Signal, Image and Video Processing
https://doi.org/10.1007/s11760-024-03532-3

ORIGINAL PAPER

# Dynamic authentication on mobile devices: evaluating continuous identity verification through swiping gestures

**Anass Sejjari**[1] · **Chouaib Moujahdi**[2] · **Noureddine Assad**[1] · **Haidine Abdelfatteh**[1]

Received: 6 July 2024 / Revised: 8 August 2024 / Accepted: 20 August 2024


**Abstract**
Biometrics, the science of identifying individuals based on unique physiological and behavioral traits, has witnessed widespread adoption in recent years due to its applications in security, access control, and authentication. Behavioral biometrics, which leverage unique behavioral patterns, offer a non-intrusive and user-friendly approach to identity verification. Swiping gestures, a fundamental interaction mechanism on mobile devices, hold significant promise for continuous verification. This paper delves into the domain of behavioral biometrics, specifically focusing on the utilization of swiping gestures for continuous identity verification on mobile devices. Unlike discrete verification methods, continuous verification offers an ongoing assessment of an individual's authenticity, aligning with the pace of modern interactions while enhancing security. We evaluate various Machine Learning one-class classifiers, including a deep learning model, to evaluate continuous verification systems while using a huge real-world and publicly available dataset. Our results shows that the used deep learning model performs well in all scenarios of test compared to traditional classifiers. A good value of the Equal Error Rate equal to 0.20% is achieved using the deep learning model. The used models in this paper can be downloaded from this link: https://github.com/AnassSej/Dynamic-Authentication-Swipes/.

**Keywords** Biometrics · Behavioral trait · Swiping gestures · Authentication · Continuous verification

## 1 Introduction

In recent years, biometrics has attracted considerable interest due to its diverse applications in security, access control, and authentication [1]. The capability to accurately verify an individual's identity has resulted in the widespread adoption of biometric systems across various domains, such as law enforcement, border control, and digital devices. These systems offer a robust and convenient user-friendly alternative to traditional authentication methods, such as passwords, PINs, and ID cards.

In an increasingly digitized world where personal data security is paramount, the utilization of biometrics has emerged as a critical solution. The remarkable accuracy that biometric systems offer stems from the fact that they leverage inherent and immutable traits specific to each individual. This distinctiveness not only enhances security but also streamlines the authentication process. With applications spanning from high-security environments to everyday devices, the use of biometric systems has contributed to a paradigm shift in how we safeguard our information and assets.

Within the realm of biometrics, two distinct categories emerge: physiological and behavioral biometrics [1]. Physiological biometrics rely on inherent physical characteristics like fingerprints, iris patterns, and facial features. These traits are deeply unique to individuals and are considered difficult to forge. In contrast, behavioral biometrics harness unique behavioral patterns, such as keystroke dynamics, gait analysis, and swiping gestures. The latter category, often referred

✉ Anass Sejjari
sejjari.anass@ucd.ac.ma

Chouaib Moujahdi
chouaib.moujahdi@is.um5.ac.ma

Noureddine Assad
assad.n@ucd.ac.ma

Haidine Abdelfatteh
haidine.a@ucd.ac.ma

[1] Chouaib Doukkali University, National School of Applied Sciences, Laboratory of Information Technologies, 24000 El Jadida, Morocco

[2] Scientific Institute, Mohammed V University in Rabat, Morocco

Published online: 02 September 2024

to as behavioral biometrics, holds great promise for its non-intrusive and user-friendly nature.

Behavioral biometrics delve into the nuances of how individuals interact with their devices and surroundings. This category capitalizes on behaviors that are less static than physiological traits, allowing for more adaptive authentication mechanisms. Behavioral biometrics can also be particularly relevant in scenarios where physiological traits might be difficult to acquire, such as remote verification. This blend of convenience and adaptability positions behavioral biometrics as an attractive avenue for various applications, ranging from seamless mobile device unlock to proactive fraud detection.

This paper delves into the domain of behavioral biometrics, with a specific focus on the utilization of swiping gestures as a means of continuous verification on mobile devices, particularly phones and tablets [2]. Unlike discrete verification methods that ascertain identity at a single point in time, continuous verification offers a dynamic and ongoing assessment of an individual's authenticity [3]. Swiping gestures, a fundamental interaction mechanism on touch-enabled devices, present an intriguing avenue for establishing identity based on unique behavioral patterns.

Swiping gestures represent a fascinating realm of human-device interaction. The intricate patterns and variations in swiping behavior are influenced by individual motor skills, hand-eye coordination, and even contextual factors [4]. By capturing and analyzing these subtleties, we can construct a comprehensive picture of the user's behavior over time. Thus, continuous verification, using swiping gestures, aligns with the pace of modern interactions, making it a suitable component of user experience while enhancing security.

