An Efficient HOS-Based Gait Authentication of Accelerometer Data

ARTICLE *in* IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY · JULY 2015

Impact Factor: 2.41 · DOI: 10.1109/TIFS.2015.2415753

2 AUTHORS:

Sebastijan Šprager
University of Ljubljana
23 PUBLICATIONS **136** CITATIONS
SEE PROFILE

Matjaz B. Juric
University of Ljubljana
69 PUBLICATIONS **543** CITATIONS
SEE PROFILE

An Efficient HOS-Based Gait Authentication of Accelerometer Data

Sebastijan Sprager, *Member, IEEE*, and Matjaz B. Juric

***Abstract*— We propose a novel efficient and reliable gait authentication approach. It is based on the analysis of accelerometer signals using higher order statistics. Gait patterns are obtained by transformation of acceleration data in feature space represented with higher order cumulants. The proposed approach is able to operate on multichannel and multisensor data by combining feature-level and sensor-level fusion. Evaluation of the proposed approach was performed using the largest currently available data set OU-ISIR containing inertial data of 744 subjects. Authentication was performed by cross-comparison of gallery and probe gait patterns transformed in feature space. In addition, the proposed approach was evaluated using data set collected by McGill University, containing long-sequence acceleration signals of 20 subjects acquired by smartphone during casual walking. The results have shown an average equal error rate of 6% to 12%, depending on the selected experimental parameters and setup. When compared with the latest state of the art, evaluated performance reveal the proposed approach as one of the most efficient and reliable of the currently available accelerometer-based gait authentication approaches.**

***Index Terms*— Gait analysis, gait authentication, inertial sensors, accelerometer, higher-order statistics, higher-order cumulants.**

I. Introduction

MOTION ability is one of the most important human properties, including gait as a basis of human transitional movement [1]. Human gait has significant influence on the quality of life (QoL) and reflects several interesting factors that reveal permanent or temporary characteristics of the individual. Thus, the analysis of human gait became indispensable in several fields of research lately, gaining its popularity with the rapid development of several sensors and devices capable of acquiring movement-related information [2]. These can be divided into three groups with the regards to their installation [2]: floor-based sensors, where motion detecting sensors (i.e. force plate sensors) are installed in the floor [3], video-based sensors, where motion data is captured using a video camera from the distance, including markers for accurate extraction of movement trajectories, and wearable sensors. The latter have become very popular lately, especially due to their positive characteristics, including small size, lightweight, low cost and low power consumption. Such sensors can be attached to the human body or are integrated into the devices that individuals can carry (i.e. smartphones). Interconnectivity of wearable sensors and devices is addressed within Body Area Networks (BAN) [4]. This concept is an important part of the Internet of Things (IoT) paradigm [5], [6] with the main purpose on integrating intelligent devices, technologies and components on several different levels, including data, communication, decision making and application level. It aims to provide complete interconnectivity, interactions and communication between the components regardless to their type or current location. One of the significant steps towards the final goal is to provide an efficient all-level integration of the wearable sensors and devices into cloud systems, which represent computing paradigm of the future [6]. In this context, security represents one of the crucial factors. Considering the fact that gait can be used as a biometric trait, wearable devices supported by services capable of analysing gait could play a significant role in biometric applications. However, several security relevant aspects, including uniqueness, permanence, universality, acceptability, collectability, performance and circumvention, need to be sufficiently addressed in order to establish comprehensive biometric system [7].

Currently, inertial measurement units (IMU) are most popular wearable sensors for gait analysis [8], [9], especially since they are nowadays widely available while embedded in the commercial smart devices. One of the most important parts of the IMU's are accelerometers since they provide instantaneous information on accelerations measured during the movement. It is worth to mention that as of 2009, accelerometers are first inertial sensors that were included as a standard in mobile phones. From this point of view, efficient gait analysis system based solely on inertial data could be offered as a service to large amount of potential users within the expansion of IoT paradigm.

In general, gait analysis is usually performed by cross-comparison of gait patterns collected by sensor data and represented within appropriate feature space. This is carried out by advanced procedures that enable efficient processing and decision making. Their main task is to estimate similarity between gait patterns on which the assessment of intra- or inter-subject gait alterations can be performed. This reveals two different aspects under consideration that each individual has its unique way of walking. The first case indicate several factors affecting subjects gait, i.e. gait-related health issues, heavy terrain, footwear, clothing, etc. while the second case enables gait-based authentication. The use of gait authentication in the field of biometry is one of the most intriguing research topics lately.

Manuscript received November 3, 2014; revised February 4, 2015; accepted March 18, 2015. Date of publication March 23, 2015; date of current version June 2, 2015. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Sviatoslav S. Voloshynovskiy.

The authors are with the Faculty of Computer and Information Science, University of Ljubljana, Ljubljana 1000, Slovenia (e-mail: sebastijan.sprager@fri.uni-lj.si; matjaz.juric@fri.uni-lj.si).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2015.2415753

One of main goals of the research groups dealing with gait-based authentication is to supplement, eventually substitute, but mainly to place novel gait authentication approaches to the side of well-established biometric authentication procedures, including fingerprint, iris or face-based authentication.

Gait-related acceleration data processing corresponds to cyclostationary, non-linear and dynamic systems, making the problem of gait authentication very intriguing. It has already been shown that gait authentication based solely on accelerometer data is feasible. Detailed description of existing work and information on current state-of-the art is given in Section II-A. The common problem of the majority of existing approaches is lack of accuracy, robustness and reliability in terms of performance. In fact, many of these approaches show satisfying accuracy on datasets including small amount of subjects, which decreases significantly when its number increases. Furthermore, addressing some of the crucial security relevant aspects of a gait as a biometric trait [7], namely uniqueness and permanence of such approaches is questionable since experimental protocols are very basic and, consequentially, several factors that affect individuals' gait are not considered in appropriate way.

Thus, main challenge was to develop and evaluate a novel gait authentication approach based on accelerometer data that would be able to cope with these limitations. Considering an interesting fact that the potential of the statistical-based approaches to such problem is fairly unexploited, we propose a novel approach based on higher-order-statistics (HOS). It relies on transformation of acceleration signals into features by employing higher-order cumulants (HOC) and provides an alternative insight into authentication problem in the context within current state-of-the-art. It is also capable to exploit the advantage of multi-channel and multi-sensor accelerometer data leading to additional improvements of its performance by combining feature-level and sensor-level fusion. Performance and reliability of our proposed approach have been evaluated on three experimental datasets covering several factors affecting gait: (a) single-sensor use on large scale dataset, (b) single-sensor location and multi-sensor fusion, and (c) data acquired in realistic scenario. The first two datasets are part of the largest available database of inertial gait signals for biometric purposes including 744 subjects [10]. The third dataset contains long-sequence accelerometer data of 20 subjects acquired in realistic walking scenario using smartphones [11].

The paper is organized as follows. In Section II, current state-of-the-art and methodological background of the proposed approach is explained. Section III details the transformation of accelerometer data into feature space using HOC, while authentication procedure is presented in Section IV. Experimental datasets and parameters are described in Section V. The proposed approach is evaluated in Section VI, security implications are explained in VII while Section VIII concludes this paper.

II. Background

In order to put the presented work in a proper context, the latest and most influential state-of-the-art on accelerometer-based gait authentication is presented in Section II-A. After that, HOS-based signal analysis is introduced in Section II-B for the purpose of accelerometer-based gait authentication.

A. Related Work

In general, existing accelerometer-based gait authentication approaches have common structure revealing the details on two crucial parts that need to be addressed separately: sensor set-up, including sensor type, sensor location and sensor orientation, and methodological properties, consisting of signal segmentation procedure, feature extraction and gait authentication procedure.

