Journal of Ambient Intelligence and Humanized Computing (2019) 10:4417–4430
https://doi.org/10.1007/s12652-018-1123-6

ORIGINAL RESEARCH

A continuous smartphone authentication method based on gait patterns and keystroke dynamics

Imane Lamiche[1] · Guo Bin[1] · Yao Jing[1] · Zhiwen Yu[1] · Abdenour Hadid[2]

Received: 18 June 2018 / Accepted: 1 November 2018 / Published online: 9 November 2018

Abstract
Behavioral biometrics, such as gait patterns and keystroke dynamics, have been becoming increasingly used in human identity recognition research for enhancing the smartphone security. A new multimodal authentication method able to strengthen the smartphone authentication system is proposed in this paper. The proposed mechanism acquires gait patterns from the accelerometer, as well as keystroke dynamics, continuously without user intervention through simultaneous walk and text input. More specifically, features are extracted from both modalities. Afterward, a feature level fusion method is applied to build a multimodal biometrics profile for the user. Fused feature vectors are subjected to the sequential floating forward selection algorithm to reduce their dimensions as well as the computational complexity. The effectiveness of the proposed method is examined through a real multimodal dataset collected from 20 subjects under various scenarios, using different machine learning classifiers. The experimental results achieved a promising accuracy of 99.11% when using multilayer perceptron classifier with the average false acceptance rate, false rejection rate and equal error rate values of 0.684%, 7%, and 1%, respectively. Furthermore, the security strength of the proposed method was evaluated against two types of attacks, the zero-effort attack and minimal-effort mimicking attack. Results demonstrate that our approach represents a robust and secure authentication solution.

Keyword Continuous authentication · Behavioral biometrics · Gait analysis · Keystroke dynamics · Smartphone sensing

1 Introduction

The prevalence of smartphones has rapidly increased due to their improved interactive features and sensing capabilities. People have come to rely on their smartphones to accomplish various tasks in their lives. With increasing smartphone dependence, increasing security measures has become an urgent need. Some of the most commonly addressed mobile security features are authentication mechanisms, traditionally including explicit methods such as the personal identification number (PIN), patterns, and passwords. However, all of these are single-time authentication methods that require active user participation which causes inconvenience to the user. Moreover, these types of authentications are easy to breach and could be effortlessly hacked by an attacker, including through shoulder surfing (Zakaria et al. 2011) and smudge attacks (Aviv et al. 2010). Recently, researchers have proposed new biometric authentication methods using built-in smartphone sensors such as accelerometers and gyroscopes. Currently proposed mechanisms have had greater reliance on the user's physiological and behavioral characteristics. Physiological authentication mechanisms are related to the user's body characteristics, such as their fingerprints, facial features or retina images. Unfortunately, physiological biometric-based authentication mechanisms are considered one-time authentication methods. The performances of these solutions are heavily influenced by external

✉ Guo Bin
guob@nwpu.edu.cn

Imane Lamiche
stic0303@gmail.com

Yao Jing
1191479758@qq.com

Zhiwen Yu
zhiwenyu@nwpu.edu.cn

Abdenour Hadid
hadidab@hotmail.com

[1] Northwestern Polytechnical University, 127 YouYi XiLu, Xi'an 710072, Shaanxi, China

[2] University of Oulu, Pentti Kaiteran katu 1, 90570 Oulu, Finland

factors. Also, these methods require specialized equipment to perform biometric scanning (Salem et al. 2016), whereas behavioral authentication methods are based on user behavior with the smartphone during everyday use, such as their touchscreen interaction (Frank et al. 2013; Kambourakis et al. 2016), gait (Damaševičius et al. 2016; Hoang et al. 2013), hand motions (Sitová et al. 2016) and so on. This type of authentication adapts to identify features of the user's behavior that do not vary over a period of time (Alzubaidi and Kalita 2016). The behavioral authentication mechanisms continuously authenticate the user without his/her intervention. Moreover, no additional hardware is required to identify the smartphone's owner. However, the majority of preexisting authentication methods use single behavioral biometrics which suffer from low accuracy and have not achieved performance good enough to allow real-world implementation (Do et al. 2014). Therefore, multimodal biometrics have been adopted in recent academic research to enhance authentication system performance. (Akhtar et al. 2017; Galdi et al. 2016).

From the above, it is evident that there is a crucial need for multimodal authentication mechanisms that continuously authenticate the smartphone user without his/her intervention. By leveraging the capacities of today's multi-sensor smartphones, sensor inputs such as gait signals and keystroke dynamics are used as sources of user authentication which can be gathered without user awareness. Most people are used to walk and perform routine behaviors in which texting while walking is most common to do. Using data acquired from the built-in smartphone sensors during simultaneous walking and typing enable to build accurate behavioral patterns for the user. As detailed in Sect. 2, academic research has demonstrated that keystroke dynamics and gait patterns are unique for each user. These two modalities are widely used in smartphone authentication studies, and most of this research uses keystrokes and gait as a single behavioral biometric or in combination with other biometrics. However, none of the existing research actually combines these two biometrics to built a user profile for authentication purposes through using a real multimodal dataset, which is the main contribution of our work.

This paper makes use of gait patterns and keystroke dynamics to build a new multimodal authentication method. The proposed method continuously acquires the user's gait signal with keystroke dynamics during simultaneous walking and text input, by using the smartphone's built-in sensors without explicitly seeking user cooperation. Moreover, to reduce the impact of continuous sensing on battery life, the proposed mechanism only uses the accelerometer sensor to measure acceleration during movement, which is considered to be the most efficient sensor in terms of energy consumption. To demonstrate the efficacy of the proposed mechanism, a real multimodal dataset of keystroke dynamics and gait patterns has been collected from 20 volunteers through various scenarios. The results obtained from the experiments show that the proposed authentication method is able to enhance the smartphone's security.

The rest of this paper is organized as follows. Section 2 addresses the related works. Section 3 describes the proposed framework architecture, Sect. 4 details the proposed authentication method. Section 5 reports the experimental results. Section 6 discusses the usability of the approach. Finally, we conclude this paper and outline further directions for this work in Sect. 7.

2 Related works

Already several studies on gait patterns and keystroke dynamics have been adopted within the field of continuous authentication. In this section, we categorize them as follows.

2.1 Gait patterns-based authentication solutions

Gait modality had received considerable attention in previous works through the proposals of different gait pattern authentication methods using accelerometer sensors for user identity recognition. Earlier studies (Derawi et al. 2010; Mantyjarvi et al. 2005) demonstrated that gait signal acquired with three-dimensional accelerometers could be used to identify mobile phone users. Unlike previous work, (Hoang et al. 2013) proposed a new gait authentication mechanism regardless installation error using both the built-in accelerometer and magnetometer, where a novel segmentation algorithm was used to segment the signal into separate gait cycles. An experiment with the participation of 38 volunteers achieved approximately 94.93% accuracy under identification mode, also a false match rate (FMR), false non-match rate (FNMR) of 0%, 3.89% and a processing time of less than 4 s under authentication mode. Later, (Choi et al. 2014) proposed a set of new gait signature metrics for recognizing different walking patterns in human gait that could efficiently extract distinctive gait characteristics and identify an individual from a list of subjects. Recently, (Zhang et al. 2015) introduced an accelerometer-based gait recognition method to avoid cycle detection failures and inter-cycle phase misalignment issues where it combined the multi-scale signature points (SP) extraction method, an SP sparse encoding scheme with implicit consideration of the phase propinquity, and the classifier for sparse-code collection (CSCC) for recognizing feature collection. The results from this methodology achieved an accuracy of 95.8% for identification, and the equal error rate (EER) of 2.2% for verification. (Zhong et al. 2015) proposed a new pace independent mobile gait biometric algorithm to address

the challenges of varying walking speed and sensor rotation. The performance analysis of the algorithm on a realistic mobile gait dataset, which contained 51 subjects, had achieved an EER of 7.22% with a performance improvement of 37%. In addition to these studies, a number of different methods had been proposed for gait based recognition on mobile devices using various types of features or classification algorithms (Damaševičius et al. 2016; Muaaz and Mayrhofer 2013, 2014; Zhao and Zhou 2017).

