GRAVITY SENSOR, GY = GYROSCOPE, H = HANDWRITING, HU = HUMIDITY, K = KEYSTROKE, L = LIGHT, LA = LINEAR ACCELEROMETER, MI = MICROPHONE, N = NETWORK LOGS, P = PRESSURE, PR = PROXIMITY, SY = SYSTEM STATS, T = TOUCHSCREEN, W = WI-FI.

Dataset	Year	Available <sup>1</sup>	Unconstrained Env. <sup>2</sup>	# of Users	# of Devices	Data Modality	Impostor Case
MIT Reality Mining [24]	2006	✓	✓	100	100	CL, B, CT, Ap	Different Device
Saevanee <i>et al.</i> [25]	2008	✗	✗	10	1	T	Same Device
Zahid <i>et al.</i> [26]	2009	✗	✗	25	13	T	Not Considered
Rice LiveLab Dataset [27]	2011	✓	✓	34	18	Ap, W	Not Considered
Frank <i>et al.</i> [28]	2012	✗	✓	41	4	T	Not Considered
Serwadda <i>et al.</i> [29]	2013	✓	✗	190	1	T	Same Device
Zhang <i>et al.</i> [30]	2015	✗	✗	50	1	T, C	Same Device
Feng <i>et al.</i> [31]	2014	✗	✓	123	3	T	Not Considered
Xu <i>et al.</i> [32]	2014	✗	✗	28	1	T, K, H	Same Device
Saevanee <i>et al.</i> [33]	2015	✗	✓	30	~30	K, Ap, LP	Different Device
Hoang <i>et al.</i> [34]	2015	✗	✓	34	1	A	Same Device
Neal <i>et al.</i> [35]	2015	✗	✓	200	~200	Ap, W, B	Different Device
Wu <i>et al.</i> [36]	2015	✗	✓	100	~100	K, P, A, G	Different Device
Nader <i>et al.</i> [37]	2015	✗	✗	20	1	T	Same Device
Murmuria <i>et al.</i> [38]	2015	✗	✓	73	1	A, Gy, T, Ap, Ba	Same Device
Sitova <i>et al.</i> (HMOG) [39]	2015	✗	✗	100	10	T, A	Not Considered
Zaliva <i>et al.</i> [40]	2015	✗	✗	14	1	T	Same Device
Lu et Lio [41]	2015	✗	✓	60	3	T	Not Considered
Coakley <i>et al.</i> [42]	2016	✓	✗	51	5	K, A, G	Not Considered
Putri <i>et al.</i> [43]	2016	✓	✗	29	1	T	Same Device
Kumar <i>et al.</i> [44]	2016	✗	✗	28	-	T, K, A, G	Not Considered
Shen <i>et al.</i> [45]	2016	✗	✗	71	3	T	Not Considered
Google Abacus Dataset [13]	2016	✗	✓	1500	~1500	C, T, A, Gy, M, W	Different Device
Antal <i>et al.</i> [46]	2016	✗	✗	71	8	T, A	Not Considered
Nixon <i>et al.</i> [47]	2016	✗	✓	20	~20	T, A, Gy	Different Device
Buriro <i>et al.</i> [48]	2016	✗	✗	30	1	T, A, M, Gy	Same Device
Mahbub <i>et al.</i> [49] (UMDAA-02)	2016	✓	✓	48	-	T, C, A, GPS, B, W, L, P, °C, Pr	Not Considered
Lee and Lee [50]	2017	✗	✓	35	2	A, Gy	Not Considered
Zhu <i>et al.</i> [51]	2017	✗	✗	20	-	A, Gy	Not Considered
Al Kork <i>et al.</i> [52]	2017	✗	✓	50	2	A, Gy	Not Considered
Li and Bours [12]	2018	✗	✓	312	~312	W, A	Different Device
Amimi <i>et al.</i> [53] (TargetAuth Dataset)	2018	✗	✗	47	-	A, Gy	Not Considered
Cilia <i>et al.</i> [17]	2018	✗	✗	24	2	K	Not Considered
Aalto University Dataset [21]	2019	✓	✓	~260k	-	K	Not Considered
Zhu <i>et al.</i> [16]	2019	✗	Mixed	1513	4	A, Gy, Gr	Not Considered
Garbuz <i>et al.</i> [15]	2019	✗	✗	36	1	T, A, Gy	Same Device
Vajdi <i>et al.</i> [14]	2019	✓	✗	93	2	A	Not Considered
Deb <i>et al.</i> [11]	2019	✗	✓	37	30	K, GPS, A, Gy, M, LA, Gr, Gy	Not Considered
Acien <i>et al.</i> [10] (HuMIdb)	2020	✓	✓	600	600	A, Gr, Gy, L, LA, M, O, Pr, L, GPS, W, B, Mi	Different Device
<b>Current Work (BehavePassDB)</b>	<b>2022</b>	<b>✓</b>	<b>✓</b>	<b>81</b>	<b>81</b>	<b>A, Gr, Gy, L, LA, M, O, P Pr, L, GPS, W, B, °C, Ba, Hu</b>	<b>Different and Same Device (Skilled)</b>

<sup>1</sup> Publicly Available.

<sup>2</sup> Unconstrained Environment, i.e., the subjects participating in the study did not receive instructions on how to perform the data collection process.

resulting in constant offsets and scaling coefficients (gains) of the output, that can be estimated by calculating integral statistics from the data. The authors analyzed techniques to mitigate such device fingerprinting either by calibrating the sensors to eliminate the signal anomalies, or by adding noise that obfuscates the anomalies. By acquiring measurements from a 30 different smartphones (5 models), they achieved a reduction of the accuracy by around 15%-20% in terms of average F-score by including additive and multiplicative noise to the raw data stream and spectral noise on the acquisition frequency. In light of this, it would be interesting to investigate how much of the authentication effectiveness should be attributed to the models extracting and recognizing features belonging to the device rather than the user. Following [18], Neverova *et al.* adopted such approach for large-scale study exploring temporal Deep Neural Networks (DNNs) for mobile biometric authentication based on accelerometer and gyroscope data [13]. The authors introduced low-level additive (offset) and multiplicative (gain) noise per training example to partially

obfuscate the inter-device variations and ensure decorrelation of user identity from device signature in the learned data representation. They achieved a 93.3% recognition accuracy by applying noise vectors obtained by drawing coefficients from a uniform distribution  $\mu \sim \mathcal{U}_{12}[0.98, 1.02]$ . Around 1500 subjects were involved, each one utilizing their own device (in all cases an LG Nexus 5).