Accelerations during gait can be measured by two types of sensors: by accelerometers embedded in special evaluation boards [12]–[16] or by accelerometers integrated in commercial smartphones [11], [17]–[19]. The first are used mainly for experimental purposes and when performing measurements in specific situations since they enable direct control of acquisition parameters, including acceleration range, resolution and sampling frequency. On the other side, the use of the smartphones for accelerometer-based authentication is more reasonable in practice. However, in order to preserve low data stream and power consumption, acceleration signals are acquired by lower and non-constant sampling frequencies, making authentication procedure more challenging.

Usually, gait authentication procedure is based on the shape of gait patterns. Single accelerometer is able to collect single-point motion trajectories with their shape depending on measurement location. Thus, similar gait patterns for the same subject can be ensured only if the sensor is mounted at exactly the same location during all measurements. Furthermore, when selecting the optimal location, it must be considered that some body locations induce motion dynamics during gait onto acceleration signals more efficiently. The researchers experimented with several locations, including conventional locations with firm attachment of the sensor that efficiently collect motion dynamics during gait, such as hip [15], [16], [19], [20] or lower leg [12], [14], and casual locations with loose attachment, typical for real-life scenarios, including bag [21], [22] and pocket [11], [17], [18] as the most convenient locations for carrying smartphones. More advanced experiments were also performed, where data from multiple sensors was acquired simultaneously in order to examine several sensor locations on authentication accuracy [10], [23] while some experiments even allowed users to choose arbitrary location [23].

Accelerometers are also orientation-sensitive. The effect of sensor orientation on the shape of gait patterns can be avoided with fixed orientation achieved by rigid and firm installation of the sensor on the selected location [21], [22]. However, this is impractical for real-life use. Thus, by smartphone-based authentication, where loose installation is allowed, the problem of sensor orientation needs to be addressed. Majority of approaches rely on the acceleration magnitude computed from multichannel acceleration observations using euclidean vector norm and recognition of obtained rotational invariant univariate signal [11], [15]–[18], [23]. However, such approach leads into information loss and, consequentially, into the significant decrease of authentication accuracy [10]. Thus, approaches that rely on multichannel observations currently propose initial calibration prior to walking [19], as well as dynamic compensation of the orientation addressed within authentication step [24].

After accelerometer signal acquisition, proper segmentation must be performed in order to enable fast decisions (i.e. real-time authentication) and to address temporal

variations of gait patterns as a consequence of gait perturbations and several factors affecting gait. Since gait can be represented as a cyclostationary process, cycle based segmentation is proposed in most existing approaches [12], [16]–[19], [22]. It relies on cycle detection step and allows for the analysis of individual gait cycles. Temporal distortion is addressed by signal registration, usually by applying dynamic time warping (DTW) [25]. The drawbacks of cycle-based approaches are their dependency on efficient cycle detection, requirement of additional processing resources and modification of gait pattern morphology. In the contrast with cycle-based approaches, frame-based segmentation is fast and trivial since it splits input acceleration into frames and thus does not require any additional processing. Besides that, it keeps the morphology of gait patterns untouched. It is used in many existing approaches [11], [15], [23], [26]. However, frame-based segmentation does not efficiently address temporal variations of gait patterns and does not control the information on gait phase, leaving this concern to feature extraction or authentication procedure.

Transformation of gait patterns to proper feature space represents one of the most important steps by gait authentication. Authors of existing approaches experimented with variety of different features or their combinations, relying on simple parameters in time domain (mean, variance, skewness, kurtosis and energy of accelerations) [18], [23], parameters in frequency domain (Fourier coefficients [18], spectral entropy [23], cepstral coefficients [15]), discrete cosine transform [18], etc., or introducing more advanced feature representation, such as template cycle computation [17], [20], curve aligning [14], singular spectrum analysis [16], inter-period phase registration [21], [22] or geometric template matching [11].

In general, authentication step can be performed in three different ways: by cross-comparison of gait patterns based on their similarity, determined by distance functions (i.e. euclidean distance [20], DTW distance [17], normalized cross-correlation [24], histogram similarity [26], etc.), by machine learning approaches, where gait authentication is represented as classification problem and can be i.e. applied by nearest neighbours or random forest [11] and hidden Markov models [15], or by model-based authentication [10], [23], where gait models are produced in terms of predefined gait characteristics.

Accelerometer-based gait authentication is dynamic problem with its performance directly depending on variety of factors. An average performance of presented state-of-the-art yields $12.4 \pm 9.1\%$ in terms of equal error rate. The problem is that majority of presented approaches were have been evaluated on datasets including small amount of test subjects only (38 ± 23 subjects in average by presented state-of-the-art) with different experimental set-up and limited experimental protocols. Therefore, the obtained results do not fully reflect the realistic performance of the proposed approaches. It has already been shown that large increase in the number of subjects or authentication in aggravating circumstances lead to significant deterioration of authentication performance [10]. This issue was addressed just recently by appearance of consistent IMU-based biometric datasets, featuring the OU-ISIR dataset [10], currently representing the largest available database, and MCGILL dataset [11] with data collected by smartphone during casual walking. It is also very important that these datasets have already been used for the evaluation of most efficient existing gait authentication approaches. Thus, it is reasonable to compare their performance with the performance of our proposed approach, putting it in a proper context within current state-of-the-art in terms of authentication performance (Section VI).

Proposed HOS-based gait authentication approach reveals many advantages over the existing approaches, including stable performance regardless to the number of subject included in authentication procedure, operability on acceleration signals of arbitrary length considering minimum admissible length that are acquired with low sampling frequency (thus improving the collectability property of the proposed authentication approach), efficient gait authentication evaluated by sensors attached to several body locations with additional improvement of its performance when applying multi-channel and multi-sensor fusion and very promising performance when applying the method on smartphone-based data acquired in real-life scenario (all of these revealing slight contribution in terms of uniqueness and permanence).

B. HOS-Based Signal Processing

HOS are proven successful when dealing with random signal processing. If random signal is Gaussian, then only the first- and second-order statistics have non-zero values. HOS carry additional information of the observed random signal only if it is not Gaussian. In this case, HOS can be used to identify the model that describes the generation process of a random signal. Furthermore, HOS convey amplitude and complete phase information [27]. Hence, HOS represent powerful tool for time series modelling, blind system identification, non-linear signal characterization, classification of non-Gaussian signals and were already used for many applications [27].

Usually, HOS-based signal processing is performed by using cumulants [28]. Cumulants are statistical measures that exhibit some interesting properties [29], especially additivity and symmetry. Cumulant-based analysis of random signals was applied to a wide range of applications lately, especially in the field of biomedical signal processing [30], [31], [32] and image processing [33].

Since there is a high degree of non-linearity and non-Gaussianity present in accelerometer-based gait signals, in order to perform efficient and reliable statistical-based gait authentication, the employment of cumulants for characterization of such signals is reasonable. Preliminary cumulant-based gait authentication attempts were already reported in [19] and [34]. These have revealed very promising potential on the application of cumulants on gait recognition problem, but however, the strength of the proposed methodological approach was fairly unexploited and its evaluation was performed in very limited conditions and on few test subjects only.

To this end, we introduce gait authentication approach which efficiently exploits the properties of higher-order cumulants (HOC) within the feature extraction step in time domain (Section III). The proposed statistical-based approach has some considerable advantages over existing ones since it operates directly on the acceleration signals of arbitrary length having lower bound determined by maximum expected

length of periodic pattern of the observed cyclostationary process. Thus, since it can be directly applied to signal segments having length of maximum expected gait cycle, the proposed approach also preserves advantages of cycle-based approaches, regardless to the fact that it relies on frame-based segmentation. When applicable, the operation on longer segments can lead into additional improvement of the authentication performance, statistically relying on redundant periodical information in gait patterns and thus suppressing noisy and distorted patterns.