2.2 Keystroke dynamics based authentication solutions

The application of keystroke dynamics for continuous authentication is not entirely new, as it is derived from research on authenticating computer access (Brown and Rogers 1993; Gunetti and Picardi 2005; Monrose and Rubin 2000). With the new interactive features of present-day touchscreen-equipped smartphones, typing behavior has become easier to extract from smartphone virtual keyboards with additional features such as pressure and the finger area. (Antal et al. 2015) examined the effect of these additional touchscreen features in identification and verification performance, it was concluded that the addition of these feature sets enhances the accuracy of both processes. Whereas (Buschek et al. 2015) proved that including spatial touch features reduces implicit authentication EER by 26.4–36.8% relative to the previously used temporal features. Keystroke dynamics are also used in Multi-factor authentication methods to strengthen user authentication on smartphones, where (Salem et al. 2016) proposed a user verification and identification system on touchscreen mobile devices, using keystroke dynamics as a second authentication factor with a password, The model achieved false acceptance rate (FAR) of 2.2%, false rejection rate (FRR) of 8.67%, and an EER of 5.43% and proved that keystroke dynamics provide an acceptable level of performance measures as a second authentication factor. (Kambourakis et al. 2016) proposed two-factor touch stroke user authentication method to discriminate between the legitimate user and intruders, the achieved experimental results of 20 participants showed that touch stroking has significant potential in designing enhanced authentication systems for smartphone devices. For investigating the effectiveness of sensor-enhanced keystroke dynamics, (Stanciu et al. 2016) implemented a statistical attack against sensor enhanced keystroke dynamics and evaluated its impact on detection accuracy. The results showed that sensor-enhanced keystroke dynamics are generally robust against statistical attacks with a marginal EER impact ($<0.14\%$). Moreover, several other research studies using different authentication algorithms and classification features also achieved promising results in continuous smartphone authentication based on keystroke dynamics (Alsultan et al. 2016; Antal and Szabó 2015; Bours and Mondal 2015; Kang and Cho 2015).

2.3 Gait patterns and keystroke dynamics in multimodal based authentication solutions

The majority of the aforementioned works on authentication use gait patterns or keystroke dynamics as a single behavioral biometric to recognize the user identity. Despite having many inherent advantages, there are numerous challenges such as the susceptibility of the biometric sensor to outside factors, the changing emotional or physical state of the user or poor data acquisition. To overcome these limitations, research has moved from unimodal biometrics to multimodal biometrics to increase authentication performance. In (Saevanee et al. 2012), keystroke dynamics were used with behavioral and linguistic profiling to discriminate users, where matching-level fusion methods were applied to study the feasibility of the proposed system. The results showed that matching-level fusion could improve classification performance with an overall EER of 8%. Later, (Crawford and Renaud 2014; Crawford et al. 2013) combined keystroke dynamics and voice recognition for mobile systems to identify the device owner, the initial results showed that the described transparent authentication framework is effective in increasing both usability and security. Furthermore, (Damer et al. 2016) introduced a multi-biometric continuous authentication solution that includes information from the face images and the keystroke dynamics of the user. Whereas, most of the existing studies based on gait patterns for multimodal authentication use video-cameras from a distance to capture gait coupled with face recognition (Almohammad et al. 2012; Guan et al. 2013; Hofmann et al. 2012; Hossain and Chetty 2011; Nanda et al. 2017; Xing et al. 2015), or body-worn motion recording sensors (Tao et al. 2018), such the work in (Vildjiounaite et al. 2006) where gait patterns had been combined with voice recognition for user authentication. The only related study within our scope of research is by (Do et al. 2014), which combined gait biometrics acquired by use of the smartphone's built-in accelerometer and magnetometer sensors with keystroke dynamics. A virtual dataset was created by fusion gait and keystroke dynamics where fusion operated at both the feature extraction level and the matching score level. The proposed methodology achieved a recognition rate of approximately 97.86% under identification mode and an EER approximately 1.11% under authentication mode.

3 The system framework

Figure 1 represents the proposed framework architecture. Specifically, the proposed framework is divided into two phases: enrolment and authentication.

-Enrolment phase: initiated by the text input and walking of the user, the system acquires gait signals and keystroke

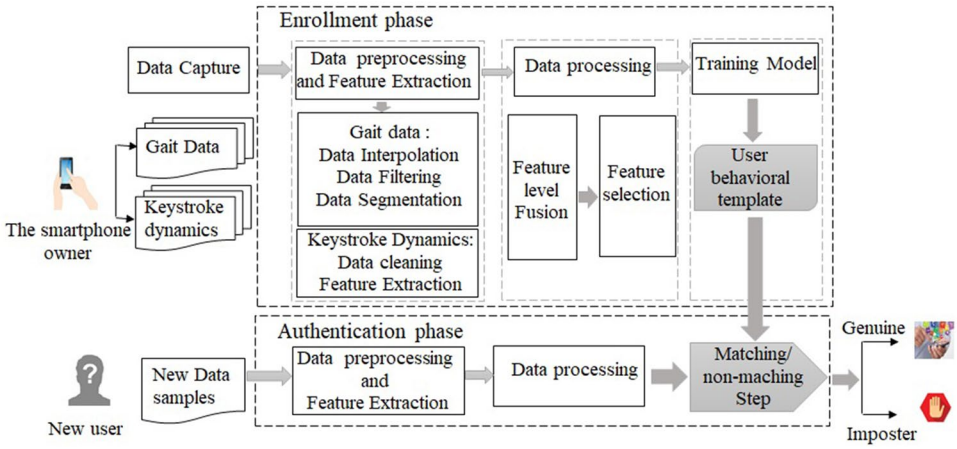


Fig. 1 The proposed smartphone user authentication framework

dynamics from the built-in smartphone sensors. The collected biometrics are first separately preprocessed and analyzed to extract features. Then the extracted features are processed to get the final data that will be used to built the behavioral profile template of the user.

-Authentication phase: the system autonomously collects the new sensor samples through any attempt to manipulate the smartphone, and compare them with the stored template. The user is only authorized to access to the smartphone services upon a successful match, otherwise, the user is classified as an imposter.

A detailed description of the authentication process will be explained in the following sections.

4 The methodology

4.1 Data acquisition

Many dataset resources containing several unimodal biometrics have been accessible for the academic research, however, no realistic multimodal dataset based gait and keystroke dynamics is available. In this paper, we collected a real multimodal dataset from 20 subjects with a balanced gender distribution, aged 22–33 years old, using the Xiaomi 2S mobile phone with the Android version (5.0.2). For the data collection task, we developed a customized Android application with a virtual keyboard for accelerometer and keystroke data collection (see Fig. 2). The application collects three-dimensional accelerometer data (X, Y, and Z axis) when the smartphone user is walking, with the user's input rhythm at the same time. As it is known, the default android keyboard is allowed to only collect pressed key IDs. As detailed in Sect. 5, more features like the pressure and the size of touch area are required in our work to construct the behavioral profile template of the user. Hence, a virtual keyboard was designed using MotionEvent and Gesture classes provided by Android SDK (Software Development Kit) and used instead of the default keyboard in the settings of the device so that additional keystroke features could be collected from all types of applications that required typing.

To evaluate the effectiveness of the proposed method, a real dataset is constructed under realistic acquisition scenarios, based on how users interact with their smartphones during their routine activities. In this paper, data is collected from each participant using the following four scenarios:

- In the first scenario, the participants were asked to put the smartphone into their trouser pocket and walk as naturally as possible in a straight corridor.
- In the second scenario, the participants were asked to hold the smartphone freely in hand and walk.
- In the third scenario, the participants were asked to answer a call while walking.
- In the last scenario, the participants were asked to walk in their usual manner and type the following phrase "*the quick brown fox jumped over the lazy ghost*." which contains every letter of the alphabet, spaces and a period at the end of the sentence to indicate the completion of the typing process. This sentence has come widely known within keystroke analysis and has been adopted by many studies (Kambourakis et al. 2016; Lau et al. 2004). This set text provided a controlled variable to ensure a similar amount of data for all participants.