### III. DESCRIPTION OF BEHAVEPASSDB

BehavePassDB includes data acquired during natural human-mobile interaction. The acquisition of the data was completed across four sessions, each of them separated by at least a 24-hour gap, in order to account for intra-subject variability. The participants were asked to install an Android application on their own smartphone and to complete eight tasks in an unsupervised scenario. The tasks are free-text keystroke, reading a text, swiping gallery images, tapping on the screen, signature, and picking up the smartphone. Simultaneously, data are acquired from 15 background sensors, i.e.,

## BehavePassDB Tasks

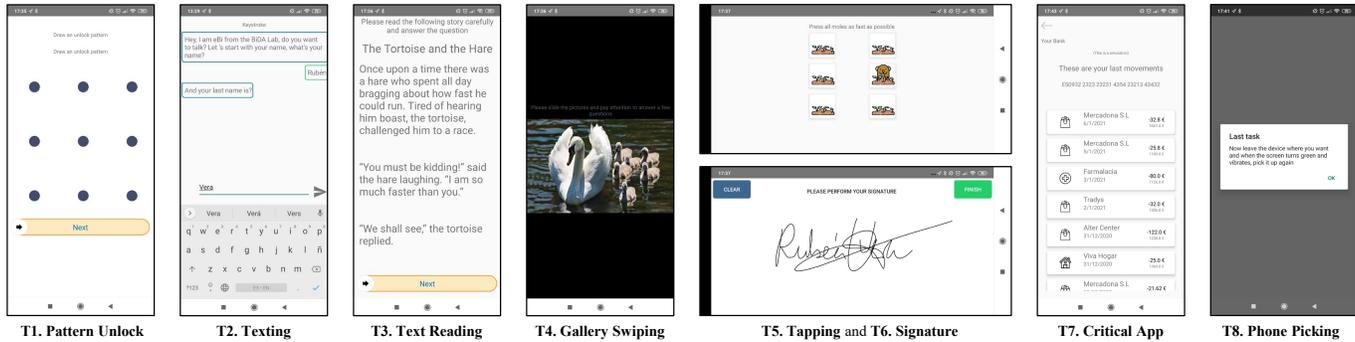


Fig. 2. Graphical representation of each of the 8 different tasks included in BehavePassDB data acquisition application.

accelerometer, linear accelerometer, gyroscope, magnetometer, ambient temperature, proximity, gravity, light, humidity, pressure, GPS, Wi-Fi, Bluetooth, and battery, collected as long as the device was able to provide such sensor information.

One of the most important novel aspect and novel contribution of BehavePassDB is its division into two subsets: a training set, containing 51 users, a validation set, containing 10 users, and an evaluation set, containing 20 users. In the first one, the acquisition scenario consists in each of the users using their own device, while the validation and evaluation sets also include two sessions of a different user on the owner's device.

Each session consists in 8 tasks, common to all sessions. Sessions 1 and 2 serve as the enrolment sessions of the user data. In sessions 3 and 4 of the evaluation dataset there was also an additional task, which is a simulation of a critical app (bank account app) with a mix of the previous different tasks. The tasks are as follows (Fig. 2):

- T1) Pattern Unlock:** the user performs a custom pattern unlock and a drag and drop gesture;
- T2) Texting:** the user is asked a series of different questions to be answered by typing. The questions are: name, last name, age, gender, two short free text questions, copying a number and a final free text question to be answered with at least 70 characters. Two different keyboards are deployed: in session 1 and 4, the keyboard presented to the user is their custom keyboard, whereas in session 2 and 3, we opt for a fixed keyboard. This choice is due to the fact that with the custom keyboard, it is typically possible to acquire only the timestamp and the value of the key pressed, from which a limited number of features can be extracted. The fixed keyboard, on the other hand, allows for the acquisition of the release time and the  $x$  and  $y$  coordinates of the touchscreen. Consequently, more features can be obtained. On the flip side, users might feel more natural when using their own preferred keyboard.
- T3) Text Reading:** the user is asked to read a text (swiping vertically) and then answer a question related to the text, followed by a drag and drop gesture.
- T4) Gallery Swiping:** the user is asked to swipe (horizontally) 4 pictures and then answer a question related to each of them, followed by a drag and drop gesture.

**T5) Tapping:** the user is asked to tap on in predetermined locations of the screen as fast as possible, followed by a drag and drop gesture.

**T6) Signature:** the user is asked to perform two handwritten signatures, one after the other.

**T7) Critical App:** this task is a simulation of a bank account app with different possible tasks inside, which are a mixture of the previous tasks.

**T8) Phone Picking:** the user is asked to leave the smartphone on a surface, wait for the screen to turn green, and then pick it up.

Regarding the age distribution, 8.86% of the users were younger than 20 years old, 64.56% are between 20 and 30 years old, 18.99% between 30 and 50 years old, and the remaining 7.59% are older than 50 years old. Regarding the gender, 46.84% of the participants were males, 53.16% females. The subjects were recruited from 8 countries (93.67% European, 5.06% American, 1.27% Asian).

## IV. SYSTEM DESCRIPTION

### A. Pre-processing and Feature Extraction

**1) Background Sensor Data:** The sensory data included in the current benchmark are acquired through the accelerometer, gravity sensor, gyroscope, linear accelerometer, and magnetometer. The acquisition frequency is set to 200Hz, however, different devices can be equipped with different sensors whose specifications do not allow for such frequency value. The time-series data are normalized through mean subtraction and division by the standard deviation, in the attempt to minimize the effect of noise and to cancel offset errors per axis per acquisition session. Following related studies [11], the Fast Fourier Transform (FFT) is computed from the raw  $x$ ,  $y$ ,  $z$  values, and the first- and second-order derivatives are included as additional features. Preliminary experiments in fact showed the impact of the derivatives to be beneficial on the system performance and negligible in terms of computational burden. Finally, for each timestamp and sensor, the final output of the pre-processing operations consist in a 12-dimensional vector, as follows:

$$[x, y, z, x', y', z', x'', y'', z'', f_{ft}(x), f_{ft}(y), f_{ft}(z)]$$

2) *Touch Data*: This benchmark is carried out considering the tasks of keystroke, text reading, gallery swiping, and tapping. The keystroke dynamics are assessed starting from data acquired during fixed questions with free answers, for instance related to the description of the last trip undertaken by the user, with a minimum answer length of 70 characters. The text acquired is in English or Spanish, depending on the preference of each subject. The entire sequence is acquired and analyzed, including the backspace key.