It is important to distinguish between the modes of identification and verification within biometric systems [5]. Identification involves determining a person's identity from a pool of potential candidates, while verification aims to authenticate a person's claimed identity. While identification suits scenarios like criminal investigations on large-scale databases, verification caters to daily interactions where users need rapid and unobtrusive access. This paper primarily addresses the latter, where the objective is to continuously verify the authenticity of an individual using swiping gestures. By focusing on verification through swipes, we can refine authentication systems that align with contemporary needs, ensuring security without compromising convenience.

The motivation behind this study stems from the desire to explore the viability of swiping gestures for continuous verification and to evaluate whether traditional Machine Learning methods or those that are based on Deep Learning are the most suitable for managing this biometric trait. To achieve this, we harness a comprehensive and publicly available dataset [6] that encompasses a substantial number of users and their swiping behaviors. By employing this dataset, we seek to analyze, evaluate, and refine the effectiveness of swiping-based continuous verification systems in conditions that are close to real world scenarios.

The rest of the paper is organized as follows. In Sect. 2, we will review the existing literature in the field. We will detail the dataset, system conception, and experimental setup in Sect. 3. Our experimental results are presented in Sect. 4. Finally, conclusions and perspectives are provided in Sect. 5.

## 2 Literature review

Swipe gestures are commonly used in mobile device authentication methods such as pattern unlock or gesture-based passwords. Recently, the biometrics research community is making great efforts to adopt swipes for continuous identity verification. Since most works on continuous identity verification using swipes extract and use relatively the same features, that we will present in Table 2 of Sect. 3, we believe, at least currently, that these approaches can be classified into two main categories: 1) those that primarily use traditional machine learning methods and 2) those that incorporate deep learning methods into their conception.

For the first category, we can find for example [7] that present a continuous authentication (CA) biometric system based on swipe gestures. The system compares user behavior with stored information and adjusts trust accordingly, blocking access if trust is low. It introduces a novel scheme for CA on mobile devices, reacting to each user action. Three verification processes and a feature selection scheme are proposed. This study introduces new performance measures (ANGA and ANIA) and shows good performance. In [8], authors focus on enhancing user authentication on mobile devices. The study involved collecting touch operation data from 11 subjects, observing their touch patterns during basic operations, text browsing, and web browsing using an Android app. This data was collected over six months and analyzed for long-term trends. The results indicated that user identification accuracy remained consistent for pinch gestures and vertical swipes during text browsing over time. However, accuracy dropped by approximately 10% for swipe gestures during web browsing as the number of experiments increased. In the same catégory, [9] presents a multi-biometric system designed for continuous and transparent student authentication within e-learning platforms. This system supports various devices and activities, using five biometric traits, including gestures, to verify students' identities based on their presence and interactions. This system operates without additional devices or actions, making it practical for student verification. Its dynamic architecture ensures fast, accurate performance across different devices and methods, combining physiological and behavioral biometrics within a time-based authentication window. Additionally, the subsys-

tems can integrate various algorithms and provide reliability measures. In [10], that use the BrainRun dataset, a interested study is conducted with the aim of developing a method for continuous implicit authentication using a One-Class Support Vector Machine (OCSVM) to detect gestures of authorized users and lock unauthorized users. The OCSVM model is trained solely on the swipe gestures of the legitimate user and tested on both the legitimate user's gestures and those of all other users. A confidence level is utilized as a classification reinforcement technique, adjusting the current user's confidence level based on the classification outcome and locking the device if the confidence level falls below a predefined threshold. Over time, the confidence level may also decrease to enforce device locking if it remains unused for a certain interval. In the same category, we can cite as well [4] and [11].

For the second category (i.e., Deep Learning methods), there is for example [12], where authors explores using deep learning networks to recognize user actions, a technique expanding beyond image, audio, and text data to structured data. Unlike previous studies that used one-class SVM for outlier detection, this research employs binary classification. It tests deep learning models with three dense layers and two configurations: 64 and 128 nodes per layer. The data, processed as tensors, undergoes 200 epochs of training and is evaluated for accuracy, mean error, and false acceptance rates. The dataset is analyzed by feature subsets, and the results, which show an average accuracy of 88% and a 15% Equal Error Rate, highlight the effectiveness of deep learning for continuous authentication on mobile devices. In another example, [13] authors have conducted a study exploring continuous authentication using touch gestures and keystroke dynamics by applying feature-level fusion to improve performance and address security and usability concerns. it introduces new feature sets and uses the BioGames App to collect data from 39 participants. Comparisons between Multi-Layer Perceptron (MLP) and Long Short-Term Memory (LSTM) networks are made for touch gestures and keystroke dynamics. The fusion of these modalities greatly enhances system performance. In the same category, we can find as well [14] that presents a continuous verification system based on the transformation of swipes from BioIdent and HMOG datasets to images, to be used later to train and test the MobileNetV2 network. This methodology has achieved an EER of 10.45%.

## 3 Dataset, system conception and experimental setup

In this section, we present an overview of the dataset used for our experiments. Then, a brief introduction to the continuous verification system is provided. Finally, we detail the used experimental setup to evaluate the developed system.