In this scenario, participants had the choice to use any application that requires typing as long they used the designed keyboard. They also were allowed to make mistakes and use the backspace key for any corrections. It should be mentioned that each scenario had to be repeated five times and that the participants activated the accelerometer when they started walking and stopped it upon their arrival at the end of the corridor.

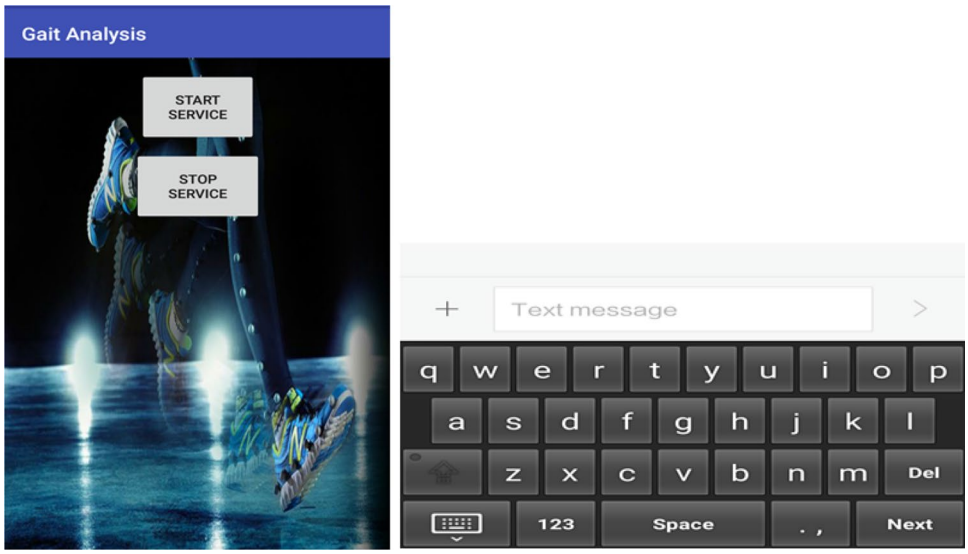


Fig. 2 The proposed application and the keyboard interface used for accelerometer and keystroke data collection

4.2 Gait data pre-processing and feature extraction

4.2.1 Data interpolation

As it is known, only when forces acting on the three axes of the smartphone have considerable change does the accelerometer sensor report output values, which enables low power consumption. Hence, acceleration signals are acquired with variable sampling rate. In our study, the sampling rate of the device is not stable which causes non-constant time interval between two successive samples. Therefore, the acquired signal is resampled to 50 Hz using Linear-interpolation to correct the irregular time interval problem.

4.2.2 Noise elimination

Gait signal acquirement using the built-in accelerometer sensor is sensitive to noise. Mobile accelerometers produce numerous noises as compared with standalone sensors since its functionality is fully governed by the mobile OS layer (Hoang et al. 2013). Therefore, noise must be eliminated to improve the quality of the acquired signal. In our study, first Outliers observations are detected and removed from data, then a FIR low-pass filter with passband cutoff frequency fp = 0.9 Hz designed using MATLAB is applied to the acquired signal. The Low pass filter is the most frequently used because it can implement linear-phase filtering which means that the filter has no phase shift across the frequency band[1].

4.2.3 Segmentation and feature extraction

In this paper, the adopted segmentation method is based on a sliding-window algorithm where sliding-window-based methods are most commonly used in activity recognition studies (Bersch et al. 2014; Niazi et al. 2017; Ravi et al. 2005). The raw data is divided into windows (i.e., segments) with a fixed length of 10 s and 50% overlap. Then a feature extraction method is applied to construct a feature vector that is later fed to the classifier. A combination of features from both time and frequency domains are extracted from four components, as shown in Fig. 3 which represents the accelerometer data reading for two randomly selected users on the X-axis, Y-axis, Z-axis and the magnitude-axis a_{xyz} Where a_{xyz} is defined as:

$$a_{xyz} = \sqrt{a_x^2 + a_y^2 + a_z^2}. \quad (1)$$

Frequency-domain features can be derived from the Fast Fourier Transform (FFT) performed on each window for the four types of acceleration. Multiple statistic features set includes maximum, minimum, mean, median and standard deviation values are derived from each type of acceleration that is mentioned above within each window for both time and frequency domains. We extended this set by adding the following features:

- Average absolute difference

$$MD = avg\left(\left|x_t - \bar{x}\right|\right), \quad (2)$$

where
x_t is the data point in time series of a window.
$\bar{x}$ is the mean.

[1] https://www.minidsp.com/applications/dsp-basics/fir-vs-iir-filtering.

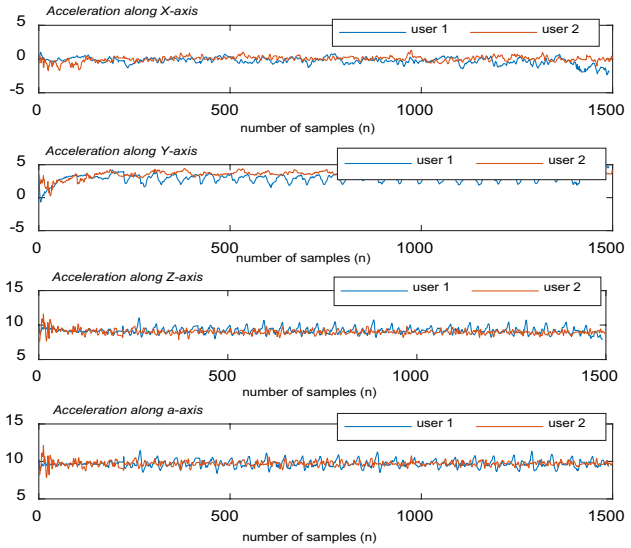


Fig. 3 Example of data samples captured from two randomly selected users

- Spectral Centroid: In this case, spectrum refers to the identification window of acceleration values (Singha et al. 2017). For the four types of acceleration. The spectral centroid of each window is calculated as in following:

$$C = \frac{1}{l}\sum_{k=1}^{l} x_{tk} * f_{tk}/l, \tag{3}$$

where
x_{tk} is the data point in time series of a window
f_{tk} is the data point in frequency series of a window
l length of the window

- Cross-correlation refers to the correlations between the entries of two vectors. In this paper, three types of correlation are calculated.

$Corr_{xy}$ Cross-correlation of x axis and y-axis
$Corr_{xz}$ Cross-correlation of x axis and z-axis
$Corr_{xz}$ Cross-correlation of y axis and z-axis

- Energy: is the normalized summation of absolute values of Discrete Fourier Transform of a windowed signal sequence.
- The first ten FFT coefficients:

$$X_k = \sum_{n=0}^{N-1} x_n e^{-\frac{i2\pi kn}{N}}, \quad k = 0, \ldots 9 \tag{4}$$

- The first ten DCT coefficients:

$$X_k = w_k \sum_{n=1}^{N} x_n \cos^{\frac{\pi(2n-1)(k-1)}{2N}}, \qquad k = 1, ...9$$

where

$$w_k = \begin{cases} \frac{1}{\sqrt{N}} & k = 1 \\ \sqrt{\frac{2}{N}} & 2 \le k \le N \end{cases}. \tag{5}$$

4.3 Keystroke dynamics data pre-processing and feature extraction

Once the keystrokes input data has been collected, data is cleaned by eliminating missing data. Various feature extraction methods are used in keystroke analysis research where the most widely-employed features in keystroke dynamics focus on the timing information such as the moment when the keys are pressed and released. In this work, the following timing features have been extracted:

- Digraphs: which are the time latencies between two successive keystrokes (Zhong and Deng 2015), including dwell time (holding time of a key) and flight time. The following types of latencies are used:
- Down–up (hold time) (DU): is the time interval between pressing and releasing the same key.
- Down–down key latency (DD): is the time interval between a key press and the next key press.
- Up–down key latency (UD): is the time interval between the release of a key and the pressing of the next key.
- Up–up key latency (UU): is the time interval between the release of a key and release of the next key.
- Trigraph: is the interval time between every other successive key press.