III. Feature Extraction

Given a set of labels $i \in \mathcal{I}$ representing I individuals (subjects) participating in measurements and set of labels $t \in \mathcal{T}$ indicating T experiments (measurements) which may consist of different measurement acquisition times (i.e. daily measurements) or different measurement factors (i.e. clothing, footwear, health conditions), compound S-dimensional signal of accelerations is represented as:

$$\mathbf{a}_{i,t}(n) = \left[x_{\beta_1,i,t}(n) \ \ldots \ x_{\beta_S,i,t}(n) \right] \tag{1}$$

where $x_{\beta_s,i,t}(n)$ stands for univariate acceleration signal of sensor set-up β representing either S-channel accelerometer data of single or multiple accelerometers, or their transformed representations (i.e. acceleration magnitude). All signals $x_{\beta_s,i,t}(n)$ are acquired simultaneously by constant delay between consecutive samples $[f_s]^{-1}$, where f_s represents sampling frequency. Segmentation of acceleration signal $\mathbf{a}_{i,t}(n)$ into J vectors $\mathbf{x}^{r,w}_{\beta_s,i,t,j}$ is described by sliding windows:

$$\begin{aligned}\mathbf{A}^{r,w}_{i,t,j} &= \begin{bmatrix} x_{\beta_1,i,t}(jr+1) & \ldots & x_{\beta_S,i,t}(jr+1) \\ x_{\beta_1,i,t}(jr+2) & \ldots & x_{\beta_S,i,t}(jr+2) \\ \vdots & & \vdots \\ x_{\beta_1,i,t}(jr+w) & \ldots & x_{\beta_S,i,t}(jr+w) \end{bmatrix} \\ &= \left[\mathbf{x}^{r,w}_{\beta_1,i,t,j} \quad \ldots \quad \mathbf{x}^{r,w}_{\beta_S,i,t,j} \right], \quad j = 0, 1, \ldots, \left\lfloor \frac{N-w}{r} \right\rfloor \end{aligned} \tag{2}$$

where parameters N, w and r stand for input signal length, window length and window overlap, respectively. The introduction of segmentation with overlapping windows has both experimental and practical background: to examine whether the proposed approach is capable to authenticate gait patterns efficiently irrespective of gait phase within the observed segment and to determine how overlapped segments and their length affect authentication performance. Thus, through the experiments we additionally allow $r \gg w$ for arbitrary selection of window positions and lengths, reasonable for simulation of real-life authentication scenarios, also contributing to the positive characteristics on the collectability of the proposed authentication approach.

Moments are statistical measures that can be used for characterization of random signal properties and are denoted by the following equation:

$$\mathbf{M}^{(k)}_x(l_1, \ldots, l_{k-1}) = \mathbb{E}\left[x^T(n)\, x(n+l_1) \ldots x(n+l_{k-1}) \right] \tag{3}$$

where $x(n)$ stands for random signal, l_i for time lag in i-th dimension and $\mathbb{E}[.]$ for expected value. HOC are derived from the combinations of moments and are more convenient to use in comparison with moments due to their properties referred in Section II-B [35], [36]. Thus, cumulants of k-th order are defined as function of $k-1$ variables [28]:

$$\begin{aligned}\mathbf{C}^{(k)}_x(\mathcal{L}) = \sum_{\bigcup_{p=1}^{q} \mathcal{L}_p = \mathcal{L}} (-1)^{q-1} (q-1)! \prod_{p=1}^{q} \mathbf{M}^{(k)}_x(\mathcal{L}_p), \\ \mathcal{L} = l_1, \ldots, l_{k-1}\end{aligned} \tag{4}$$

where $\bigcup_{p=1}^{q} \mathcal{L}_p = \mathcal{L}$ stands for sum over all partitions of set $\mathcal{L}$ representing time lags. The partitions of $\mathcal{L}$ are defined as unordered group of non-empty sets $\mathcal{L}_p$, such that $\bigcup_p \mathcal{L}_p = \mathcal{L}$. In example, the following partitions are corresponding to cumulant order $k = 4$: $q = 1$ for $\{(1,2,3)\}$, $q = 2$ for $\{(1), (2,3)\}$, $\{(2), (1,3)\}$ and $\{(3), (1,2)\}$, and $q = 3$ for $\{(1), (2), (3)\}$.

When introducing HOC to the problem of accelerometer gait authentication, symmetry as one of their most important properties needs to be considered. Let us examine the symmetrical behavior of HOC in an example of cumulant order $k = 3$. In this case, the domain of support is one of the six-sided regions as shown in Fig. 1b, bounded by thin solid lines l_1, l_2 and $l_1 = l_2$. Thus, we only have to consider the cumulant coefficients contained within one of its non-redundant regions. The principal region is in Fig. 1b denoted as a region bounded by l_1 and $l_1 = l_2$. This property is in the same manner easily extended to the arbitrary order of cumulant k. Thus, non-redundant regions of interest for k-th order cumulants are defined by:

$$\{(l_1, \ldots, l_{k-1}) : 0 \leqslant l_1 \leqslant \ldots \leqslant l_{k-1} \leqslant \infty\} \tag{5}$$

Since accelerometer-based gait signal is represented as cyclostationary process, its transformation into cumulant coefficients results in a repetition property. In Fig. 1b, the repeating six-sided patterns through the domain can easily be noticed. Information on gait patterns is induced in the principal region around the origin (i.e. dashed line in Fig. 1b). Thus, it is reasonable to set the additional constraints on the principal region of interest. The constraint value ℓ should determine maximum expected period of the observed phenomenon. In case of gait authentication it is necessary to cover gait cycle of the maximum expected length, therefore the value of ℓ rely on the physiological properties of gait, i.e. minimum expected gait frequency [37]. In Fig. 1b, the region of interest constrained by similarity properties and constraint value ℓ is depicted by thick blue-bordered triangle region. Based on these assumptions, acceleration vectors $\mathbf{x}^{r,w}_{\beta_s,i,t,j}$ are transformed into unified feature space as one-dimensional feature vectors by considering preselected set of cumulant orders $k \in \mathcal{K}$ used in authentication procedure:

$$\begin{aligned}&\mathbf{f}^{\beta_s,k,r,w}_{i,t,j} \\ &= \left[\mathbf{C}^{(k)}_{\mathbf{x}^{r,w}_{\beta_1,i,t,j}}(l_1, \ldots, l_{k-1}) \quad \ldots \quad \mathbf{C}^{(k)}_{\mathbf{x}^{r,w}_{\beta_S,i,t,j}}(l_1, \ldots, l_{k-1}) \right]^T\end{aligned} \tag{6}$$

by the following constraints on time lags considered:

$$\{(l_1, \ldots, l_{k-1}) : 0 \leqslant l_1 \leqslant \ldots \leqslant l_{k-1} \leqslant \ell\} \tag{7}$$