As explained in T2) (Sec. III), the keystroke data are acquired with two different type of keyboards depending on the acquisition session. In the current work, we utilize the inter-press time and the normalized value of the ASCII code for all sessions.

With regard to the tasks of text reading, gallery swiping, and tapping, the spatial  $x$  and  $y$  coordinates of the screen are used. Such data undergo a pre-processing process similar to the case of background sensor signals, including first- and second-order derivatives and the FFT, as reported below:

$$[x, y, x', y', x'', y'', \text{fft}(x), \text{fft}(y)]$$

The  $x$  and  $y$  data are normalized as well to the height and width values of the screen to reject potential sources of bias across devices.

### B. System Architecture

The proposed authentication system is based on an LSTM RNN, a DL network designed to exploit long-term dependencies in time-series data [56], [57]. The architecture implemented relies on two 64-unit layers with *tan-h* activation functions. Additional steps include batch normalization, dropout (with a rate of 0.5) between layers, and recurrent dropout (with a rate of 0.5) in each of the layers to limit the effect of overfitting. Preliminary tests led to the hyper-parameter configuration.

$M$ -sample time windows are created by including consecutive data samples. The time windows are zero-padded if the obtained sequence is too short. In our system, a time window corresponds to the biometric information unit fed to the system for training and testing purposes. The size of the time window  $M$  is modality-dependent ( $M = 150$  for background sensors,  $M = 100$  for all touch tasks except for keystroke, for which  $M = 50$ , and tap, for which  $M = 20$ ). These values were chosen in order to obtain an adequate amount of information for touch gestures in a similar amount of time.

For any  $M$ -sample time window, the corresponding DL model outputs a feature embedding, i.e., an  $E$ -dimensional array of real values that serves as a compact representation of the discriminative features hidden in the time-series data ( $E = 64$  for all cases). The goal of each model is mapping time windows belonging to the same user to similar representations in the embedding space, whereas embeddings of different users should be as distant as possible from each other.

### C. Training Approach

For each modality, a separate unimodal network is trained, totaling 9, i.e., 4 touch tasks and 5 background sensors. Each

of the background sensor models is developed by obtaining time windows evenly from each of the touch tasks. In fact, preliminary experiments proved this approach to be more effective, in comparison to developing a different network for every *task-modality* combination. By doing so, the features learned by the background sensor networks are more general and robust.

### D. Triplet Loss Function

In the field of neural networks, the triplet loss is an extension of the constrastive loss function, allowing networks to learn simultaneously from positive and negative comparisons. The constrastive loss function, on the other hand, only allows one *posivite-negative* comparison at once [58]. A triplet is made of an ordered sequence of three independent time windows belonging to two different classes: the Anchor (A) and the Positive (P) are time windows extracted from different acquisition sessions of the same user, whereas Negative (N) is a time window from different user data. The triplet loss function is defined as follows:

$$\mathcal{L}_{TL} = \max\{0, d^2(\mathbf{v}_A, \mathbf{v}_P) - d^2(\mathbf{v}_A, \mathbf{v}_N) + \alpha\}$$

where  $\alpha$  is the margin between positive and negative pairs and  $d$  is the Euclidean distance between *anchor-positive* ( $\mathbf{v}_A - \mathbf{v}_P$ ) pairs and *anchor-negative* ( $\mathbf{v}_A - \mathbf{v}_N$ ) pairs ( $\alpha = 1.5$ ). The triplet loss function is employed to minimize the distance between embedding vectors from the same class ( $d^2(\mathbf{v}_A, \mathbf{v}_P)$ ), and to maximize it for different class embeddings ( $d^2(\mathbf{v}_A, \mathbf{v}_N)$ ) in a single step.

### E. Fusion of Modalities

In the area of biometrics, a variety of fusion methods have been proposed in the literature [59]. In the current work, we adopt the fusion at score level, i.e., the fusion is achieved through a linear combination of the scores. In particular, the scores consist in the Euclidean distances between embeddings computed starting from simultaneous time windows pertaining to different modalities. In this way, the authentication system benefits from modularity. In fact, in the proposed authentication system, the independent models can be included at different times or easily be replaced, if their output embeddings have the same size. Consequently, the separate models can be improved individually, leaving margin for improvement. During any of the touch tasks, six modalities at most are combined: the touch information from each task (keystroke, text reading, gallery swiping, tapping), and the five background sensors (accelerometer, gravity sensor, gyroscope, linear accelerometer, magnetometer), yielding 63 different fusion combinations.

## V. EXPERIMENTAL PROTOCOL

BehavePassDB is divided into three subsets: (i) the training set, including 51 users, in which the data have been collected with every user using their own device, (ii) the validation set, including 10 users, and (iii) the evaluation set, containing 20 users. The last two sets include the same acquisition scenario

considered in the case of the training set (each user using their own device), but also the scenario of an impostor user using the same device as the owner in the last two of the four acquisition sessions. Consequently, as the training set only contains the random impostor cases, the models are optimized to compare random forgeries rather than skilled ones.

The assessment of the performance of the network is based on the comparison of embeddings belonging to each of the users with their own and with other users' embeddings. In all phases (training, validation, and evaluation), the first two sessions of each user are considered for enrolment, whereas the remaining two for verification.

With regard to the hyper-parameters in training, each of the models is trained for 150 epochs, the batch size is 512, the learning rate is 0.05, the Adam optimizer is employed with  $\beta_1 = 0.9$ ,  $\beta_2 = 0.999$  and  $\epsilon = 10^{-8}$ . Keras-Tensorflow is used to develop the models.

The training of the networks takes place by randomly withdrawing initial time instants from the whole duration of the time sequence of each of the acquisition sessions, always guaranteeing, if possible, full  $M$ -sample time windows and avoiding zero-padding.