In our study, additional non-timing features are extracted from keystroke data, such as

- Pressure: the pressure exerted on the keyboard when the key is pressed.
- Size of the touch area: size of the touch area when the user's finger presses a key.
- Typing speed: the average time to press and release a key.
- Typing error: the number of times the backspace key is pressed.

Table 1 List of the final feature subset

Feature	Description	Info. gain	Feature	Description	Info. gain
MeanDW	Mean dwell time	2.43	dct_x_1	1st dct coefficient of x raw data	1.50
speed	Typing speed	2.43	fft_{xyz}_6	6th fft coefficient of a_{xyz} raw data	1.33
min_x	Minimum acceleration on x-axis	2.03	fft_z_5	5th fft coefficient of z raw data	1.31
max_x	Maximum acceleration on x-axis	2.00	std_size	Standard deviation of touch size	1.22
std_{fftxyz}	Standard deviation of fft a_{xyz} data	1.85	max_{xyz}	Maximum acceleration on a_{xyz} raw data	1.13
$median_{xyz}$	Median of a_{xyz} data	1.72	dct_z_5	5th dct coefficient of z raw data	1.04
mean_pre	Mean of pressure	1.70	fft_y_4	4th fft coefficient of y raw data	0.97
dct_y_1	1st dct coefficient of y raw data	1.64	dct_x_5	5th dct coefficient of x raw data	0.94
min_z	Minimum acceleration on z-axis	1.61	dct_{xyz}_4	4th dct coefficient of a_{xyz} raw data	0.70
meanFT	Mean flight time	1.57	$corr_{xy}$	Cross-correlation of x and y-axis	0.67
fft_x_8	8th fft coefficient of x raw data	1.57	$corr_{xz}$	Cross-correlation of x and z-axis	0.57
std_{fftz}	Standard deviation of fft z raw data	1.53	$corr_{yz}$	Cross-correlation of y and z-axis	0.56

4.4 Fusion method

After preprocessing and analyzing the acquired gait and keystroke dynamics data, the constructed feature vectors are combined to get a final feature vector that will be fed to machine learning classifier to determine if the user is genuine or an imposter. Feature level fusion is believed to be more effective owing to the fact that a feature set contains richer information about the input biometric data than the matching score or the output decision of a classifier (Ross and Jain 2004). A simple feature fusion method is to concatenate various feature vectors to a single feature vector. Let $X = \{x_1, x_2, ..., x_m\}$ and $Y = \{y_1, y_2, ., y_n\}$ represent the gait and keystroke feature vectors respectively, the resultant feature vector Z can be obtained by concatenating the normalized vectors X′ and Y′, then applying feature selection on the fusion feature vector. In this paper, the concatenated feature vector is normalized by applying the Min–Max normalization technique where all values are scaled within the range − 1 to 1.

4.5 Feature selection

The feature selection approaches aims to select a small subset of features that minimize redundancy and maximize relevance to the target such as the class labels in classification (Tang et al. 2014). In this study, Fusion of gait and keystroke vectors through concatenation produces a feature vector with a large dimension leading to increasing complexity of the classifier. Therefore, the sequential floating forward selection (SFFS) Algorithm (Somol et al. 1999) is applied to perform feature selection on the resultant vector. The SFFS algorithm is an extension of the Sequential Forward Selection (SFS) algorithm where it consists of an additional forward or backward step to remove features once they were included or excluded so that a larger number of feature subset combinations can be sampled. We have used selected features instead of using all features to decrease the training time of the algorithm, taking into consideration the susceptibility of smartphones to memory and computational costs. Although reducing the feature subset into 24 features has decreased the accuracy of the proposed method (0.9%), it is still acceptable when looking at its gains, such as lower memory and processing time costs (the time taken to build a model decreased from 72.478 s to less than 1 s). Table 1 illustrates components of the final feature subset with the information gain of each feature. The dimension of the final feature vector is reduced to 24 features by using SFFS algorithm.

5 Evaluation

5.1 Database description

The data was collected from 20 participants in a single session under a controlled environment using a Xiaomi 2S mobile phone. A total of 63,500 samples from the accelerometer sensor and more than 8600 keystrokes were collected from all participants. After the data preprocessing task, a dataset of 24 features was constructed with a separate file for each user per scenario. In total 80 files were created, where each file contained samples of the genuine user and samples of all the remained 19 users which are considered as impostors. Each data row is composed of the 24 features and the binary representation of the genuine and imposter classes ‘TRUE’ and ‘FALSE’, respectively.

Table 2 Performance of each classifier per scenario

		99% Confidence					
		Acc	EER			Acc	EER
1	SVM	0.9105 0.8918–0.9291	0.4261 0.3937–0.4584	3	SVM	0.94 0.9240–0.9559	0.0191 0.0098–0.0283
	RF	0.9654 0.9534–0.9773	**0.0973** 0.0779–0.1166		RF	0.981 0.9718–0.9901	**0.0334** 0.0213–0.0454
	RT	0.9463 0.9315–0.9610	0.0673 0.0517–0.0846		RT	0.969 0.9573–0.9806	0.0218 0.0119–0.0316
	NB	0.9324 0.9159–0.9488	0.3147 0.2843–0.3450		NB	0.918 0.8995–0.9364	0.4828 0.4491–0.5164
	MLP	0.9304 0.9137–0.9470	0.3663 0.3347–0.3978		MLP	0.9111 0.8919–0.9302	0.2953 0.2646–0.3259
2	SVM	0.9116 0.8904–0.9327	0.4263 0.3894–0.4631	4	SVM	0.9482 0.9355–0.9608	0.2688 0–0.6305
	RF	0.9734 0.9614–0.9853	**0.0682** 0.0494–0.0869		RF	0.9713 0.9641–0.9784	0.0547 0–0.2402
	RT	0.9576 0.9425–0.9726	0.0561 0.0389–0.0732		RT	0.9668 0.9585–0.9750	0.0482 0–0.2229
	NB	0.9263 0.9068–0.9457	0.2834 0.2498–0.3169		NB	0.9818 0.9771–0.9864	0.06 0–0.2537
	MLP	0.9304 0.9114–0.9493	0.331 0.2959–0.3660		MLP	**0.9911** 0.9888–0.9933	**0.01** 0–0.0911