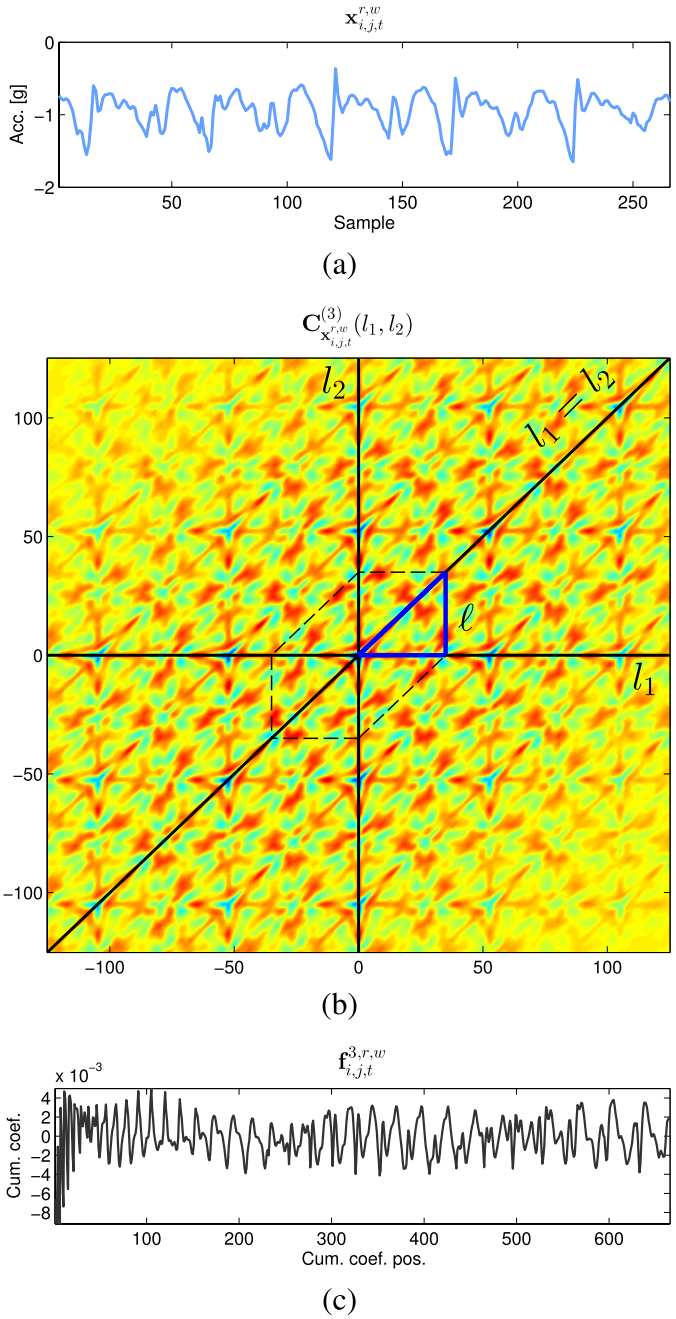


Fig. 1. An example of accelerometer data transformation to feature vectors by $k = 3$: (a) input single-channel acceleration signal; (b) 3rd ordered cumulants computed from (a) using Eq. 4 – symmetric regions are divided by thin solid lines (periodic gait patterns can be easily noted); (c) vector of cumulant coefficients obtained by diagonal scanning of the region of interest in the principal region bounded by parameter ℓ (thick blue-bordered triangle).

Since HOC are represented as functions of $k-1$ variables, cumulant coefficients having $k \geq 3$ are reshaped into one-dimensional vectors. By doing so, we propose multidimensional diagonal scanning with the respect to ascending time lags in order to maintain the adjacency of cumulant coefficients within the region of interest.

Considering the constraints defined by Eq. 7, feature vectors $\mathbf{f}_{i,t,j}^{\beta_s,k,r,w}$ have unified representation by fixed length $N_{\mathbf{f}}$ irrespective to the length of input vectors $\mathbf{x}_{\beta_s,i,t,j}^{r,w}$, which applies for the same sensor set-up β and set of cumulant orders $k \in \mathcal{K}$. Signals having similar statistical properties are described by similar coefficient values regardless to their length.

Complete authentication domain is defined as a feature matrix $\mathbf{F}$ consisting of feature vectors $\mathbf{f}$ subject to $t \in \mathcal{T}$ indicating particular experiments (measurements):

$$\mathbf{F}_t^{\beta_s,k,r,w} = \Big[\mathbf{f}_{1,t,1}^{\beta_s,k,r,w} \quad \dots \quad \mathbf{f}_{1,t,J_1}^{\beta_s,k,r,w} \quad \dots \quad \mathbf{f}_{i,t,1}^{\beta_s,k,r,w} \quad \dots \quad \mathbf{f}_{i,t,J_i}^{\beta_s,k,r,w} \quad \dots \quad \mathbf{f}_{I,t,J_I}^{\beta_s,k,r,w}\Big]^T \tag{8}$$

Since the problem of gait authentication can base either on cross-comparative similarity analysis of gait patterns or machine-learning-based approaches, two collections of gait patterns are constructed: one collection contains learning (reference) patterns, defined as gallery patterns $\{\tilde{\mathbf{g}}_m\}$, while the other collection consists of testing patterns, defined as probe patterns $\{\tilde{\mathbf{p}}_m\}$ [10]. According to Eq. 8, both collections of gait patterns can be represented as gallery matrix $\tilde{\mathbf{G}}$ and probe matrix $\tilde{\mathbf{P}}$, where both sets of gait patterns are treated separately with respect to the preselected cumulant orders $k \in \mathcal{K}$ and sensor set-up β_s:

$$\tilde{\mathbf{G}}^{\beta_s,k,r,w} = \mathbf{F}_t^{\beta_s,k,r,w}, \quad t \in \mathcal{T}_G \subset \mathcal{T}$$
and
$$\tilde{\mathbf{P}}^{\beta_s,k,r,w} = \mathbf{F}_t^{\beta_s,k,r,w}, \quad t \in \mathcal{T}_P \subset \mathcal{T} \tag{9}$$

where $\mathcal{T}_G \cap \mathcal{T}_P = \varnothing$. This step is essential since individual features (cumulant coefficients) for each k are represented within different context, and is reasonable in order to consider the contribution of sensor set-up that can rely on multi-channel (also multi-sensor) readings, where each channel carries the information on motion trajectories depending directly on sensor location and the measurement directions (accelerometer axes). Such multi-modal representation is modelled in order to combine feature-based and sensor-based data fusion within the authentication step. To facilitate this, two additional steps are necessary: feature scaling and dimension reduction.

Feature scaling is important in order to achieve uniform representation of individual cumulant coefficients within feature vectors. Let vectors μ_c and σ_c contain estimated mean values and standard deviations of c-th cumulant coefficient along the columns of gallery matrix $\tilde{\mathbf{G}}$, respectively. Normalized gallery pattern $\hat{\mathbf{g}}^{\beta_s,k,r,w}$ is obtained by standardization of individual feature values in $\tilde{\mathbf{g}}^{\beta_s,k,r,w}$ as:

$$\hat{\mathbf{g}}_c^{\beta_s,k,r,w} = \frac{\tilde{\mathbf{g}}_c^{\beta_s,k,r,w} - \mu_c^{\beta_s,k,r,w}}{\sigma_c^{\beta_s,k,r,w}} \tag{10}$$

When performing authentication scenario on large dataset, the use of z-score normalization is reasonable since it turns out that produces common numerical range regardless to the observed parameters β_s and k.

A considerable amount of redundancy can appear in feature vectors represented by HOC. Therefore, we propose the transformation of normalized matrix $\hat{\mathbf{G}}$ into its approximated version preserving non-redundant information by employing truncated singular value decomposition (tSVD). For arbitrary value of e representing reduced dimension, where $e \ll N_c$, tSVD of $\hat{\mathbf{G}}$ is defined as:

$$\hat{\mathbf{G}}_e = \mathbf{U}_e \boldsymbol{\Sigma}_e \mathbf{V}_e{}^T \tag{11}$$

where $\mathbf{U}_e$, Σ_e and $\mathbf{V}_e$ contain top e left-singular vectors, right-singular vectors and associated singular values, respectively. Thus, gallery matrix $\mathbf{G}^{\beta_s,k,r,w}$ of reduced dimension e is obtained by projecting feature vectors $\mathbf{g}^{\beta_s,k,r,w}$ onto the top of e eigenfeatures represented by columns of $\mathbf{V}_e$:

$$\mathbf{G}^{\beta_s,k,r,w} = \mathbf{U}_e^{\beta_s,k,r,w} \Sigma_e^{\beta_s,k,r,w} = \hat{\mathbf{G}}^{\beta_s,k,r,w} \mathbf{V}_e^{\beta_s,k,r,w} \quad (12)$$

Reduced dimension e is defined implicitly by proportion of variance, covered by top e eigenfeatures.

Parameters μ_c, σ_c and $\mathbf{V}_e$ obtained by feature scaling and dimensionality reduction step on gallery patterns represent the basis for the transformation of probe patterns into normalized and reduced feature space. Thus, prior to authentication step, each of further incoming probe patterns is normalized:

$$\hat{\mathbf{p}}_c^{\beta_s,k,r,w} = \frac{\tilde{\mathbf{p}}_c^{\beta_s,k,r,w} - \mu_c^{\beta_s,k,r,w}}{\sigma_c^{\beta_s,k,r,w}} \quad (13)$$

and projected onto first e eigenfeatures by

$$\mathbf{p}^{\beta_s,k,r,w} = \hat{\mathbf{p}}^{\beta_s,k,r,w} \mathbf{V}_e^{\beta_s,k,r,w} \quad (14)$$

respectively.