For the purpose of validation and evaluation, up to 50 embeddings per session per user are computed, considering a variable length overlap of time windows  $\Delta$  (for the case of keystroke  $\Delta = 20$ , for the cases of text reading, gallery swiping and tap  $\Delta = 10$ , and for the case of all other background sensors  $\Delta = 50$ ). The pairwise comparison distances of all computed embeddings belonging to the 2 sessions considered at a time are averaged to obtain a single distance value for each session-to-session comparison. For each of the subjects in the validation and evaluation dataset, we obtain the score distributions as follows:

- genuine distribution: 2 values per user in the set, obtained comparing the 2 genuine verification sessions with the user's enrolment sessions;
- random impostor distribution: 2 values per user in the set, obtained comparing 2 verification sessions of a different user with the user's enrolment sessions;
- skilled impostor distribution: 2 values per user in the set, obtained comparing 2 skilled impostor sessions acquired on the same device with the user's enrolment sessions.

The performance scores described in Sec. VI are obtained considering the overall distributions as described above. In the current article, the experimental protocol and database adopted are the same as the ones used in the recently proposed Mobile Behavioral Biometrics Competition (MobileB2C) at the International Conference of Joint Biometrics (IJCB) 2022, which will be made ongoing. Consequently, the current article serves as a first, thorough benchmark.

## VI. EXPERIMENTAL RESULTS

### A. Random Impostor Case

1) *Individual Modalities*: Table II shows the results obtained on the evaluation set (the validation set scores are in brackets) considering each modality individually in the random impostor scenario. The metric chosen to evaluate

the system performance is the Area Under the Curve (AUC) of the Receiving Operating Characteristic (ROC). Each row presents the results pertaining to the touchscreen data of single task, and the corresponding background sensor data acquired simultaneously in the following columns. In terms of unimodal touchscreen information performance, the most effective task is text reading, achieving 73.22% AUC. Then, the gallery swiping and the tapping tasks achieve an AUC performance of respectively 63.58% and 64.56%. Finally, an AUC score of 57.48% is obtained during the keystroke task. Such values individually are far from satisfactory. However, such results show that in this experimental setup it is possible to extract more discriminative information from the text reading dynamics than in the case of the other tasks. The last row of Table II shows the AUC scores achieved by each background sensor averaged over the tasks. The magnetometer and the linear accelerometer consistently proves to be the best performing sensors (respectively 73.03% and 75.43% AUC), while the accelerometer, gravity sensor, and gyroscope do not reach similar results (respectively 61.80%, 60.61% and 62.86% AUC).

2) *Fusion of Modalities*: In Table III, the best subsets originated from the fusion of modalities are included. In any case, the improvement in the performance of the system due to the fusion of modalities is significant. The individual modalities altogether achieve an average 65.84% AUC, whereas the average AUC of the best modality combinations is 82.47%, i.e., a relative improvement of 25% AUC. The best performance is achieved for the task of keystroke with a fusion of touch, gyroscope, lin. accelerometer, and magnetometer, reaching 87.20% AUC. In this case, the AUC produced by the fusion of modalities is around 30% higher in absolute terms compare to the one achieved with the touch data only. The other modalities reach a level of performance around 80% AUC.

### B. Skilled Impostor Case

1) *Individual Modalities*: Table IV shows the results obtained on the evaluation set considering each modality individually in the skilled impostor scenario. The table is structured as its counterpart for the random impostor scenario. Once again the most discriminative touch modality is text reading, achieving 66.05% AUC. Then, gallery swiping produces a score 62.22% AUC. Finally, an AUC score below 60% is obtained during the tasks of keystroke and tapping. Such values individually are slightly lower than in the case of the random impostor scenario. The last row of Table IV shows the AUC scores achieved by each background sensor averaged over the tasks. In this case linear accelerometer proves to be the best performing sensor (60.06% AUC), followed by gyroscope (57.80% AUC), gravity sensor (56.35% AUC), magnetometer (55.60% AUC), and accelerometer (55.39% AUC).

2) *Fusion of Modalities*: Table V shows the best subsets originated from the fusion of modalities for the skilled impostor scenario. The fusion of the different modalities is generally beneficial for the system performance in the skilled impostor

TABLE II

RESULTS IN TERMS AUC (%) OF THE DIFFERENT INDIVIDUAL MODALITIES FOR EACH TASK IN THE **RANDOM IMPOSTOR SCENARIO**. IN BRACKETS THE RESULTS OBTAINED ON THE VALIDATION SET ARE DISPLAYED. THE BEST RESULTS ARE HIGHLIGHTED IN BOLD.

Task	Touchscreen	Accelerometer	Gravity Sensor	Gyroscope	Lin. Accelerometer	Magnetometer
<b>Keystroke</b>	57.48 (72.19)	66.23 (68.94)	63.84 (57.56)	66.47 (65.75)	79.25 (78.13)	<b>81.55</b> (65.50)
<b>Text Reading</b>	<b>73.22</b> (67.00)	58.61 (58.99)	57.28 (50.13)	59.66 (55.44)	64.72 (67.63)	<b>72.39</b> (64.87)
<b>Gallery Swiping</b>	63.58 (57.88)	62.08 (63.00)	60.47 (60.00)	60.75 (62.00)	<b>77.50</b> (79.36)	75.20 (77.31)
<b>Tapping</b>	64.56 (67.38)	60.27 (55.31)	60.83 (56.69)	64.56 (58.75)	70.66 (71.88)	<b>72.58</b> (73.25)
<b>Average of Background Sensors</b>	61.80 (61.56)	60.61 (56.10)	62.86 (60.49)	73.03 (74.25)	<b>75.43</b> (70.26)	

TABLE III

RESULTS IN TERMS OF AUC (%) OF THE BEST SUBSETS ORIGINATED FROM THE FUSION OF THE DIFFERENT INDIVIDUAL MODALITIES FOR EACH TASK IN THE **RANDOM IMPOSTOR SCENARIO**. IN BRACKETS THE RESULTS OBTAINED ON THE VALIDATION SET ARE DISPLAYED. THE BEST RESULT IS HIGHLIGHTED IN BOLD.

Task	AUC (%)	Best Modality Subset
<b>Keystroke</b>	<b>87.20</b> (83.56)	K, Gy, L, M (K, A, Gy, L)
<b>Text Reading</b>	81.31 (78.75)	TR, Gr, M (TR, A, L, M)
<b>Gallery Swiping</b>	81.58 (84.56)	Gr, L, M (GS, L, M)
<b>Tap</b>	79.80 (81.50)	Gr, Gy, L, M (T, Gy, L, M)

Acronyms of Tasks: K = Keystroke, TR = Text Reading, GS = Gallery Swiping, T = Tap. Acronyms of Background Sensors: A = Accelerometer, Gr = Gravity Sensor, Gy = Gyroscope, L = Linear Accelerometer, M = Magnetometer.