**Table 1** Some statistics on BrainRun dataset

| Item | Number |
|---|---|
| Users | 2221 |
| Devices | 2418 |
| Played Games | 106,805 |
| Gestures | 3,110,101 |
| Taps | 2,463,115 |
| Swipes | 646,986 |

### 3.1 Dataset overview

The dataset utilized in this research is derived from an educational game called "BrainRun", developed by [6] to capture a diverse array of hand gestures and sensor data from numerous users and devices. It consists of three main components: gesture data, user/game details, and sensor data. The dataset covers a wide range of scenarios, users, and devices, making it well-suited for continuous authentication research. The data is organized into JSON files with appropriate labels, allowing for easy processing and querying using MongoDB. The dataset is anonymized to ensure privacy and can be utilized for research purposes concerning continuous authentication. Table 1 presents some statistics about this dataset.

The dataset includes 3.11 million gestures collected from 2221 users and 2418 devices, featuring taps and swipes with detailed attributes such as type, session ID, device ID, timestamps, screen, and data points. User and game data provide comprehensive information on registered users, their devices, games played, and gestures performed, with attributes like correct and wrong answers, user ID, device ID, game stage, game type, stars earned, timestamps, and experience points. The data includes raw sensor measurements from accelerometers, gyroscopes, magnetometers, and device motion sensors.

Figure 1 illustrates that approximately 79% of the collected gestures are taps. Thus, depicted in Fig. 2, we have separated these gestures to use just swipes for our experimentation.

### 3.2 Continuous verification system

The Continuous Verification System (CVS) revolutionizes user authentication, moving beyond the traditional binary approach. Unlike point-of-entry authentication, CVS continuously validates user identity during interactions, analyzing behavioral and biometric patterns like keystrokes, gestures, and facial expressions. CVS utilizes behavioral analysis for dynamic profiles, distinguishing genuine users from threats.

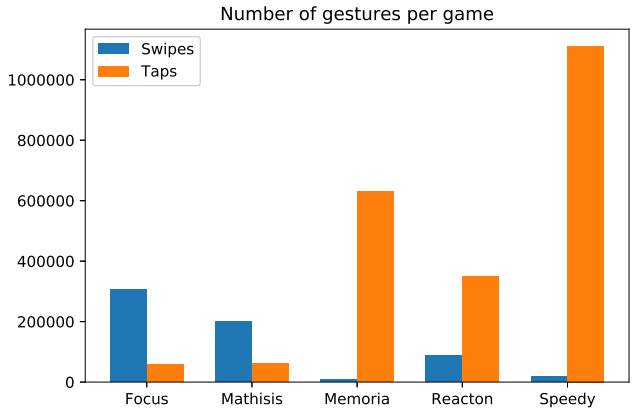


**Fig. 1** Number of gestures per game

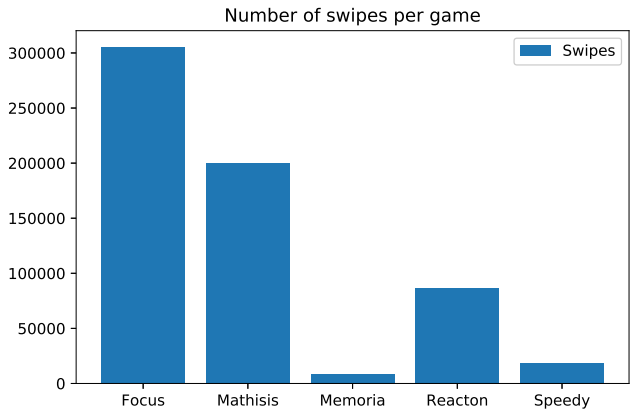


**Fig. 2** Number of swipes per game

It adapts in real-time, integrates multi-modal biometrics for enhanced security, and detects suspicious activities. With applications in finance, e-commerce, enterprise, and healthcare, CVS offers fortified security, improved experiences, and adaptive authentication. As technology advances, CVS stands to be a pivotal solution for secure digital interactions.

The Fig. 3 illustrates the general principle of operation of a CVS. When classic authentication is launched successfully, the responsibility of continuous authentication is to validate the user's gestures. If the gesture is approved, the user can proceed with device usage. However, if the gesture is not accepted, the user will be disconnected.

### 3.3 Experimental setup

To evaluate continuous identity verification through swiping gestures, "One against the universe" scenario [15] will be used. During each stage of experimentation, only the swipes of a specific individual will be known beforehand as legitimate authorized to use the device, and the selected classifier for evaluation will be trained only on theses swipes. Thus, all gestures of all other identities will be considered as impostors and they must be denied by the system, which will subsequently result in the device being locked. It is evident then that the classifier used for this purpose is a one-class classifier model.