IV. Gait Authentication

By gait authentication in general, probe patterns $\{\mathbf{p}_m\}$ are compared to gallery patterns $\{\mathbf{g}_m\}$. Depending on the methodological approach, each probe pattern is recognized or classified as a gait pattern corresponding to one (or none) of the subjects having their gait patterns included in a gallery. There are several different options to perform gait authentication depending on the methodological approach. By employing machine learning approaches, gallery is denoted as training set and each gallery pattern is labelled by the corresponding class (gait owner). Followed by the learning step, classification process assigns one of the labels defined within the training set to each of the input probe patterns. On the other hand, pairs of gait patterns transformed into predefined feature space can be compared crosswise. In this manner, gait recognition is performed by computing dissimilarity score $d(\mathbf{g}_i, \mathbf{p})$ for any pair $(\mathbf{g}_a, \mathbf{p}_b)$ consisting of arbitrary gallery pattern $\mathbf{g}_i$ for the owner i and arbitrary probe pattern $\mathbf{p}$. If dissimilarity score does not exceed predefined global acceptance threshold, $\mathbf{p}$ is with the correspondence to $\mathbf{g}_i$ accepted as owner i and rejected otherwise. Dissimilarity score $d(\mathbf{g}_i, \mathbf{p})$ is computed using suitable distance metric between $\mathbf{g}_i$ and $\mathbf{p}$ (i.e. correlation distance).

Since proposed approach exploits properties of multi-modal representation relying on sensor set-up β_s (multi-channel or multi-sensor observations) and preselected cumulant orders $k \in \mathcal{K}$, pairs of gait patterns $(\mathbf{g}_i, \mathbf{p})$ are compared by combining feature-based and sensor-based fusion [38], allowed by proper data standardization (Eq. (10)). Initially, dissimilarity scores computed individually for each combination of β_s and $k \in \mathcal{K}$ are gathered in the score vector $\mathbf{d}$:

$$\mathbf{d} = \left[d\left(\mathbf{g}_i^{\beta_1,k}, \mathbf{p}^{\beta_1,k}\right) \quad \ldots \quad d\left(\mathbf{g}_i^{\beta_S,k}, \mathbf{p}^{\beta_S,k}\right) \right]^T, \quad k \in \mathcal{K} \quad (15)$$

Fused dissimilarity score φ of the gait pattern pair $(\mathbf{g}_i, \mathbf{p})$ is then determined implicitly by applying predefined fusion operation $\mathcal{F}[.]$ on score vector $\mathbf{d}$:

$$\varphi\left(\mathbf{g}_i^{\beta_s,k}, \mathbf{p}^{\beta_s,k}\right) = \underset{\beta_s,k}{\mathcal{F}}[\mathbf{d}]. \quad (16)$$

where $\mathcal{F}[.]$ relies on one of the known fusion techniques [38].

For realistic gait authentication scenario it is reasonable to have collection of multiple gait patterns for each owner in the gallery that can be extended by additional gait patterns over time. In practice, these patterns are collected either by several daily random measurements or from single measurement, where interruptions apply during the acquisition. Such operability enhances the collectability property of the proposed approach. In this case, signals having sufficient length (holding one gait cycle at least) are preserved while the other are discarded. The same applies also for the collection of probe patterns. Adopting this concept, the reliability of the proposed authentication approach should ensure sufficient performance irrespective to the input signal length or number of gait patterns in the collections for the owner. Therefore, three versions of dissimilarity scores, δ_1, δ_2 and δ_3, based on Eq. 16 in terms of collection handling are introduced and applied in the following.

Basically, when adopting the gait authentication step as proposed in [10], for any probe pattern $\mathbf{p}$, dissimilarity score between it and the gallery collection $\mathbf{G}_i$ of the owner i is obtained by applying minimum rule:

$$\delta_1\left(\mathbf{G}_i^{r,w}, \mathbf{p}^{r,w}\right) = \min_{j_i} \varphi\left(\mathbf{g}_{i,j_i}^{\beta_s,k,r,w}, \mathbf{p}^{\beta_s,k,r,w}\right). \quad (17)$$

In practice, it is expected that gallery collection of gait-based authentication system will contain large amount of gait patterns obtained by large number of owners. That means that comparison of individual probe patterns by each pattern in a gallery would be computational consuming. Proposed HOS-based approach has interesting property, where after the transformation into feature space the values of particular cumulant coefficients do not vary much when comparing similar gait patterns. Thus, whole gallery collection $\mathbf{G}_i$ of the owner i can be represented by single template $\bar{\mathbf{g}}_i$ in terms of mean values of particular cumulant coefficients over all gallery patterns of the owner i. In this case, dissimilarity score between it and any probe pattern can be computed as:

$$\delta_2\left(\mathbf{G}_i^{r,w}, \mathbf{p}^{r,w}\right) = \varphi\left(\bar{\mathbf{g}}_i^{\beta,k,r,w}, \mathbf{p}^{\beta,k,r,w}\right). \quad (18)$$

The same concept can be applied when handling multiple probe patterns obtained by a single measurement (i.e. divided into segments on purpose or when interruptions during acquisition apply). In this case, collection of probe patterns $\mathbf{P}_a$ of the owner a is transformed into single gait pattern template $\bar{\mathbf{p}}_a$ in the same manner as $\bar{\mathbf{g}}_i$ and dissimilarity score is then computed as:

$$\delta_3\left(\mathbf{G}_i^{r,w}, \mathbf{P}_a^{r,w}\right) = \varphi\left(\bar{\mathbf{g}}_i^{\beta,k,r,w}, \bar{\mathbf{p}}_a^{\beta,k,r,w}\right). \quad (19)$$

Finally, global acceptance threshold is applied to either of δ_1, δ_2 or δ_3 in order to decide whether the observed probe pattern corresponds to gallery collection owner i or not.

V. Experimental Datasets

Evaluation of the proposed approach relies on three recently published gait datasets. First two datasets, OU-ISIR-1 and OU-ISIR-2, are subsets of OU-ISIR Biometric Database, provided by Osaka University [10], representing currently the world largest inertial-sensor-based biometric dataset, while the third gait dataset, MCGILL, is provided by researchers

of McGill University [11]. These datasets were already used for the evaluation of some latest efficient gait authentication approaches. OU-ISIR datasets were used for the evaluation of approaches proposed in [12], [13], [21], and [39], while the MCGILL dataset was used for the performance evaluation of the framework for time-series analysis based on geometric template matching proposed in [11].

By OU-ISIR-1 and OU-ISIR-2, acceleration data was acquired by triaxial accelerometers inside three IMUZ sensors. These were mounted on a waist belt having two IMUZ located at the left and the right of subjects waist and one IMUZ and smartphone located at the center back. In this manner, unified sensor set-up is ensured for all the subjects. Each of datasets contains two collections of shorter gait sequences represented by accelerometer data acquired for each subject. In our experiments, collections of gallery and probe patterns are in both cases constructed from first and second collection, respectively. First dataset, OU-ISIR-1, contains accelerometer data of 744 subjects acquired by triaxial accelerometer mounted at the center back of the waist belt, covering wide age distribution and equal gender ratio of the subjects. The average length of gallery sequence is 5.97 ± 1.18 s, while the average length of probe sequence is 4.85 ± 1.10 s. Large number of subjects included in OU-ISIR-1 allows us to examine how the number of subjects affect the performance of the proposed authentication approach and to determine how efficient is proposed approach on large dataset by complete OU-ISIR-1 dataset included in the authentication step. On the other hand, OU-ISIR-2 dataset is primarily used for investigation of authentication performance influenced by different sensor locations. Besides that, OU-ISIR-2 dataset is also used for the evaluation of fusion concept of the proposed approach. In this case, accelerometer data was acquired simultaneously by all three triaxial accelerometers. Dataset contains accelerometer data of 495 subjects having an average length of gallery sequence of 4.89 ± 1.07 s and the average length of probe sequence of 5.58 ± 0.79 s.