TABLE IV

RESULTS IN TERMS OF AUC (%) OF THE DIFFERENT INDIVIDUAL MODALITIES FOR EACH TASK IN THE **SKILLED IMPOSTOR SCENARIO**. IN BRACKETS THE RESULTS OBTAINED ON THE VALIDATION SET ARE DISPLAYED. THE BEST RESULTS ARE HIGHLIGHTED IN BOLD.

Task	Touchscreen	Accelerometer	Gravity Sensor	Gyroscope	Lin. Accelerometer	Magnetometer
<b>Keystroke</b>	56.18 (60.63)	56.22 (65.88)	59.43 (58.06)	58.89 (60.75)	<b>67.28</b> (59.75)	60.27 (54.56)
<b>Text Reading</b>	<b>66.05</b> (69.12)	52.92 (54.56)	<b>56.31</b> (59.75)	50.78 (51.37)	53.33 (54.50)	50.67 (55.13)
<b>Gallery Swiping</b>	62.22 (67.25)	51.45 (55.56)	53.77 (61.25)	60.53 (52.62)	<b>63.73</b> (54.06)	57.36 (57.00)
<b>Tapping</b>	59.11 (51.13)	<b>60.98</b> (50.50)	55.88 (58.81)	<b>60.98</b> (64.19)	55.88 (68.38)	54.08 (67.06)
<b>Average of Background Sensors</b>	55.39 (58.22)	56.35 (59.47)	57.80 (57.23)	<b>60.06</b> (59.17)	55.60 (58.44)	

TABLE V

RESULTS IN TERMS OF AUC (%) OF THE BEST SUBSETS ORIGINATED FROM THE FUSION OF THE DIFFERENT INDIVIDUAL MODALITIES FOR EACH TASK IN THE **SKILLED IMPOSTOR SCENARIO**. IN BRACKETS THE RESULTS OBTAINED ON THE VALIDATION SET ARE DISPLAYED. THE BEST RESULT IS HIGHLIGHTED IN BOLD.

Task	AUC (%)	Best Modality Subset
<b>Keystroke</b>	<b>68.72</b> (70.50)	K, A, Gr, Gy, L, M (K, A, Gr, Gy, L)
<b>Text Reading</b>	66.73 (69.12)	TR, Gr (TR)
<b>Gallery Swiping</b>	67.52 (67.25)	GS, Gy, L (GS)
<b>Tap</b>	61.92 (70.62)	T, A, L (Gy, L)

Acronyms of Tasks: K = Keystroke, TR = Text Reading, GS = Gallery Swiping, T = Tap. Acronyms of Background Sensors: A = Accelerometer, Gr = Gravity Sensor, Gy = Gyroscope, L = Linear Accelerometer, M = Magnetometer.

case as well, even though the overall performance is not as good compared to the random impostor scenario. This is in fact a much more challenging scenario in which the impostor user can imitate the behavior of the genuine user and also they both use exactly the same device. The individual modalities achieve an average 58.75% AUC, whereas the average AUC of the best modality combinations is 66.22% AUC, i.e., a relative improvement of 12.71% AUC. The best performance is achieved for the task of keystroke with a fusion of all modalities, reaching 68.72% AUC. In this case, the AUC produced by the fusion of modalities is around 10% higher in absolute terms compared to the one achieved with the touch data only. The performance of the remaining modalities is comparable, apart from the task of tapping (60.98% of AUC), which does not improve very much.

### C. Discussion

Interesting conclusions can be drawn by comparing the results presented in the tables above.

The beneficial effects of the fusion of the different modalities is consistent, and it is greater in the cases where the fused modalities achieve already good results individually. Consequently, developing unimodal models able to perform well is a key aspect in order to improve the system performance.

With regard to the quantification of the device bias in the learned representation, we can compare the results shown in Table II with those of Table IV. In the last row of the two tables it is possible to see the values averaged over the different tasks. All background sensors achieve lower performance in the more challenging skilled scenario. Such trend is graphically represented also in Fig. 3, which shows the ROC curves for