The main objective of this classification is to minimize the False Acceptance Rate (FAR), which represents the percentage of impostors or unknown users who are incorrectly considered as the legitimate user, which gives them a control on the device with unknown consequences. At the same time, it is equally important to minimize the False Rejection Rate (FRR) as much as possible. The FRR measures the percentage of instances where the model does not recognize the original user, thereby preventing them from using the device until they reactivate their access again. The equations shown in 1 and 2 illustrate the calculation of FAR and FRR, respectively:

$$\text{FAR} = \frac{\text{Impostor accepted attempts}}{\text{Total impostor attempts}} \tag{1}$$

$$\text{FRR} = \frac{\text{Genuine refused attempts}}{\text{Total genuine attempts}} \tag{2}$$

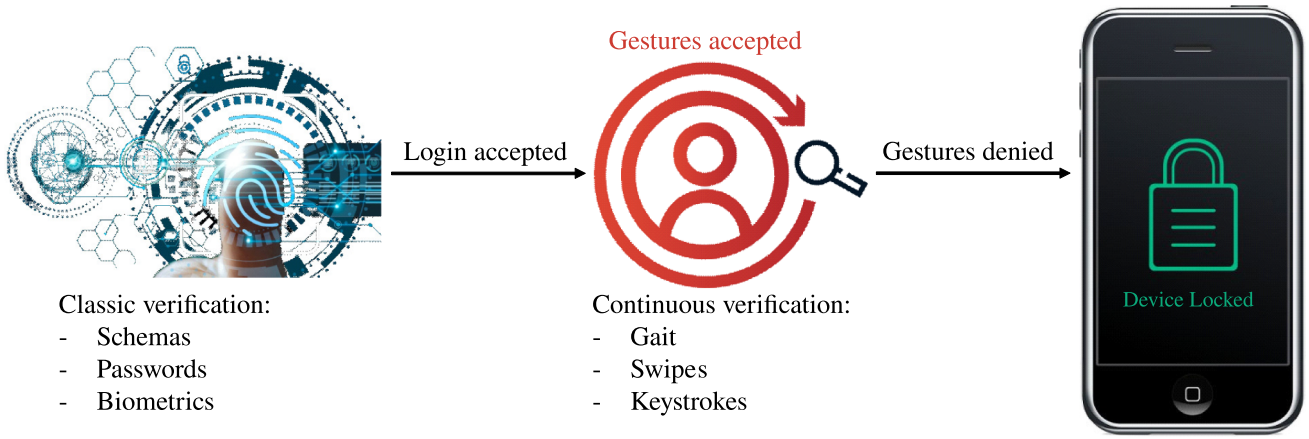


**Fig. 3** Continuous verification system architecture

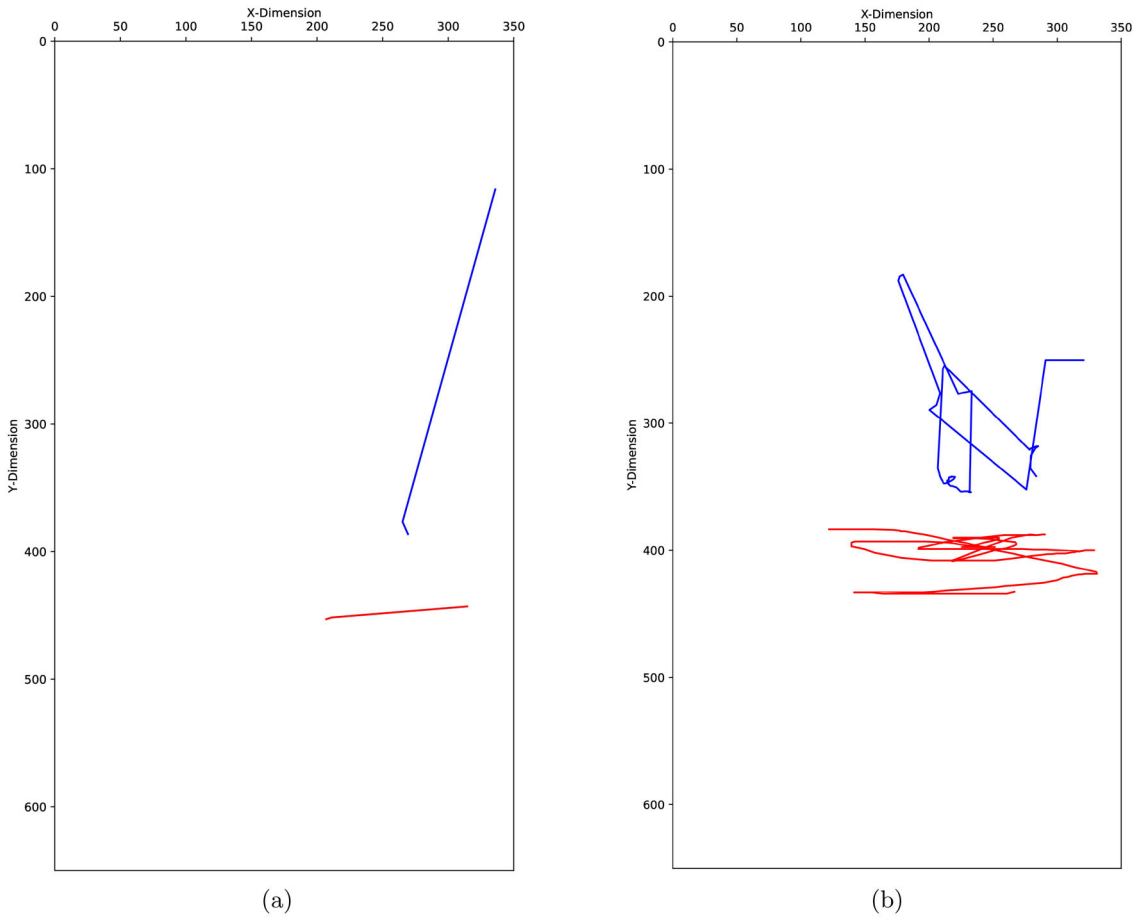


**Fig. 4** Visualization of sample swipes. **a** Swipes with a duration of less than 100 ms. **b** Swipes with a duration of less than 100 ms

Within the framework of Machine Learning modeling, to use the "One against the universe" scenario, we have selected several classifier: One-Class Support Vector Machine (OCSVM) [16], One-Class Gaussian Mixture Model (OCGMM) [17], One-Class Isolation Forest (OCIF) [18], One-Class K-Nearest Neighbor (OCKNN) [19] and the Auto-Encoder model [20]. In our specific situation, these classifiers are employed to define the feature space associated with the legitimate user and to detect the features, along with the corresponding gestures, that deviate from this profile. By extracting features from the collection of gestures, we calculate the essential attributes required for constructing the classification model. Subsequently, we proceed with the evaluation and comparison of the results generated by these diverse classifiers.

With this perspective, it should be noted that we will eliminate all data containing "tap" gestures performed by users, as well as "swipe" gestures with a duration of less than 100 ms. These "swipes" correspond to "tap", where the user's finger activates more than one point on the device. In Fig. 4a, examples of swipe movements with a duration of less than 100 ms can be seen. We will use the remaining "swipes" because they contain significantly more information, generate more precise features, and have demonstrated better results in terms of classification, as shown in the Fig. 4b. For each collected and stored "swipe" in the gestures collection, multiple points on the screen are triggered by the hand's movement and sampled by the device. The raw data of each "swipe" goes through the feature extraction layer to apply the feature calculation process.