One of the most important goals is to investigate whether the proposed approach operates sufficiently also in real-life scenario, putting authentication procedure in considerably aggravated circumstances that directly affect both uniqueness and permanence of gait patterns. In Section II-A we already introduced the importance of smartphone based gait authentication and its limitations, including sensor location and orientation. Thus, dataset collected using smartphones during subjects' casual walking and behavior is reasonable in such case. MCGILL dataset [11] contains data from 20 subjects acquired when carrying smartphone in their pocket. Two daily measurements were carried out for each subjects performing 15 minute walk on several different surfaces and slopes. Phone was casually placed in their pocket and they were allowed to change clothing and footwear for each daily measurement.

By first two datasets, acceleration signals were acquired by constant frequency of 100 Hz. In realistic case, due to limited bandwidth and power consumption of wearable devices and sensors, it is desired to achieve good performance having the lowest amount of data as possible when carrying out authentication procedure. Thus, all signals from OU-ISIR-1 and OU-ISIR-2 datasets were downsampled by factor 4 to a sampling frequency of 25 Hz. By MCGILL dataset, all signals were sampled by non-constant sampling frequency. Thus, acceleration signals were resampled to a fixed sampling frequency, also of 25 Hz, using linear interpolation.

A. Experimental Parameters

Proposed transformation into feature space of HOC relies on the selection of two parameters: $k \in \mathcal{K}$ representing set of preselected cumulant orders K, used for computation of feature vectors using Eq. 6, and parameter ℓ used to set constraints on non-redundant principal region of cumulants (Eq. 7). Considering parameter K, we experimented with the cumulants of 2nd, 3rd and 4th order. Second parameter, ℓ, should determine maximum expected period length of the observed phenomenon. According to [37], the minimum expected step frequency is equal to 1.4 Hz. Then, by minimum expected gait frequency of 0.7 Hz, maximum expected length between two consecutive gait onsets is approx. 1.4 s. It is interesting that this value also corresponds within the optimal interval length for on-body activity recognition systems, as recently determined in [9]. Considering predefined sampling frequency f_s equal to 25 Hz, parameter ℓ is set to 35. Since the values of cumulant coefficients do not vary drastically according to their adjacent values, computational complexity can be further reduced by skipping time lags l_i during the calculation of cumulant coefficients. In our experiments, even time lags were considered only: $\{(l_1, \ldots, l_{k-1}) : 0 \leq \ldots \leq l_{2i} \leq \ldots \leq \ell\}$, reducing feature vector length by factor 2. Thus, after the transformation of j-th single-channel signal segment $\mathbf{x}_{\beta_s}$ of arbitrary length into feature space, we obtain 1539 cumulant coefficients. Since the length of feature vectors is directly related to k, ℓ and f_s, their length is equal for OU-ISIR-1, OU-ISIR-2 and MCGILL dataset. Furthermore, when applying tSVD (Eq. 12), dimensionality of feature matrix was reduced by selecting parameter e such that represents the number of top eigenfeatures that cover 96% of variance in data. When performing authentication procedure, correlation distance was used as dissimilarity score $d(\mathbf{g}_i, \mathbf{p})$ and sum of scores was used as fusion operation $\mathcal{F}[.]$ (see Section VI-B for more details on evaluation of fusion techniques).

VI. Evaluation and Results

Datasets presented in Section V were used for the performance evaluation of the proposed approach considering the following aspects: impact of the number of subjects and evaluation on large dataset (Section VI-A), impact of sensor location and evaluation of sensor fusion (Section VI-B), and evaluation of casual authentication scenario using smartphones (Section VI-C), relying on OU-ISIR-1, OU-ISIR-2 and MCGILL datasets, respectively.

When evaluating the proposed authentication approach by OU-ISIR-1 and OU-ISIR-2 datasets, its performance is determined by ROC curve [10] representing the trade-off between false acceptance rate (FAR) and false rejection rate (FRR) by varying global acceptance threshold in authentication procedure. Performance measure is provided by equal error rate (EER) determined by rate at which FAR and FRR are equal.

Furthermore, an additional metric is introduced in order to evaluate the impact of the number of subjects on authentication performance by estimating the standard deviation of the FRR $\hat{\rho}$

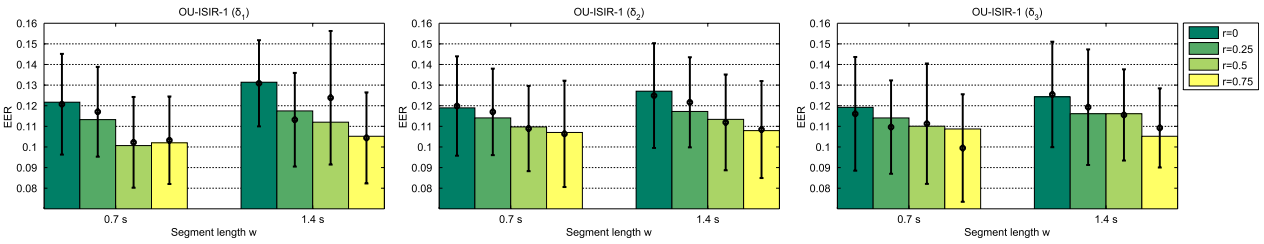


Fig. 2. Evaluation by OU-ISIR-1 dataset: EER values obtained when applying proposed approach on short segments of length $w = \{0.7\text{ s}, 1.4\text{ s}\}$ considering dissimilarity scores $\delta_{\{1,2,3\}}$ are denoted with bars, while errorbars represent average ERR values and their deviation on 30 random subsets of 60 subjects.

during multiple recognition attempts for each subject i as proposed and confirmed in [10]:

$$\hat{\sigma}\left(\hat{\rho}\right) = \sqrt{\frac{\sum a_i^2 - 2\hat{\rho}\sum a_i J_i + \hat{\rho}\sum J_i^2}{\bar{j}^2 I\left(I-1\right)}} \tag{20}$$

where a_i stands for the number of false rejections for i-th subject, J_i stands for the number of probe gait patterns for i-th subject, $\bar{j}$ stands for the average number of probe gait patterns per subject and I stands for the total number of subjects included in evaluation process. By estimating $\hat{\sigma}\left(\hat{\rho}\right)$, ROC curves can be shown along with their corresponding deviation boundaries. As the number of subjects used in evaluation process increases, performance becomes more reliable. This results in a narrower deviation boundaries around corresponding ROC curve. Based on these assumptions, the impact of the number of subjects by several authentication approaches or parameters used by authentication step can also be compared. Narrower the deviation boundaries, more reliable the authentication performance. Thus, it is also interesting to determine the reliability of the authentication approach using subsets that include smaller number of subjects. We proceed in the exact way as proposed in [10]. Considering our proposed experimental parameters, each experiment is repeated by 30 random subsets of gait patterns including 60 subjects. An average ROC curve is then computed from 30 obtained ROC curves and provided by deviation boundaries by applying Eq. 20. Overall average EER and its variability is also provided.

A. Performance Evaluation on Large Dataset

Applying the proposed approach on OU-ISIR-1 dataset, its performance on short acceleration signal segments was examined in the first place. Authentication procedure was evaluated using all three proposed dissimilarity scores $\delta_{\{1,2,3\}}$. For each of three authentication cases, ERRs were calculated for entire signal set, as well as the average ERR and its $\hat{\sigma}$ for the 30 random subsets of 60 subjects. Results are depicted in Fig. 2. In this case, we intended to examine the performance of the proposed approach when considering minimum allowed input gait sequence length. As already mentioned, it is directly related to maximum expected time interval between two consecutive gait cycles and is equal to 1.4 s [37]. Along that, the influence of signal overlapping prior to the transformation in feature space according to the parameter r was examined. It can be easily seen that ERR values in all cases slightly decrease while r increases. The reason lies in the fact that overlapped signal segments cover a wider range of gait phase transitions resulting in more complete representation of subjects gait pattern.