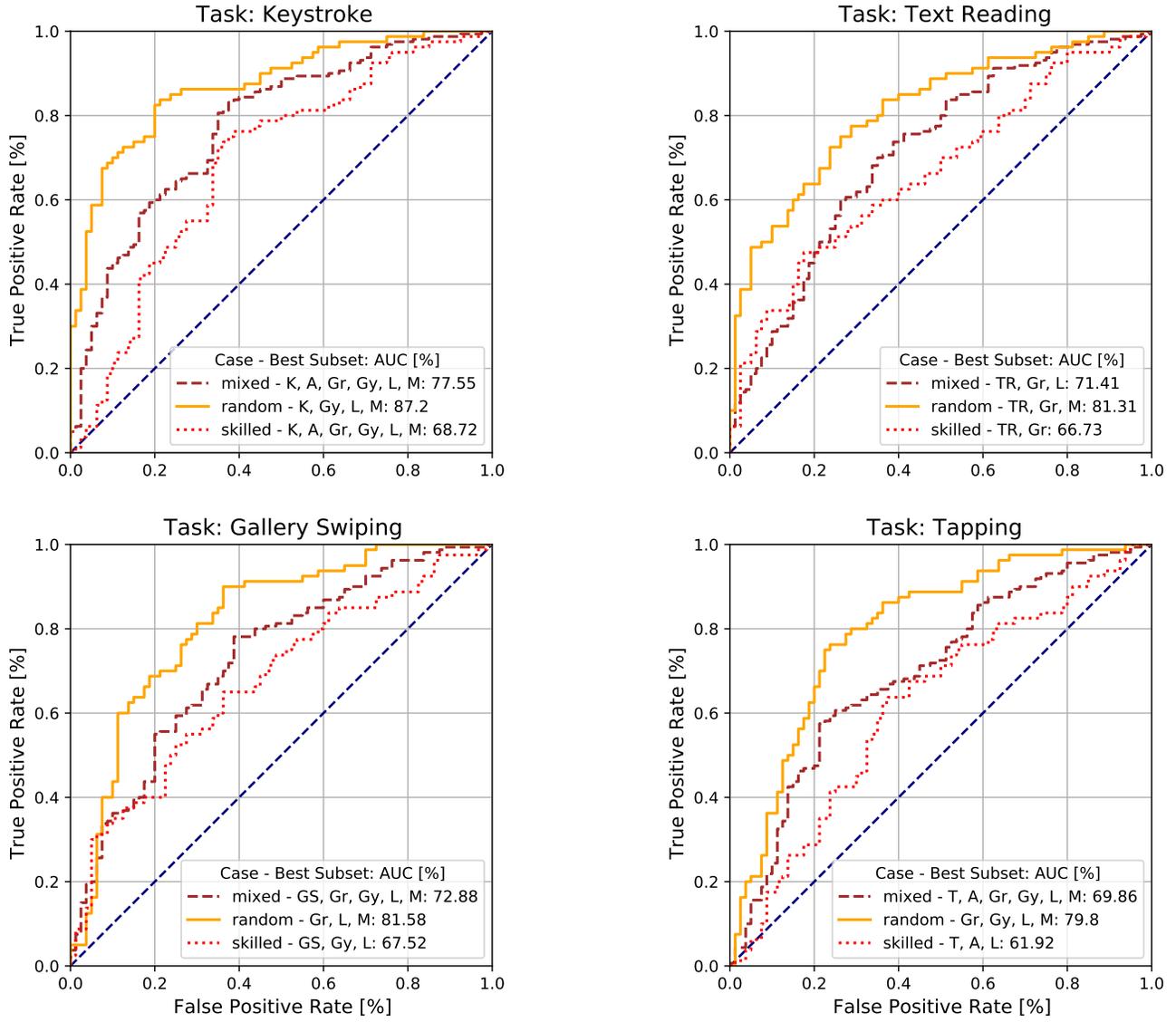


Fig. 3. The ROC curves calculated for each of the tasks: keystroke, text reading, gallery swiping, tapping. Each ROC curves shows the best results for the random, skilled, and the mixed distribution of impostor data. The AUC value is also indicated in the legend.

the four tasks considered. Each of the graph is related to a different task and shows the ROC curve for the best fusion subset considering both the described impostor scenarios. Additionally, it is possible to see the *mixed scenario*, in which the impostor distribution is obtained including both previously described impostor cases. In particular, the greatest impact is on the magnetometer and lin. accelerometer (respectively 20% and 13% lower in absolute terms), whereas the other modalities only undergo a 5% AUC reduction. This trend might be due to the fact that these two sensors have a greater device bias impact in the performance, reflecting more the device fingerprint compared to the others. However, it should be pointed out that this is a more challenging case as the impostor user is next to the genuine one and could imitate the dynamics of the genuine user in a better way. Moreover, the training set of the models only contains the random impostor cases, consequently they are optimized to compare random forgeries rather than skilled ones. In order to further improve the skilled scenario it would be needed to also have examples of skilled forgeries during the training process, but such data

collection on a larger scale can be difficult to achieve, while guaranteeing the same realistic conditions as the evaluation dataset. On the flip side, such bias could be exploited to implement a transparent security technology as a second factor in a 2-factor authentication (2FA) process, as could be a remote security-wise critical mobile application, as every user would be using their own mobile device. Such trend also characterizes the touch tasks, although the AUC reduction is slightly less.

In comparison with recent related studies in the field [7], [11], [13], [19] (see Sec. II), although adopting a similar biometric system, the authentication results achieved in this article are not as high. This trend could be due to the fact that BehavePassDB is a very challenging database, especially for the dedicated skilled impostor case, as it is designed to investigate the feasibility of BBICA systems in different real-world scenarios. In the field of mobile behavioral biometrics, it is in fact often difficult to reach a global and significant conclusion from the comparison of different systems, given the different approaches, scopes, metrics, and the usage of self-

collected non-public databases. Therefore, we aim to provide a useful tool to the biometric community to advance towards different application use cases and impostor scenarios.

## VII. CONCLUSIONS

This article has focused on an analysis of individual and multimodal behavioral biometric traits suitable for the application of mobile continuous authentication, with fusion at score level. We presented BehavePassDB, a new publicly available database of wide ranging mobile interaction data, collected in an unsupervised scenario. The novel aspect of this database is the possibility to evaluate the effectiveness of developed systems considering the case of several users using their own device (random impostor scenario), and two different users on the same device (skilled impostor scenario). A first benchmark of the database has been carried out in the current paper, considering several modalities such as touchscreen and background sensor data. For every individual modality, a separate LSTM RNN with triplet loss has been considered. Our results show that the best performing source is the keystroke dynamics for touchscreen data, and the magnetometer and the gravity sensor for background sensors. Nevertheless, the discriminative ability of the system is significantly enhanced by the fusion, typically reaching a 80%-87% AUC range in the random impostor case and 62%-69% AUC in the skilled impostor case. It appears clear that the learned features in the random impostor case are not robust when data are coming from the same device.

Finally, given the fact that we opted for a data collection approach in which the user interaction data are acquired during dense gesture-based dedicated sessions to maximize the amount of biometric information acquired. Consequently, it would be interesting, for future work, to assess possible system performance improvements due to more training data, including the generation of synthetic data, which proved to be a powerful tool in related fields [60].

## ACKNOWLEDGMENT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 860315, and from Orange Labs. R. Vera-Rodriguez, R. Tolosana, and A. Morales are also supported by INTER-ACTION (PID2021-126521OB-I00 MICINN/FEDER).