Table 2 presents the computed features for every swipe gesture. The first eleven features are used by [10] and several other works in the literature. The last two features (i.e., DT and CA) are proposed by this study to show the importance of this conception step to improve the performance of continue verification using swipes.

Figure 2 illustrates that "swipe" movements were recorded from the games "Focus", "Mathisis", and "Reacton", while "tap" gestures were collected from the games "Speedy", "Memoria", and "Reacton". For our experiment, we have chosen to focus on "swipes". Therefore, we will use the data collected from the games "Focus", "Mathisis", and "Reacton". However, the creators of BrainRun [6] have indicated that the game "Reacton" requires users to either press or per-

**Table 2** Extracted features from every swipe gesture [10]

| Alias | Name | Description |
|---|---|---|
| HTL | Horizontal trace length | Calculated the distance between the first and last points of the swipe on the horizontal axis |
| VTL | Vertical trace length | Calculated the distance between the first and last points of the swipe on the vertical axis |
| Slope | Slope | The slope of the straight line that best fits the swipe's trace |
| MSE | Mean squared error | The mean squared error between the swipe's points and the straight line |
| MAE | mean absolute error | The mean absolute error between the swipe's points and the straight line |
| MedAE | Median absolute error | The median absolute error between the swipe's points and the straight line |
| CoD | Coefficient of determination | The coefficient of determination between the swipe's points and the straight line |
| HA | Horizontal acceleration | The mean acceleration of the user's movement along the horizontal axis |
| VA | Vertical acceleration | The mean acceleration of the user's movement along the vertical axis |
| HMP | Horizontal mean | The average position of the user's gesture along the horizontal axis |
| VMP | Vertical mean | The average position of the user's gesture along the vertical axis |
| DT* | Distance travelled | **Calculate the Euclidean distance between the initial and final points of the swipe** |
| CA* | Covered area | **The rectangular area covered by the swipe** |