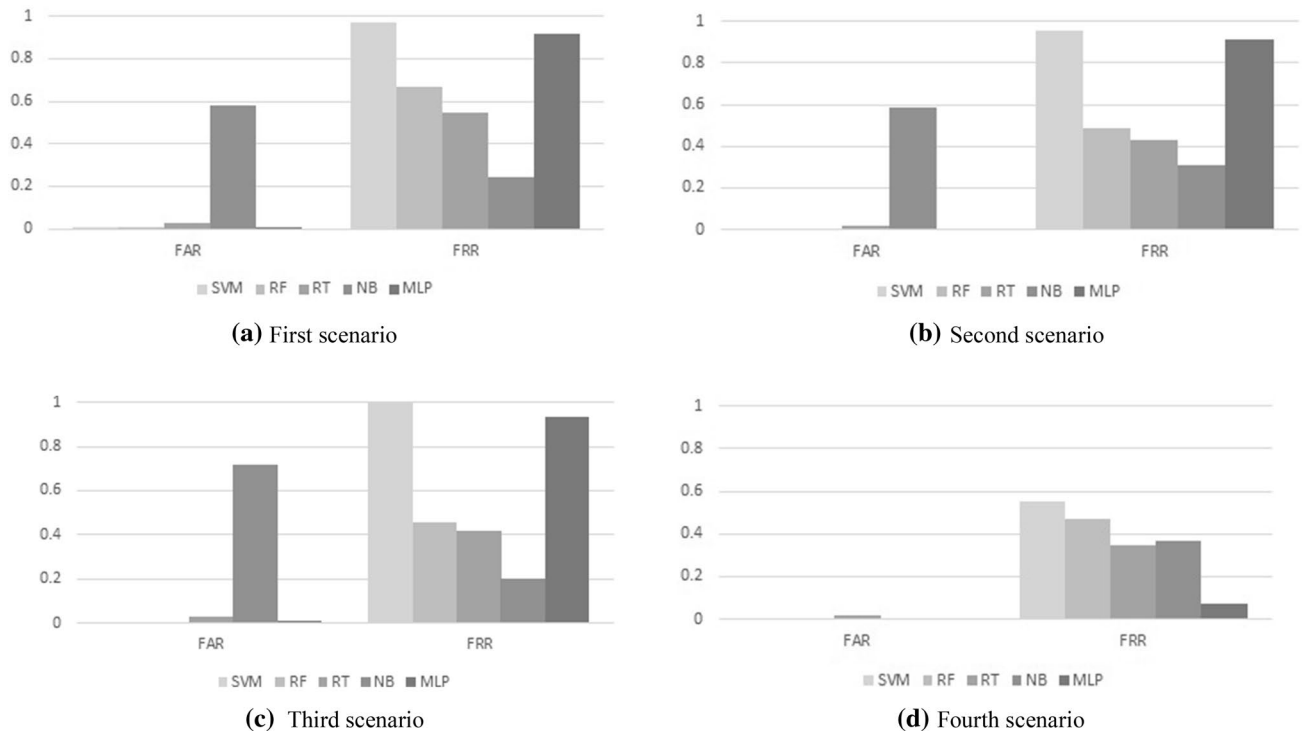
Bold values indicate achieved highest EERs and accuracies for each scenario

5.2 Evaluation of performance

With the aim of selecting the most applicable model for the proposed authentication system, experiments were conducted considering various classifiers. We use 10-fold cross-validation technique to evaluate the performance of the learning models which is based on partitioning the dataset into equally sized folds (groups of instances) where each fold gets the opportunity of appearing in both training and test datasets. Five popular algorithms implemented in Weka (Holmes et al. 1994) are considered in this work: support vector machines (SVM), random forest (RF), random tree (RT), Naïve Bayes (NB) and multilayer perceptron (MLP). To find out how effective are the learning models considered in this study, we used different statistical metrics taking into account that the authentication task is a binary classification problem, in which the system accepts or rejects the user identity. Therefore, we make use of FAR and FRR rates to show the proportion of imposters and authorized users that are incorrectly accepted and rejected, respectively, by the proposed biometric system. In addition to EER rate and accuracy metrics.

Table 2 summarises the experimental results obtained over accuracy and EER metrics across four different scenarios (as detailed in Sect. 4) and Fig. 4 shows the average FAR and FRR values of each classifier per scenario. The obtained results demonstrate the efficiency of the proposed multimodal authentication system using the MLP classifier, which achieved the highest accuracy of 99.11% with the average FAR%, FRR% and EER% values of 0.684, 7 and 1, respectively. The MPL classifier outperforms the NB and RF classifiers which only reached an acceptable accuracy because the FRR is still high. Whereas, SVM and RT achieved the lowest accuracy in comparison with other classifiers with a high FRR as well. This issue is the result of the imbalance between genuine and imposter class data. In order to compare the EER between different scenarios, we performed different test procedures such as Chi square test for testing independence and Marascuilo's test for testing equality of several proportions. As shown in Table 3, the critical value of $\chi 2$ with 12 degrees of freedom is 12.026 (P value < 0.001) which indicates a significant difference of EER values among the results achieved under different scenarios. By applying Marascuillo test, the comparisons including (p1–p3), (p2–p3), (p3–p4) are significantly different from each other where p1, p2, p3, p4 refers to scenario 1, scenario 2, scenario 3, and scenario 4, respectively. Whereas, the differences between the remaining scenarios are not statistically significant.

Moreover, the performance of gait authentication which used all of the extracted features is evaluated from the first three scenarios where participants had been asked to walk while holding the phone during various activities. Acceptable results for the three scenarios, with average EER% values of 9.73, 6.82 and 3.34 respectively, had been obtained when using the RF classifier. To study the effect of the adopted fusion method, we also evaluated the performance of keystroke dynamics separately. Table 4 shows the obtained results.



(a) First scenario **(b)** Second scenario

(c) Third scenario **(d)** Fourth scenario

Fig. 4 The average FAR and FRR values of each classifier per scenario

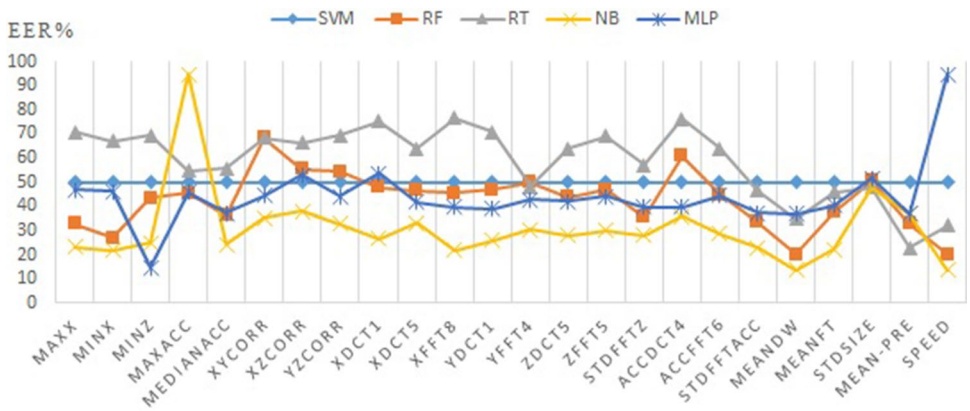


Fig. 5 Multimodal authentication with a single feature

5.3 Identification result

Based on the encouraging results obtained in authentication mode, we conducted an experiment to evaluate the effectiveness of the proposed method under identification mode as well. Table 5 illustrates the experimental results for each classifier. It can easily be observed that the SVM classifier achieved the best results in identification. More specifically, the average accuracy and EER% values are 97.5 and 0 respectively. Our experimental results under both authentication and identification mode, are competitive with the results stated by (Do et al. 2014). Different from their work, we propose an energy efficiency model that requires less sensors reading to authenticate the smartphone user. Moreover, the effectiveness of our proposed model is evaluated using a real multimodal dataset collected under realistic acquisition scenarios. Finally, the effectiveness of each feature of the final selected subset is also examined independently for both authentication and identification mode, Figs. 5 and 6 illustrate the impact of each feature on EER value of the five classification models used in this study.