## REFERENCES

- [1] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: Approaches, threats and trends," *Computer Networks*, vol. 170, p. 107118, 2020.
- [2] S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection*. 2nd Ed., Springer, 2019.
- [3] C. Rathgeb, R. Tolosana, R. Vera-Rodriguez, and C. Busch, "Handbook of digital face manipulation and detection: From deepfakes to morphing attacks." 2022.
- [4] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "BioTouchPass2: Touchscreen Password Biometrics Using Time-Aligned Recurrent Neural Networks," *IEEE Trans. on Information Forensics and Security*, vol. 15, pp. 2616–2628, 2020.
- [5] P. Perera and V. M. Patel, "Efficient and low latency detection of intruders in mobile active authentication," *IEEE Trans. on Information Forensics and Security*, vol. 13, no. 6, pp. 1392–1405, 2017.
- [6] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges," *IEEE Signal Processing Magazine*, vol. 33, no. 4, pp. 49–61, 2016.
- [7] G. Stragapede, R. Vera-Rodriguez, R. Tolosana, A. Morales, A. Acien, and G. Le Lan, "Mobile behavioral biometrics for passive authentication," *Pattern Recognition Letters*, 2022.
- [8] P. Delgado-Santos, G. Stragapede, R. Tolosana, R. Guest, F. Deravi, and R. Vera-Rodriguez, "A survey of privacy vulnerabilities of mobile device sensors," *ACM Computing Surveys*, 2022.
- [9] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Preventing Lunchtime Attacks: Fighting Insider Threats With Eye Movement Biometrics," in *The Network and Distributed System Security Symposium*, 2015.
- [10] A. Acien, A. Morales, J. Fierrez, R. Vera-Rodriguez, and O. Delgado-Mohatar, "BeCAPTCHA: Behavioral bot detection using touchscreen and mobile sensors benchmarked on HuMidd," *Engineering Applications of Artificial Intelligence*, vol. 98, p. 104058, 2021.
- [11] D. Deb, A. Ross, A. K. Jain, K. Prakah-Asante, and K. V. Prasad, "Actions Speak Louder Than (Pass)Words: Passive Authentication of Smartphone\* Users via Deep Temporal Features," in *Proc. 2019 Intl. Conf. on Biometrics*, 2019.
- [12] G. Li and P. Bours, "Studying WiFi and accelerometer data based authentication method on mobile phones," in *Proc. of the 2018 2nd Intl. Conf. on Biometric Engineering and Applications*, 2018.
- [13] N. Neverova, C. Wolf, G. Lacey, L. Fridman, D. Chandra, B. Barbello, and G. Taylor, "Learning Human Identity From Motion Patterns," *IEEE Access*, vol. 4, pp. 1810–1820, 2016.
- [14] A. Vajdi, M. R. Zaghian, S. Farahmand, E. Rastegar, K. Maroofi, S. Jia, M. Pomplun, N. Haspel, and A. Bayat, "Human Gait Database for Normal Walk Collected by Smart Phone Accelerometer," *arXiv:1905.03109*, 2019.
- [15] A. Garbuz, A. Epishkina, and K. Kogos, "Continuous Authentication of Smartphone Users via Swipes and Taps Analysis," in *Proc. of the 2019 European Intelligence and Security Informatics Conf.*, 2019.
- [16] T. Zhu, Z. Qu, H. Xu, J. Zhang, Z. Shao, Y. Chen, S. Prabhakar, and J. Yang, "RiskCog: Unobtrusive real-time user authentication on mobile devices in the wild," *IEEE Transactions on Mobile Computing*, vol. 19, no. 2, pp. 466–483, 2019.
- [17] D. Cilia and F. Inguanez, "Multi-Model authentication using keystroke dynamics for Smartphones," in *Proc. of the 2018 IEEE 8th Intl. Conf. on Consumer Electronics*, 2018.
- [18] A. Das and *et al.*, "Exploring ways to mitigate sensor-based smartphone fingerprinting," *arXiv:1503.01874*, 2015.
- [19] M. Abuhamad, T. Abuhmed, D. Mohaisen, and D. Nyang, "AUToSen: Deep-Learning-Based Implicit Continuous Authentication Using Smartphone Sensors," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5008–5020, 2020.
- [20] A. Acien, A. Morales, R. Vera-Rodriguez, and J. Fierrez, "Smartphone Sensors For Modeling Human-Computer Interaction: General Outlook And Research Datasets For User Authentication," in *Proc. IEEE Intl. Workshop on Consumer Devices and Systems*, 2020.
- [21] K. Palin, A. M. Feit, S. Kim, P. O. Kristensson, and A. Oulasvirta, "How Do People Type on Mobile Devices? Observations from a Study with 37,000 Volunteers," in *Proc. of the 21st Intl. Conf. on Human-Computer Interaction with Mobile Devices and Services*, 2019.
- [22] A. Acien, A. Morales, J. V. Monaco, R. Vera-Rodriguez, and J. Fierrez, "Typenet: Deep learning keystroke biometrics," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 4, no. 1, pp. 57–70, 2022.
- [23] G. Stragapede, R. Vera-Rodriguez, R. Tolosana, A. Morales, A. Acien, and G. Le Lan, "Mobile passive authentication through touchscreen and background sensor data," in *Proc. of the IEEE Intl. Workshop on Forensics and Biometrics*, 2022.
- [24] N. Eagle and A. Pentland, "MIT Reality Mining Dataset," *Journal Personal and Ubiquitous Computing*, vol. 10, no. 4, pp. 255–268, 2006.
- [25] H. Saeveane and P. Bhatarakosol, "User authentication using combination of behavioral biometrics over the touchpad acting like touch screen of mobile device," in *Proc. of the 2008 Intl. Conf. on Computer and Electrical Engineering*, 2008.
- [26] S. Zahid, M. Shahzad, S. A. Khayam, and M. Farooq, "Keystroke-based user identification on smart phones," in *Proc. of the Intl. Workshop on Recent Advances in Intrusion Detection*, 2009.
- [27] C. Shepard, A. Rahmati, C. Tossell, L. Zhong, and P. Kortum, "LiveLab: measuring wireless networks and smartphone users in the field," *ACM SIGMETRICS Performance Evaluation Review*, vol. 38, no. 3, pp. 15–20, 2011.