*New proposed features

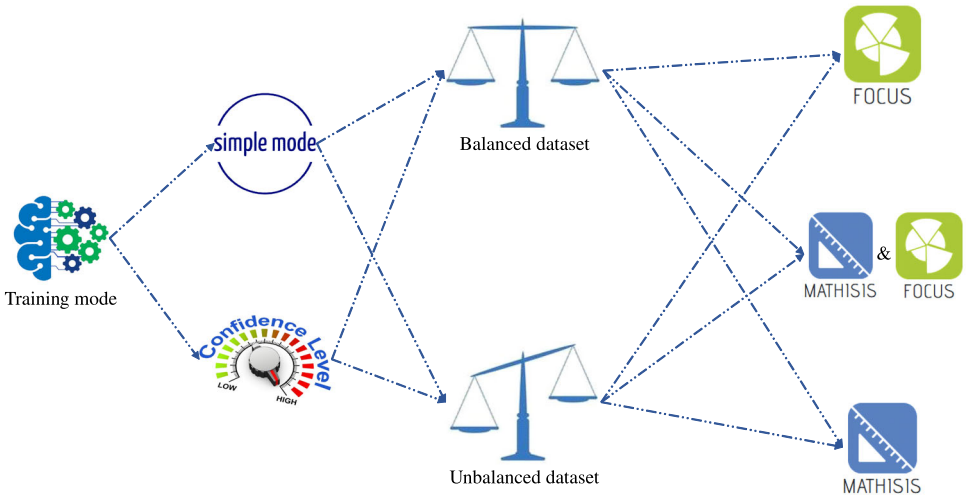


**Fig. 5** All scenarios of the used training procedure

form a "swipe" in a specific area, which may not be relevant for classification. Due to these considerations, our experiments will exclusively rely on "swipes" from the games "Mathisis" which generate horizontal movements, "Focus" that generate vertical movements, and "Mathisis&Focus" which combine both horizontal and vertical movements.

In the classification experiments, we conducted simple trials using classifiers alone (i.e., "Simple" mode), as well as precision improvements by leveraging the system's confidence level (i.e., "Confidence Level" mode). The confidence level is an enhancement technique that is integrated into our system, representing the system's certainty about the current user's identity on the device. Initially, this confidence level is set at 60%, and it has a threshold of 30% below where the device locks. Each gesture processed by the system impacts the used confidence level based on the classification result. If the gesture is classified as belonging to the legitimate user, the confidence level for that user increases by 5% (with a limit of 100%). Conversely, if a gesture is classified as an impostor, the confidence level decreases by 10% and can lead to the system being locked if it falls below 30%. In this scenario, unlocking the device requires the use of a traditional authentication mechanism, such as a password, and the system's confidence level is reset to its predefined starting value (i.e., 60%).

The experiments with the "simple" mode or with the "confidence level" mode are divided into two distinct scenarios. In the first one, balanced datasets are used, covering numbers of "swipes" ranging from 50, 100, 250, 500, 1000, 2000, to 3000. In the second scenario, unbalanced datasets are used, exploring various scenarios with numbers of swipes equal to or greater than 10, 20, 30, 40, 50, 60, 70, 80, 90, and 100. All these experimental scenarios are conducted using the three datasets "Focus", "Mathisis", and "Mathisis&Focus".

**Table 3** Results of experiments using the different classifiers

| Model | Confidence level | | | | | | Simple | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Balanced | | | Unbalanced | | | Balanced | | | Unbalanced | | |
| | M | F | M&F | M | F | M&F | M | F | M&F | M | F | M&F |
| OCSVM | 21.83 | 23.33 | 24.39 | 31.77 | 24.16 | 26.03 | 50.00 | 50.00 | 50.00 | 50.00 | 50.00 | 50.00 |
| OCGMM | 20.00 | 16.00 | 12.00 | 14.63 | 12.00 | 11.54 | 50.00 | 50.00 | 48.00 | 50.00 | 48.00 | 50.00 |
| OCIF | 37.80 | 36.20 | 39.84 | 40.63 | 42.87 | 45.14 | 50.00 | 50.00 | 50.00 | 50.00 | 50.00 | 50.00 |
| OCKNN | 16.00 | 14.00 | 16.00 | 11.11 | 14.8 | 33.33 | 50.00 | 50.00 | 50.00 | 44.44 | 48.64 | 33.33 |
| A-E | 08.75 | 05.50 | 03.50 | 03.50 | 00.21 | 00.69 | 16.25 | 06.50 | 04.50 | 08.25 | 00.20 | 03.00 |

Figure 5 illustrates the various scenarios that we will use to train the models and to perform result comparisons. Finally, to determine the reliability of the prediction, each model measures the distance between the sample and the hyperplane established by the model.

## 4 Experimental results

In this section, the results of traditional Machine learning classifiers (i.e., OCSVM, OCGMM, OCIF and OCKNN) and those of the auto-encoder model will be presented separately, and then they will be compared during our discussion.

The Table 3 presents results of experiments using different the classifiers across different conditions: Balanced and Unbalanced datasets, and for swipes categorized as M (Mathis), F (Focus), and M&F (Mathis and Focus combined).

Based on the results presented for the traditional ML classifiers, several trends and performances can be observed. The OCSVM classifier shows improved Equal Error Rates (EERs) in the balanced data scenario, particularly with 3000 swipe movements, achieving significant reductions in EERs when the confidence level is utilized compared to sessions without it. This trend holds similarly in the unbalanced data scenario with datasets containing 70 or more swipe movements.