We also examined the possibility of further decreasing minimum allowed signal length. This can be achieved when considering physiological gait properties and sensor location in this specific scenario. If sensor is attached on healthy subjects in the way such that swing and stance phase relative to both legs affect acceleration signal in symmetrical way, then gait patterns of individual steps are similar. Based on this assumption, single period relies on single step irrespective of left or right foot. In this special case, maximum expected time interval can be reduced by half. Since OU-ISIR-1 contains data where sensor was located on the subjects center back during the acquisition, we also experimented with $w = 0.7$ s. The results are compared in Fig. 2. It is interesting that ERR values for $w = 0.7$ s and $w = 1.4$ s are similar, making the use of shorter segments in this particular case feasible. However, this specific situation was evaluated for experimental purposes only since such case is unlikely to appear in real-case authentication scenarios.

Comparing results obtained for three authentication cases relying on dissimilarity scores $\delta_{\{1,2,3\}}$ in Fig. 2, it can be easily seen that EER values do not vary much. This fulfils our expectations that gait authentication by the proposed approach can be performed on the basis of single representative gait template for each subject.

Influence of short signal segments on authentication performance by large dataset was further evaluated by ROC curves. Since results are very similar for $w = \{0.7\text{ s}, 1.4\text{ s}\}$ and $\delta_{\{1,2,3\}}$ (Fig. 2), only the representative case having $w = 1.4$ s and authentication procedure based on dissimilarity score δ_1 is depicted. Fig. 3a shows the ROC curve for the entire dataset. Obtained ERR is around 12% for the non-overlapping gait patterns and decreases when r increases and becomes stable at $r = 0.5$ having ERR of approx. 10%. It also needs to be considered that w is set to lowest allowable limit in this particular case and gait patterns are more diverse in terms of statistical representation due to unstable gait patterns and by higher r these fluctuations and gait phase transitions are within the gallery $\mathbf{G}$ covered more completely. Fig. 3b shows ROC curve obtained by evaluation of subsets on short signal segments having $w = 1.4$ s. Obtained average EER values for all r are similar to the values obtained on whole dataset (Fig. 3a) and vary for about $\pm 2\%$. This indicates the reliability of the proposed approach irrespective to the number of subjects involved in the dataset.

In contrast to the evaluation of the proposed approach on short segment lengths, Fig. 3c shows ROC curves obtained by the evaluation on full-length signals. Results of the whole dataset are similar to these corresponding to $w = 1.4$ s (Fig. 3a). According to the fact that only one gait pattern is used for gallery and probe and the input gait

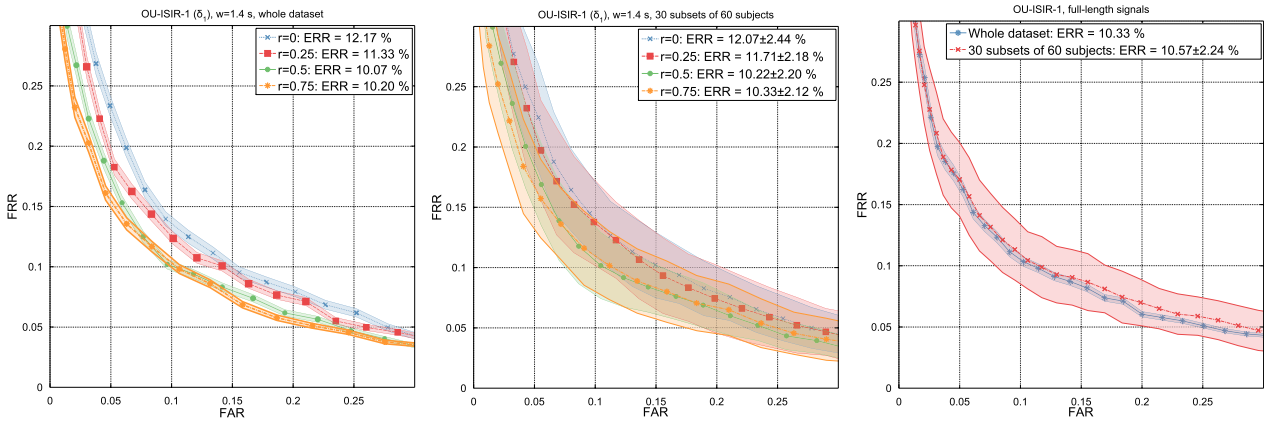


Fig. 3. Evaluation by OU-ISIR-1 dataset on short segments: (a) whole dataset; (b) 30 random subsets of 60 subjects (b); and (c) evaluation on full-length signals.

sequences do not have unified length, we can state that longer gait sequences more efficiently reflect the properties of gait patterns due to the statistical nature of the proposed approach. This is also proven by comparing ROC curve of the subsets in the Fig. 3c to the best-case scenario on Fig. 3b, resulting in both similar average EER values and their deviation.

Obtained ERR values can be compared directly with the latest most efficient gait authentication approaches that were already evaluated with OU-ISIR-1 dataset as reported in [10]. In this context, the best authentication approach yields ERR of 13.7%. In similar conditions, our proposed approach improves EER by 3.5%. Obtained results reveal that our approach outperforms the existing approaches, those evaluated on the OU-ISIR-1 and those evaluated on considerably smaller datasets. Reliability of the proposed approach is proven by standard deviation ranges represented by very narrow bands around ROC curves (Fig. 3) calculated by using Eq. 20 on whole datasets.

B. Performance Evaluation on Multi-Sensor Dataset

OU-ISIR-2 dataset was used for the evaluation of the proposed approach on multi-sensor data containing gait sequences acquired simultaneously by three different sensor locations: center back, left waist and right waist. We experimented with segment lengths $w = \{1.4\text{ s}, 2.8\text{ s}\}$. Fig. 4 shows EER values for all three sensor locations, where three authentication cases relying on dissimilarity scores $\delta_{\{1,2,3\}}$ were performed for each location. By comparing the results considering both values of parameter w for each δ and sensor location (pair-wise comparison within plots) it can be easily seen that we obtained similar EER values that decrease when r increases. Similar EER values can be easily noticed also when comparing three authentication cases by dissimilarity scores $\delta_{\{1,2,3\}}$ for each of sensor locations (column-wise comparison). However, there is significant difference in EER values when observing different sensor locations. A further insight into authentication performance is provided by Fig. 5, where ROC curves for the authentication scenario of all three sensor locations are shown, evaluated on whole dataset and on 30 random subsets of 60 subjects, for the representative case having segment length $w = 1.4$ s and dissimilarity score δ_1. As in [10], authentication performance results in significant improvement when sensor is located on the waist instead of the back. It is also interesting, that the recognition accuracy of sensor located on left waist provides slightly better result as the sensor, located on right waist, proving that sensor location can have significant influence on authentication performance.

Fusion-based operability is one of the most important properties of proposed authentication approach. As already mentioned, fusion process is designed in a generalized way relying on single fusion technique by combining feature-based fusion depending on the selection of cumulant orders used by transformation of gait sequences into HOC, and sensor-based fusion, regarding to sensor set-up, fusing multi-channel or multi-sensor data for particular sensors. OU-ISIR-2 dataset was most convenient to use for the evaluation of several fusion techniques, consequentially leading into selection of the most appropriate one for all authentication cases when applying fusion operation $\mathcal{F}[.]$ within the authentication procedure (Eq. 16). We experimented with several fusion techniques as proposed in [38]. They were evaluated on non-overlapping and short signal segments having length $w = 1.4$ s. ROC curves and corresponding EER values after the fusion process employing several fusion techniques are shown in Fig. 6a. Based on these results, sum of scores turns out as the best fusion technique having a slight precedence over maximum value of scores.