- [28] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE transactions on information forensics and security*, vol. 8, no. 1, pp. 136–148, 2012.
- [29] A. Serwadda, V. V. Phoha, and Z. Wang, "Which verifiers work?: A benchmark evaluation of touch-based authentication algorithms," in *Proc. of the 2013 IEEE 6th Intl. Conf. on Biometrics: Theory, Applications and Systems*, 2013.
- [30] H. Zhang, V. M. Patel, M. Fathy, and R. Chellappa, "Touch gesture-based active user authentication using dictionaries," in *Proc. of the 2015 IEEE Winter Conf. on Applications of Computer Vision*, 2015.
- [31] T. Feng, J. Yang, Z. Yan, E. M. Tapia, and W. S., "Tips: Context-aware implicit user identification using touch screen in uncontrolled environments," in *Proc. of the 15th Workshop on Mobile Computing Systems and Applications*, 2014.
- [32] H. Xu, Y. Zhou, and M. R. Lyu, "Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones," in *Proc. of the 10th Symposium On Usable Privacy and Security*, 2014.
- [33] H. Saevanee, N. Clarke, S. Furnell, and V. Biscione, "Continuous user authentication using multi-modal biometrics," *Computers & Security*, vol. 53, pp. 234–246, 2015.
- [34] T. Hoang, D. Choi, and T. Nguyen, "Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme," *International Journal of Information Security*, vol. 14, no. 6, pp. 549–560, 2015.
- [35] T. J. Neal, D. L. Woodard, and A. D. Striegel, "Mobile device application, bluetooth, and Wi-Fi usage data as behavioral biometric traits," in *Proc. of the 2015 IEEE 7th Intl. Conf. on Biometrics Theory, Applications and Systems*, 2015.
- [36] J. Wu and Z. Chen, "An implicit identity authentication system considering changes of gesture based on keystroke behaviors," *International Journal of Distributed Sensor Networks*, vol. 11, no. 6, p. 470274, 2015.
- [37] J. Nader, A. Alsadoon, P. W. C. Prasad, A. Singh, and A. Elchouemi, "Designing touch-based hybrid authentication method for smartphones," *Procedia Computer Science*, vol. 70, pp. 198–204, 2015.
- [38] R. Murmura, A. Stavrou, D. Barbará, and D. Fleck, "Continuous authentication on mobile devices using power consumption, touch gestures and physical movement of users," in *Proc. of the Intl. Symp. on Recent Advances in Intrusion Detection*, 2015.
- [39] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "HMOG: New behavioral biometric features for continuous authentication of smartphone users," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 877–892, 2015.
- [40] V. Zaliva, W. Melicher, S. Saha, and J. Zhang, "Passive user identification using sequential analysis of proximity information in touchscreen usage patterns," in *Proc. of the 2015 8th Intl. Conferenc.e on Mobile Computing and Ubiquitous Networking*, 2015.
- [41] L. Lu and Y. Liu, "Safeguard: User reauthentication on smartphones via behavioral biometrics," *IEEE Transactions on Computational Social Systems*, vol. 2, no. 3, pp. 53–64, 2015.
- [42] M. J. Coakley, J. V. Monaco, and C. C. Tappert, "Keystroke biometric studies with short numeric input on smartphones," in *Proc. of the 2016 IEEE 8th Intl. Conf. on Biometrics Theory, Applications and Systems*, 2016.
- [43] A. N. Putri, Y. D. W. Asnar, and S. Akbar, "A continuous fusion authentication for android based on keystroke dynamics and touch gesture," in *Proc. of the 2016 Intl. Conf. on Data and Software Engineering*, 2016.
- [44] R. Kumar, V. V. Phoha, and A. Serwadda, "Continuous authentication of smartphone users by fusing typing, swiping, and phone movement patterns," in *Proc. of the 2016 IEEE 8th Intl. Conf. on Biometrics Theory, Applications and Systems*, 2016.
- [45] C. Shen, Y. Zhang, X. Guan, and R. A. Maxion, "Performance analysis of touch-interaction behavior for active smartphone authentication," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 498–513, 2015.
- [46] M. Antal and L. Z. Szabó, "Biometric authentication based on touchscreen swipe patterns," *Procedia Technology*, vol. 22, pp. 862–869, 2016.
- [47] K. W. Nixon, X. Chen, Z. Mao, and Y. Chen, "Slowmo-enhancing mobile gesture-based authentication schemes via sampling rate optimization," in *Proc. of the 2016 21st Asia and South Pacific Design Automation Conf.*, 2016.
- [48] A. Buriro, B. Crispo, F. Delfrari, and K. Wrona, "Hold and sign: A novel behavioral biometrics for smartphone user authentication," in *Proc. of the 2016 IEEE Security and Privacy Workshops*, 2016.
- [49] U. Mahbub, S. Sarkar, V. M. Patel, and R. Chellappa, "Active user authentication for smartphones: A challenge data set and benchmark results," in *Proc. of the 2016 IEEE 8th Intl. Conf. on Biometrics Theory, Applications and Systems*, 2016.
- [50] W. Lee and R. B. Lee, "Implicit smartphone user authentication with sensors and contextual machine learning," in *Proc. of the 2017 47th Annual IEEE/IFIP Intl. Conf. on Dependable Systems and Networks*, 2017.
- [51] H. Zhu, J. Hu, S. Chang, and L. Lu, "ShakeIn: Secure user authentication of smartphones with single-handed shakes," *IEEE transactions on mobile computing*, vol. 16, no. 10, pp. 2901–2912, 2017.
- [52] S. K. Al Kork, I. Gowthami, X. Savatier, T. Beyrouthy, J. A. Korbane, and S. Roshdi, "Biometric database for human gait recognition using wearable sensors and a smartphone," in *Proceedings of the 2017 2nd Intl. Conf. on Bio-engineering for Smart Technologies*, 2017.
- [53] S. Amini, V. Noroozi, A. Pande, S. Gupte, P. S. Yu, and C. Kanich, "Deepauth: A framework for continuous user re-authentication in mobile apps," in *Proc. of the 27th ACM Intl. Conf. on Information and Knowledge Management*, 2018.
- [54] M. Singh, R. Singh, and A. Ross, "A comprehensive overview of biometric fusion," *Information Fusion*, vol. 52, pp. 187–205, 2019.
- [55] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognition Letters*, vol. 79, pp. 80–105, 2016.
- [56] Ruben T. and R. Vera-Rodriguez *et al.*, "SVC-onGoing: Signature verification competition," *Pattern Recognition*, vol. 127, p. 108609, 2022.
- [57] R. Tolosana, R. Vera-Rodriguez, J. Fierrez and J. Ortega-Garcia, "Deep-sign: Deep on-line signature verification," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 2, pp. 229–239, 2021.
- [58] K. Q. Weinberger and L. K. Saul, "Distance Metric Learning for Large Margin Nearest Neighbor Classification," *Journal of Machine Learning Research*, vol. 10, no. 9, pp. 207–244, 2009.
- [59] A. Ross and A. Jain, "Information fusion in biometrics," *Pattern recognition letters*, vol. 24, no. 13, pp. 2115–2125, 2003.
- [60] R. Tolosana, P. Delgado-Santos, A. Perez-Uribe, R. Vera-Rodriguez, J. Fierrez, and A. Morales, "Deepwritsyn: On-line handwriting synthesis via deep short-term representations," in *Proc. AAAI Conference on Artificial Intelligence*, 2021.