Conversely, the OCGMM classifier demonstrates varying success across balanced and unbalanced datasets. In the balanced scenario with 250 swipe movements, utilizing the confidence level yields EERs of 20% for "Mathisis", 16% for "Focus", and 12% for "Mathisis&Focus". However, excluding the confidence level results in higher EERs of 50%. In unbalanced data, promising results are achieved with datasets of 30 or more swipe movements, showing EERs of 14.63% for "Mathisis", 12% for "Focus", and 11.54% for "Mathisis&Focus". The performance remains comparable across balanced and unbalanced datasets.

In contrast, the OCIF classifier displays less favorable results overall, with EERs ranging between 37% and 45% when using the confidence level, and consistently at 50% when the confidence level is excluded, across both balanced and unbalanced datasets.

Lastly, the OCKNN classifier achieves EERs of 16% for "Mathisis", 14% for "Focus", and 16% for "Mathisis&Focus" in the balanced scenario with 250 swipe movements when using the confidence level. In unbalanced data scenarios with 20 or more swipe movements, the EERs increase to 11.11% for "Mathisis", 14.86% for "Focus", and 33.33% for "Mathisis&Focus". Excluding the confidence level generally leads to higher EERs approaching 50%.

For the auto-encoder model, it represents a baseline with generally lower ERR values, indicating better performance compared to other classifiers in all cases. A good value of ERR equal to 0.20% is achieved using this model. We believe that this model achieves this notable success because it can reduce the dimensionality of swipe data while preserving essential features, thereby enhancing the discriminative ability for authentication purposes.

We can conclude that traditional ML classifiers achieve good results only when the confidence level is applied, especially with "Mathisis&Focus" data, as they encompass both horizontal and vertical movements. However, the auto-encoder model performs great in all scenarios of test, especially using the confidence level.

To further improve results, we believe that testing new extracted features can improve performance as well. To prove that, and conclude our experimentation, new features, namely "traveled distance (DT)" and "covered area (CA)" (Table 2), will be used by the system based on using the auto-encoder model in the scenario of confidence level and unbalanced dataset. We can clearly see in Fig. 6 that the Equal Error Rate (EER) decreases from 0.69% to 0.41% when adding the two new features. Therefore, we can say that the use of new features, or maybe also removing others of Table 2, will yield to better results.

## 5 Conclusion

In this paper, we conducted a comprehensive evaluation of continuous verification through swiping gestures on mobile

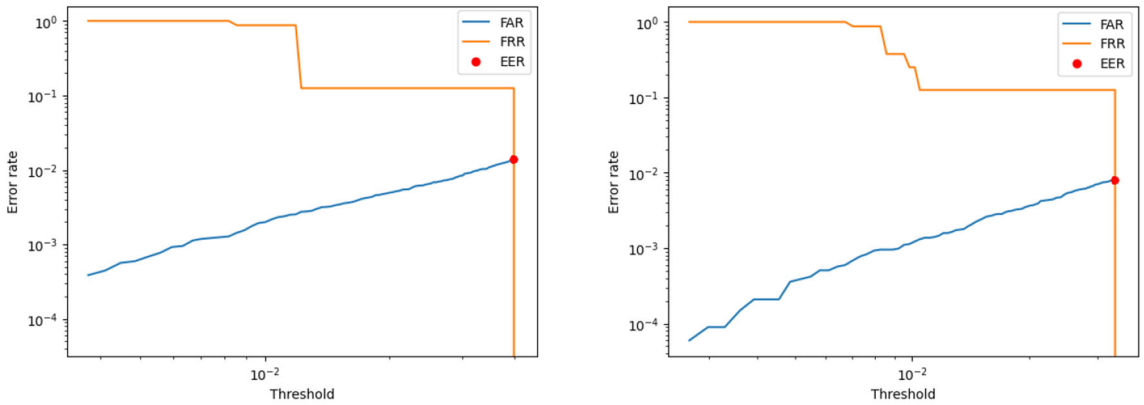


**Fig. 6** Visualizing the sample results after changing the features using Auto-Encoder. **a** FAR and FRR curves using old features. **b** FAR and FRR curves using new features

devices, using various one-class classifiers and the Auto-Encoder model. Our experiments involved both balanced and unbalanced datasets, with different numbers of swipe movements. The best results are achieved using the auto-encoder model in all scenarios of test.

The achieved results in the paper lead to several promising directions for our future research. First, The use of Deep Learning models, confidence levels and balanced data scenarios have proven to enhance system performance. Second, our experimentation proves that the use of new features, such as "Distance Travelled" and "Covered Area," can further improve the accuracy of the classifiers. Finally, combining swiping gestures with other biometric modalities, such as fingerprint recognition or facial recognition, for dynamic verification, could enhance security and accuracy.

**Author Contributions** All authors have participate equally in the elaboration of this work.

**Data availability** The used models can be downloaded from this link: https://github.com/AnassSej/Dynamic-Authentication-Swipes/.