5.4 Realistic usage scenarios

The smartphone user may utilize his/her device under different conditions, such as stress and fatigue, or on different

Table 3 Significance test of EER

Test		Values
Chi square statistic value		81.56186
Chi square critical value		21.026
P value		< 0.00001
Level of significance		0.05
Statistic value in the Marascuilo procedure	|p1-p2|	0.0308
	|p1-p3|	0.3126
	|p1-p4|	0.2734
	|p2-p3|	0.3435
	|p2-p4|	0.2426
	|p3-p4|	0.5861
Critical value in the Marascuilo procedure	|p1-p2|	0.2805
	|p1-p3|	0.2055
	|p1-p4|	0.3876
	|p2-p3|	0.2174
	|p2-p4|	0.3940
	|p3-p4|	0.3446

Table 4 Performance of keystroke dynamics

	SVM	RF	RT	NB	MLP
Acc	90.68	94.34	94.18	**96.91**	96.66
EER	47.56	**11.47**	15.44	13.94	13.75
Rec	95.10	96.20	94.00	96.15	96.45

Table 5 Performance of the proposed multimodal system under identification mode

	SVM	RF	RT	NB	MLP
Acc	**97.50**	96.50	68.00	90.40	93.30
EER	**0**	0	8.06	0	0
Rec	**97.00**	96.00	65.00	89.00	93.00

types of ground. Therefore, the study also verifies the effectiveness of the proposed method under several walking and typing conditions. To evaluate the efficacy of our approach across a variety of real-life conditions, in the second experiment within our study consisted of only two subjects (1 male, 1 female). The two volunteers were in good health. In this experiment, we address a series of real-life walking and typing conditions: fatigue, walking in high-heel shoes, and walking on different types of ground (flat and level, grassy and uneven forest terrain). Data were collected from participants on two separate days. On the first day, data was gathered from the subjects throughout the day under different levels of fatigue (morning, noonday, evening). On the second day, the two participants were asked to walk and type in three distinct experimental settings, Fig. 7 shows the different types of grounds used in this experiment. Finally, the woman was asked to wear high-heel shoes (100 mm heel height) and type while walking in a straight corridor. In total, 45 iterations were completed by the woman and 40 iterations by the man. Table 6 reports the accuracy and EER values of participants under the aforementioned conditions. Results suggest that the change of user conditions or environmental grounds does not affect the performance of the proposed system. Many research works such as (Ulinskas et al. 2018, 2017) have reported that a person's typing characteristics could be effected by the level of fatigue during the day. We observe that our approach overcomes this issue; by using multimodal traits it is highly unexpected that the system would be affected by the above-mentioned conditions. However, some diseases such as Parkinson's can affect the walking and typing rhythm of the user which leads to a significant change in the characteristics of these two biometrics. In future works, we aim to address this by expanding the number of participants and taking into consideration different health conditions in order to provide even more accurate results.

5.5 Resistance against attacks

From the results of the aforementioned experiments, we validate that multimodal biometric-based gait and keystroke dynamics represent a reliable identifier of the smartphone

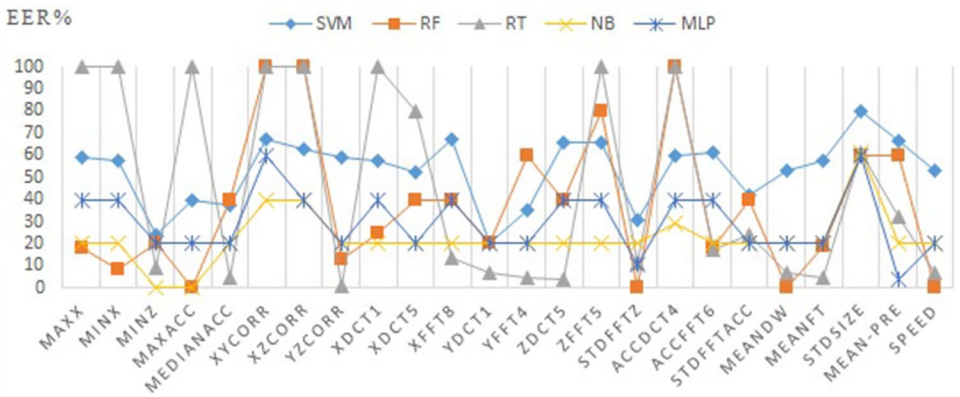


Fig. 6 Multimodal identification with a single feature

(a) Flat ground (Lab experiment) **(b)** Grassy ground **(c)** Uneven forest terrain

Fig. 7 The experimental settings

user. However, walking and typing behaviors can be easily observed and impersonated by an attacker. To evaluate the security strength of the proposed method against various attacks, we designed a real-world experiment which included 10 participants (6 males, 4 females). The participants were randomly selected. Five of them had already participated in the previous experiment, whereas the remaining five were new volunteers without any prior knowledge of the system. In same-gendered pairs, each subject played either the role of an attacker or victim and then exchanged roles with their partners. There were two types of attacks considered in the experiment:

- Zero-effort attack: the attacker has no prior knowledge about the victim's behavior, he randomly tries to type and walk using the victim's smartphone.
- Minimal-effort mimicking attack: the attacker has to observe the victim's behavior before trying to mimic him/her. The attacker was asked to watch the target walking and typing as many times as they wanted, to focus on his/her behaviors, and then to try to mimic him /her by walking side by side.

Before starting the experiment, we first collected data from the victims; they were asked to walk at their usual pace and type using the same sentence provided in the previous experiment (see Sect. 2). Then each attacker was asked to make 20 attempts per attack. Every participant in this experiment executed 20 rounds as a victim and 40 rounds as an attacker, in total, 80×10 trials were done.

To estimate the FAR values, we matched the mimicked gait samples of the attacker to the victim's gait samples, Fig. 8 shows the FAR values of each attacker for the zero-effort attack and minimal-effort attack. An average FAR value of 0.112% for the ten attackers under the zero-effort attack and 0% under the minimal-effort attack. The results demonstrate the resistance of the proposed method against these types of attacks. Moreover, we noted no significant difference between FAR values of the two examined attacks which proved that imitating the target's typing and walking behavior did not give the attacker a higher chance of matching the victim's template.

It should be mentioned that all participants declared it difficult to emulate a target's walking and typing manner at the same time. Focus on behavior impersonation lead to failing to simultaneously remain focused on the second behavior of the target, which validates the hypothesis that multimodal systems generally provide higher levels of security against attacks.

6 Discussion

The evaluation of the proposed method showed a high-security level (99.1% accuracy). The results from our experiment measured the security strength of the smartphone-based gait and keystroke authentication system against zero-effort attacks and minimal-effort mimicking attacks and demonstrated that the proposed system's ability to resist such types

Table 6 Performance of the system under different conditions

	Female		Male	
	Acc	EER	Acc	EER
Different grounds	100%	0%	100%	0%
Different levels of fatigue	100%	0%	100%	0%
Wear high-heel shoes	100%	0%		

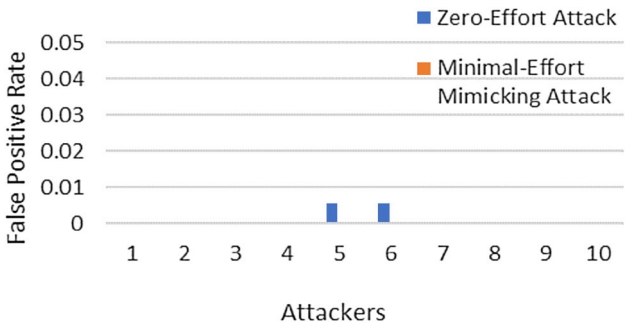


Fig. 8 Performance of the proposed multimodal system against zero-effort attack and minimal effort mimicking attack

of attacks. However, the security level alone cannot measure the success of an authentication system, evaluating usability is also an essential part of the system. Therefore, we developed a study questionnaire containing six questions in a 5-point Likert scale (from strongly agree to strongly disagree, respectively). After completing the data collection task, participants were asked to answer the questions. We first asked the smartphone users whether they preferred to use behavioral authentication methods over the traditional authentication methods, such as passwords and patterns, for smartphone authentication. Of the participants, 86% agreed or strongly agreed that they preferred to use behavioral authentication systems over traditional ones. Afterwards, 92% of participants agreed or strongly agreed that the proposed system was easy to use. Of the users, 68% reported that they often type while walking, whereas 20% of them disagreed which meant it was not convenient for them simultaneously type and walk. The balance between security level, time, and energy consumption was also questioned where 40% of users had declared that it was acceptable for them to decrease the security level of the system to gain lower time and memory consumption whereas 40% of them disagreed or strongly disagreed with having a decrease in the security level. Moreover, 44% of the volunteers agreed or strongly agreed with the continuous sensing's draining impact on the battery life as long as they received a high-security system; however, 28% of them disagreed. Finally, participants were asked about the security of the proposed system. Of participants, 68% of them agreed or strongly agreed that it was difficult to attack the system, while only 8% of users agreed or strongly agreed that the system could be easily attacked. We observed that user preference differs from person to person, where some participants considered security level as the most important criteria in authentication systems whereas the rest preferred not only high levels of security but also convenient and fast systems. Based on this analysis, we can say that the proposed smartphone-based gait and keystroke authentication system might have high acceptance rates by real life users (Fig. 9).