## Declarations

**Conflict of interest** The authors declare no Conflict of interest.

## References

1. Jain, A., Flynn, P., Ross, A.: Handbook of biometrics. Springer, NY (2008)
2. Frank, M., Biedert, R., Ma, E., Martinovic, I., Song, D.: Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans. Info. Forensics Secur. **8**(1), 136–148 (2013). https://doi.org/10.1109/TIFS.2012.2225048
3. Davydenko, S., Kostyuchenko, E., Novikov, S.: Evaluation of the informativeness of features in datasets for continuous verification. Info. Autom. **23**, 65–100 (2024). https://doi.org/10.15622/ia.23.1.3
4. Chao, J., Hossain, M.S., Lancor, L.: Swipe gestures for user authentication in smartphones. J. Info. Secur. Appl. **74**, 103–450 (2023). https://doi.org/10.1016/j.jisa.2023.103450
5. Meddad, M., Moujahdi, C., Mikram, M., Rziza, M.: Convolutional Siamese neural network for few-shot multi-view face identification. Signal Image Video Process. **17**, 1–10 (2023). https://doi.org/10.1007/s11760-023-02535-w
6. Papamichail, M.D., Chatzidimitriou, K.C., Karanikiotis, T., Oikonomou, N.-C.I., Symeonidis, A.L., Saripalle, S.K.: Brainrun: a behavioral biometrics dataset towards continuous implicit authentication. Data **4**(2), 60 (2019). https://doi.org/10.3390/data4020060
7. Mondal, S., Bours, P.: Swipe gesture based continuous authentication for mobile devices. In: 2015 International conference on biometrics (ICB), pp. 458–465 (2015). https://doi.org/10.1109/ICB.2015.7139110
8. Watanabe, Y., Kun, L.: Long-term influence of user identification based on touch operation on smart phone. Proced. Comput. Sci. **112**, 2529–2536 (2017). https://doi.org/10.1016/j.procs.2017.08.196
9. Fenu, G., Marras, M., Boratto, L.: A multi-biometric system for continuous student authentication in e-learning platforms. Pattern Recognit. Lett. **113**, 83–92 (2018). https://doi.org/10.1016/j.patrec.2017.03.027. (**Integrating Biometrics and Forensics**)
10. Karanikiotis, T., Papamichail, M.D., Chatzidimitriou, K.C., Oikonomou, N.-C.I., Symeonidis, A.L., Saripalle, S.K.: Continuous implicit authentication through touch traces modelling. In: 2020 IEEE 20th International conference on software quality, reliability and security (QRS), pp. 111–120 (2020)
11. Al-Saraireh, J., AlJa'afreh, M.R.: Keystroke and swipe biometrics fusion to enhance smartphones authentication. Comput. Secur. **125**, 103022 (2023)
12. Volaka, H.C., Alptekin, G., Basar, O.E., Isbilen, M., Incel, O.D.: Towards continuous authentication on mobile phones using deep learning models. Proced. Comput. Sci. **155**, 177–184 (2019). https://doi.org/10.1016/j.procs.2019.08.027
13. Stylios, I., Chatzis, S., Thanou, O., Kokolakis, S.: Continuous authentication with feature-level fusion of touch gestures and keystroke dynamics to solve security and usability issues. Comput. Secur. **132**, 103–363 (2023). https://doi.org/10.1016/j.cose.2023.103363
14. Naji, Z., Bouzidi, D.: Deep learning approach for a dynamic swipe gestures based continuous authentication. In: The 3rd Interna-

tional conference on artificial intelligence and computer vision (AICV2023), pp. 48–57 (2023). https://doi.org/10.1007/978-3-031-27762-7_5
15. Lahmidi, A., Moujahdi, C., Minaoui, K., Rziza, M.: On the methodology of fingerprint template protection schemes conception: meditations on the reliability. EURASIP J. Info. Secur. **2022**, 3 (2022). https://doi.org/10.1186/s13635-022-00129-6
16. Zheng, Y., Wang, S., Chen, B.: Multikernel correntropy based robust least squares one-class support vector machine. Neurocomputing **545**, 126–324 (2023). https://doi.org/10.1016/j.neucom.2023.126324
17. Paalanen, P., Kamarainen, J.-K., Ilonen, J., Kälviäinen, H.: Feature representation and discrimination based on gaussian mixture model probability densities-practices and algorithms. Pattern Recognit. **39**(7), 1346–1358 (2006). https://doi.org/10.1016/j.patcog.2006.01.005
18. Alonso-Sarria, F., Valdivieso-Ros, C., Gomariz-Castillo, F.: Isolation forests to evaluate class separability and the representativeness of training and validation areas in land cover classification. Remote Sens. **11**(24), 3000 (2019). https://doi.org/10.3390/rs11243000
19. Sarmadi, H., Karamodin, A.: A novel anomaly detection method based on adaptive Mahalanobis-squared distance and one-class kNN rule for structural health monitoring under environmental effects. Mech. Syst. Signal Process. **140**, 106–495 (2020). https://doi.org/10.1016/j.ymssp.2019.106495
20. Hou, B., Yan, R.: Convolutional autoencoder model for finger-vein verification. IEEE Trans. Instrum. Meas. **69**(5), 2067–2074 (2020). https://doi.org/10.1109/TIM.2019.2921135