7 Conclusion and future works

Continuous authentication methods based on user behavior have been widely used to enhance smartphone security. In this paper we have proposed a new continuous biometric multimodal authentication system for smartphone users. Our approach is based on analyzing gait signals and keystroke dynamics acquired from built-in smartphone sensors, and then applying a fusion method on the acquired biometrics to build a final profile for user authentication purposes. A series of experiments consisting of various realistic acquisition scenarios was conducted with 20 participating subjects.The achieved results in terms of FAR = 1.68, FRR = 7, EER = 1 and accuracy 99.1% are very promising for further investigation in designing enhanced authentication systems on smartphones. The security strength of the proposed system was investigated against two types of attacks, the zero-effort attack and minimal-effort mimicking attack. Our evaluation shows

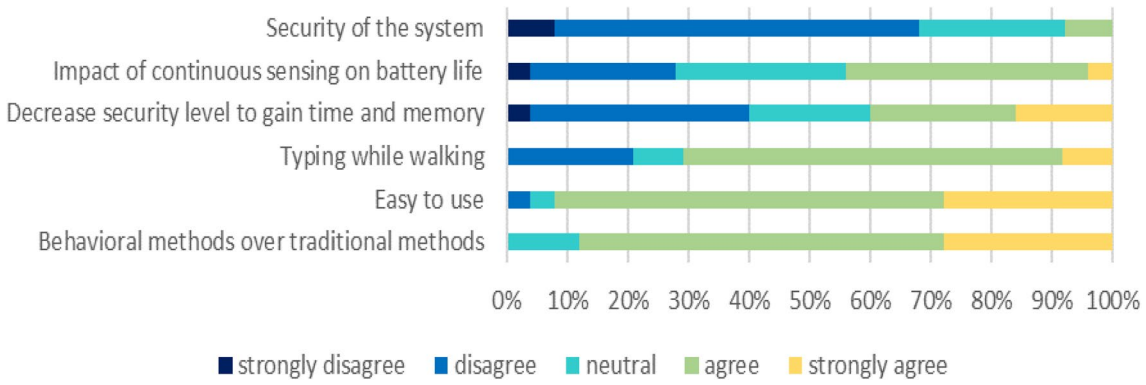


Fig. 9 Preferences of the smartphone users

that the proposed method is robust and secure regardless of the level of knowledge about the target's behavior. While smartphone use does happen in positions beyond those considered in this study (sitting, standing, lying in a bed, etc), this can be addressed by enhancing the system with a seamless activity recognition step to detect the user's current activity and provide the right model based on spotted activity. In future work, we plan (1) to evaluate the performance of the method through expanding the participant base (2) to include more complex scenarios for data collection (3) to apply advanced segmentation methods and extract new features to improve the accuracy of the proposed multimodal biometric system.

Acknowledgements This work was partially supported by the National Key R&D Program of China (2017YFB1001803), and the National Natural Science Foundation of China (nos. 61772428, 61725205).

References

Akhtar Z, Buriro A, Crispo B, Falk TH (2017) Multimodal smartphone user authentication using touchstroke, phone-movement and face patterns. In: Signal and information processing (GlobalSIP), 2017 IEEE Global Conference. IEEE, pp 1368–1372. https://doi.org/10.1109/GlobalSIP.2017.8309185

Almohammad MS, Salama GI, Mahmoud TA (2012) Human identification system based on feature level fusion using face and gait biometrics. In: Engineering and technology (ICET), 2012 international conference. IEEE, pp 1–5. https://doi.org/10.1109/ICEngTechnol.201.6396120

Alsultan A, Warwick K, Wei H (2016) Free-text keystroke dynamics authentication for Arabic language. IET Biometr 5:164–169. https://doi.org/10.1049/iet-bmt.2015.0101

Alzubaidi A, Kalita J (2016) Authentication of smartphone users using behavioral biometrics. IEEE Commun Surv Tutor 18:1998–2026. https://doi.org/10.1109/COMST.2016.2537748

Antal M, Szabó LZ (2015) An evaluation of one-class and two-class classification algorithms for keystroke dynamics authentication on mobile devices. In: Control systems and computer science (CSCS), 2015 20th international conference. IEEE, pp 343–350. https://doi.org/10.1109/CSCS.2015.16

Antal M, Szabó LZ, László I (2015) Keystroke dynamics on android platform. Procedia Technol 19:820–826. https://doi.org/10.1016/j.protcy.2015.02.118

Aviv AJ, Gibson KL, Mossop E, Blaze M, Smith JM (2010) Smudge attacks on smartphone. Touch Screens Woot 10:1–7. https://doi.org/10.1145/1610252.1610287

Bersch SD, Azzi D, Khusainov R, Achumba IE, Ries J (2014) Sensor data acquisition and processing parameters for human activity classification. Sensors 14:4239–4270. https://doi.org/10.3390/s140304239

Bours P, Mondal S (2015) Continuous authentication with keystroke dynamics. Norwegian Information Security Laboratory NISlab 41–58. https://doi.org/10.13140/2.1.2642.5125

Brown M, Rogers SJ (1993) User identification via keystroke characteristics of typed names using neural networks Int J Man Mach Stud 39:999–1014. https://doi.org/10.1006/imms.1993.1092

Buschek D, De Luca A, Alt F (2015) Improving accuracy, applicability and usability of keystroke biometrics on mobile touchscreen devices. In: Proceedings of the 33rd annual ACM conference on human factors in computing systems. ACM, pp 1393–1402. https://doi.org/10.1145/2702123.2702252

Choi S, Youn I-H, LeMay R, Burns S, Youn J-H (2014) Biometric gait recognition based on wireless acceleration sensor using k-nearest neighbor classification. In: Computing, networking and communications (ICNC), 2014 international conference. IEEE, pp 1091–1095. https://doi.org/10.1109/ICCNC.2014.6785491

Crawford H, Renaud K (2014) Understanding user perceptions of transparent authentication on a mobile device. J Trust Manag 1:7. https://doi.org/10.1186/2196-064X-1-7

Crawford H, Renaud K, Storer T (2013) A framework for continuous, transparent mobile device authentication. Comput Secur 39:127–136. https://doi.org/10.1016/j.cose.2013.05.005

Damaševičius R, Maskeliūnas R, Venčkauskas A, Woźniak M (2016) Smartphone user identity verification using gait characteristics. Symmetry 8:100. https://doi.org/10.3390/sym8100100

Damer N, Maul F, Busch C (2016) Multi-biometric continuous authentication: a trust model for an asynchronous system. In: Information fusion (FUSION), 19th international conference. IEEE, pp 2192–2199

Derawi MO, Nickel C, Bours P, Busch C (2010) Unobtrusive user-authentication on mobile phones using biometric gait recognition. In: Intelligent information hiding and multimedia signal processing (IIH-MSP), sixth international conference, IEEE, pp 306–311. https://doi.org/10.1109/IIHMSP.2010.83

Do S, Hoang T, Luong C, Choi S, Lee D, Bang K, Choi D (2014) Using keystroke dynamics for implicit authentication on smartphone. J Korea Multim Soc 17:968–976. https://doi.org/10.9717/kmms.2014.17.8.968

Frank M, Biedert R, Ma E, Martinovic I, Song D (2013) Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans Inf Forens Secur 8:136–148. https://doi.org/10.1109/TIFS.2012.2225048

Galdi C, Nappi M, Dugelay J-L (2016) Multimodal authentication on smartphones: combining iris and sensor recognition for a double check of user identity. Pattern Recogn Lett 82:144–153. https://doi.org/10.1016/j.patrec.2015.09.009

Guan Y, Wei X, Li C-T, Marcialis GL, Roli F, Tistarelli M (2013) Combining gait and face for tackling the elapsed time challenges. In: Biometrics: theory, applications and systems (BTAS), sixth international conference. IEEE, pp 1–8. https://doi.org/10.1109/BTAS.2013.6712749

Gunetti D, Picardi C (2005) Keystroke analysis of free text. ACM Trans Inf Syst Secur (TISSEC) 8:312–347. https://doi.org/10.1145/1085126.1085129

Hoang T, Choi D, Vo V, Nguyen A, Nguyen TA (2013) lightweight gait authentication on mobile phone regardless of installation error. In: IFIP international information security conference, Springer, pp 83–101. https://doi.org/10.1007/978-3-642-39218-4_7

Hofmann M, Schmidt SM, Rajagopalan AN, Rigoll G (2012) Combined face and gait recognition using alpha matte preprocessing. In: Biometrics (ICB), 2012 5th IAPR international conference, IEEE, pp 390–395. https://doi.org/10.1109/ICB.2012.6199782

Holmes G, Donkin A, Witten IH (1994) Weka: a machine learning workbench. In: Intelligent information systems, 1994. In: Proceedings of the 1994 Second Australian and New Zealand Conference. IEEE, pp 357–361. https://doi.org/10.1109/ANZIIS.1994.396988

Hossain E, Chetty G (2011) Multimodal face-gait fusion for biometric person authentication. In: Embedded and ubiquitous computing (EUC), 2011 IFIP 9th international conference. IEEE, pp 332–337. https://doi.org/10.1109/EUC.2011.52

Kambourakis G, Damopoulos D, Papamartzivanos D, Pavlidakis E (2016) Introducing touchstroke: keystroke based authentication system for smartphones. Secur Commun Netw 9:542–554. https://doi.org/10.1002/sec.1061

Kang P, Cho S (2015) Keystroke dynamics-based user authentication using long and free text strings from various input devices. Inf Sci 308:72–93. https://doi.org/10.1016/j.ins.2014.08.070

Lau E, Liu X, Xiao C, Yu X (2004) Enhanced user authentication through keystroke biometrics. Massachusetts Institute of Technology 9

Mantyjarvi J, Lindholm M, Vildjiounaite E, Makela S-M, Ailisto H (2005) Identifying users of portable devices from gait pattern with accelerometers. In: Acoustics, speech, and signal processing, 2005. Proceedings.(ICASSP'05). IEEE international conference. IEEE, pp ii/973–ii/976. Vol. 972. https://doi.org/10.1109/ICASSP.2005.1415569

Monrose F, Rubin AD (2000) Keystroke dynamics as a biometric for authentication. Futur Gen Comput Syst 16:351–359. https://doi.org/10.1016/S0167-739X(99)00059-X

Muaaz M, Mayrhofer R (2013) An analysis of different approaches to gait recognition using cell phone based accelerometers. In: Proceedings of international conference on advances in mobile computing & multimedia, ACM, p 293. https://doi.org/10.1145/2536853.2536895

Muaaz M, Mayrhofer R (2014) Orientation independent cell phone based gait authentication. In: Proceedings of the 12th international conference on advances in mobile computing and multimedia. ACM, pp 161–164. https://doi.org/10.1145/2684103.2684152

Nanda A, Sa PK, Chauhan DS, Majhi B (2017) A person re-identification framework by inlier-set group modeling for video surveillance. J Ambient Intell Human Comput:1–13. https://doi.org/10.1007/s12652-017-0580-7

Niazi AH, Yazdansepas D, Gay JL, Maier FW, Ramaswamy L, Rasheed K, Buman MP (2017) Statistical analysis of window sizes and sampling rates in human activity recognition. In: HEALTHINF, pp 319–325. https://doi.org/10.5220/0006148503190325

Ravi N, Dandekar N, Mysore P, Littman ML (2005) Activity recognition from accelerometer data. In: AAAI, vol 2005. pp 1541–1546

Ross A, Jain AK (2004) Multimodal biometrics: an overview. In: Signal processing conference, 2004 12th European. IEEE, pp 1221–1224

Saevanee H, Clarke NL, Furnell SM (2012) Multi-modal behavioural biometric authentication for mobile devices. In: IFIP international information security conference. Springer, pp 465–474. https://doi.org/10.1007/978-3-642-30436-1_38

Salem A, Zaidan D, Swidan A, Saifan R (2016) Analysis of strong password using keystroke dynamics authentication in touch screen devices. In: Cybersecurity and cyberforensics conference (CCC). IEEE, pp 15–21. https://doi.org/10.1109/CCC.2016.11

Singha TB, Nath RK, Narsimhadhan A (2017) Person Recognition using smartphones' accelerometer data. arXiv:171104689

Sitová Z, Šeděnka J, Yang Q, Peng G, Zhou G, Gasti P, Balagani KS (2016) HMOG: New behavioral biometric features for continuous authentication of smartphone users. IEEE Trans Inf Forens Secur 11:877–892. https://doi.org/10.1109/TIFS.2015.2506542

Somol P, Pudil P, Novovičová J, Paclık P (1999) Adaptive floating search methods in feature selection. Pattern Recognit Lett 20:1157–1163. https://doi.org/10.1016/S0167-8655(99)00083-5

Stanciu V-D, Spolaor R, Conti M, Giuffrida C (2016) On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks. In: Proceedings of the sixth ACM conference on data and application security and privacy. ACM, pp 105–112. https://doi.org/10.1145/2857705.2857748

Tang J, Alelyani S, Liu H (2014) Feature selection for classification: a review. In: Aggarwal C (ed) Data classification: algorithms and applications. CRC Press, Boca Raton, pp 37–64

Tao S, Zhang X, Cai H, Lv Z, Hu C, Xie H (2018) Gait based biometric personal authentication by using MEMS inertial sensors. J Ambient Intell Humaniz Comput:1–8. https://doi.org/10.1007/s12652-018-0880-6

Ulinskas M, Woźniak M, Damaševičius R (2017) Analysis of keystroke dynamics for fatigue recognition. In: International conference on computational science and its applications. Springer, pp 235–247. https://doi.org/10.1007/978-3-319-62404-4_18

Ulinskas M, Damaševičius R, Maskeliūnas R, Woźniak M (2018) Recognition of human daytime fatigue using keystroke data. Procedia Comput Sci 130:947–952. https://doi.org/10.1016/j.procs.2018.04.094

Vildjiounaite E, Mäkelä S-M, Lindholm M, Riihimäki R, Kyllönen V, Mäntyjärvi J, Ailisto H (2006) Unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices. In: International conference on pervasive computing. Springer, pp 187–201. https://doi.org/10.1007/11748625_12

Xing X, Wang K, Lv Z (2015) Fusion of gait and facial features using coupled projections for people identification at a distance. IEEE Signal Process Lett 22:2349–2353. https://doi.org/10.1109/LSP.2015.2481930

Zakaria NH, Griffiths D, Brostoff S, Yan J (2011) Shoulder surfing defence for recall-based graphical passwords. In: Proceedings of the seventh symposium on usable privacy and security. ACM, p 6. https://doi.org/10.1145/2078827.2078835

Zhang Y, Pan G, Jia K, Lu M, Wang Y, Wu Z (2015) Accelerometer-based gait recognition by sparse representation of signature points with clusters. IEEE Trans Cybernet 45:1864–1875. https://doi.org/10.1109/TCYB.2014.2361287

Zhao Y, Zhou S (2017) Wearable device-based gait recognition using angle embedded gait dynamic images and a convolutional neural network. Sensors 17:478. https://doi.org/10.3390/s17030478

Zhong Y, Deng Y (2015) A survey on keystroke dynamics biometrics: approaches, advances, and evaluations. Recent advances in user authentication using keystroke dynamics biometrics Science Gate Publishing:1–22. https://doi.org/15579/gcsr.vol2.ch1

Zhong Y, Deng Y, Meltzner G (2015) Pace independent mobile gait biometrics. In: Biometrics theory, applications and systems (BTAS),7th international conference. IEEE, pp 1–8. https://doi.org/10.1109/BTAS.2015.7358784