Furthermore, since the proposed concept can be easily adopted to multi-sensor fusion, an additional attempt of further improving authentication performance was made by simultaneously combining gait sequences acquired by all three sensors. Sensor fusion was performed implicitly by applying Eq. 16. Authentication performance by applying sensor fusion is evaluated by ROC curves joined to the ROC curves showing performance of individual sensor locations on short signal segments ($w = 1.4$ s) in Fig. 5 for easier comparison when employing whole dataset (Fig. 5d) and 30 random subsets of 60 subjects (Fig. 5h). As by large dataset, the performance of the proposed approach was also evaluated by applying full-length signals from the second dataset for all three sensor locations separately as well as by their fusion. ROC curves for the whole dataset are shown in Fig. 6b and for 30 random subsets of 60 subjects in Fig. 6c.

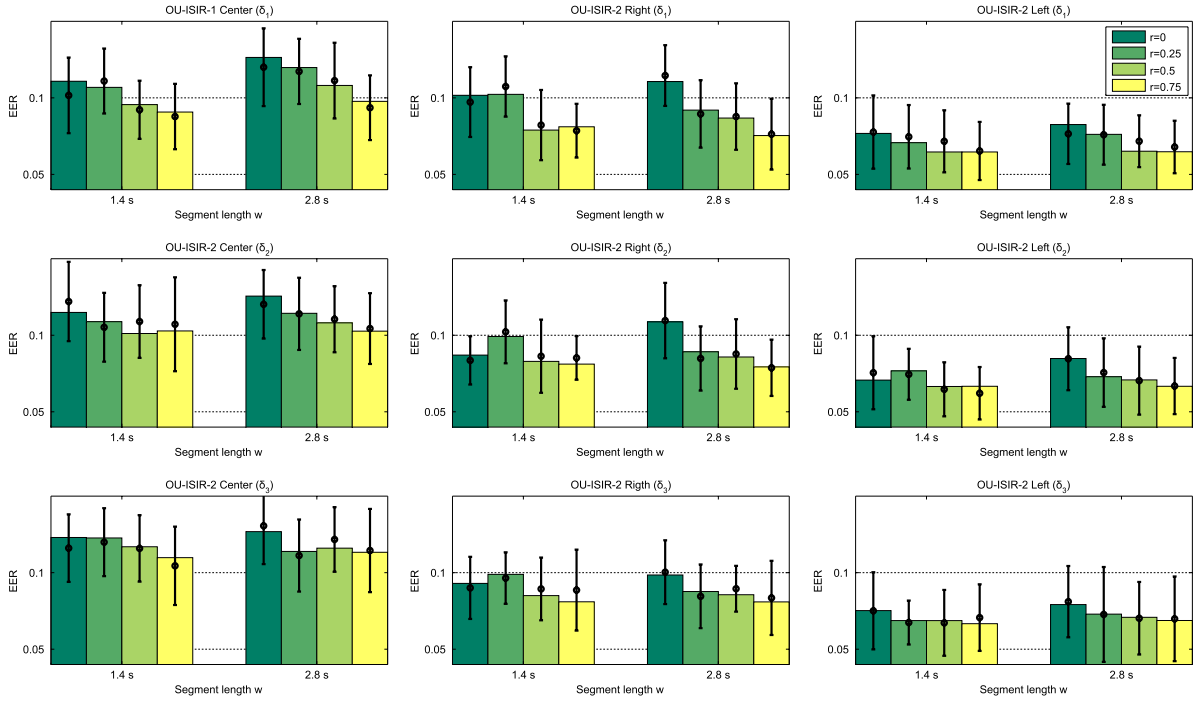


Fig. 4. Evaluation by OU-ISIR-2 dataset: EER values obtained when applying proposed approach on short segments having $w = \{1.4\text{ s}, 2.8\text{ s}\}$ considering dissimilarity scores $\delta_{\{1,2,3\}}$ are denoted with bars, while errorbars represent average ERR values and their deviation on 30 random subsets of 60 subjects.

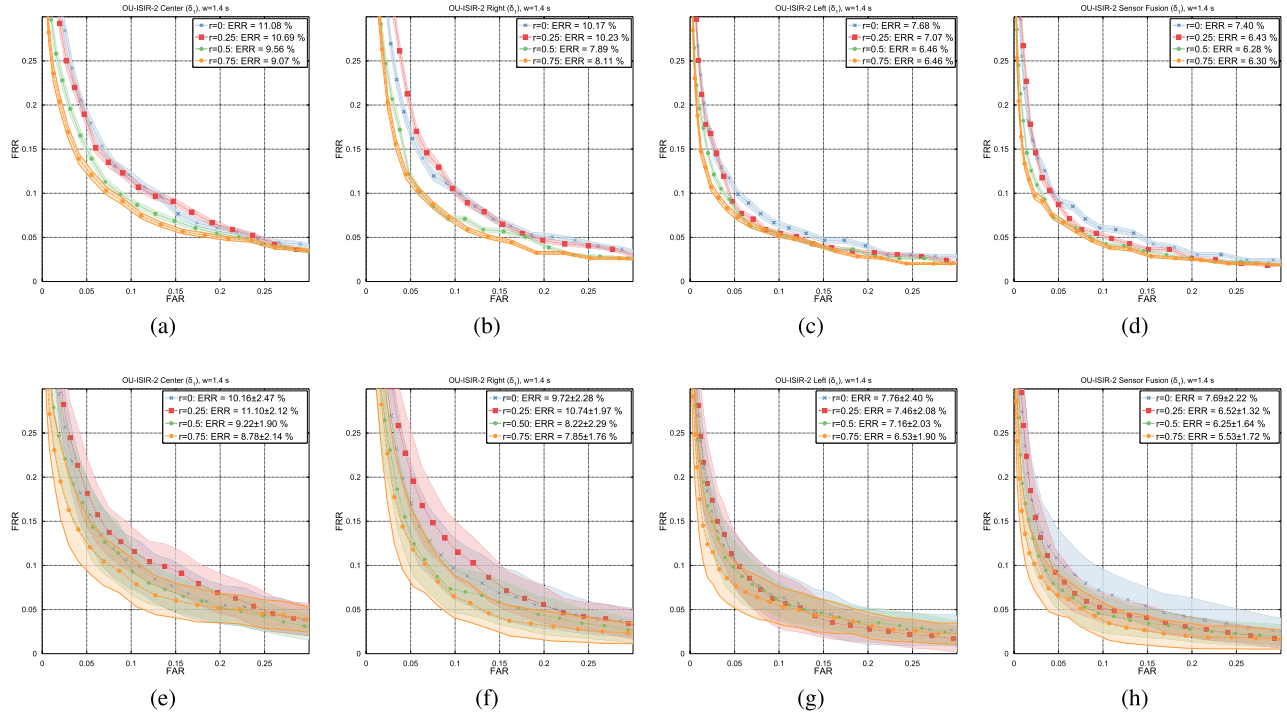


Fig. 5. Evaluation by OU-ISIR-2 dataset on short segments: (a-d) whole dataset; and (e-h) 30 random subsets of 60 subjects.

As expected, authentication performance considering individual sensor location reveal similar disclosures as by authentication performance evaluated on large dataset presented in Section VI-A. When comparing results obtained by both datasets including data acquired from sensor located at center back, the results are basically the same. The choice of more appropriate sensor location has lead into significant improvement of accuracy – the EER is reduced to approx 6.5% in the case of left waist sensor, and was further slightly reduced for about 0.5% when applying sensor fusion.

We have compared the performance of our proposed approach with the best-performing approach evaluated using OU-ISIR-2 in [10]. Acceleration magnitude signals were used instead of 3-channel readings. This resulted in higher EER values in general. Reported EER values for the center back, left waist and right waist sensors are 19.5%, 16.1% 14.9%, respectively. In our case, by performing authentication using

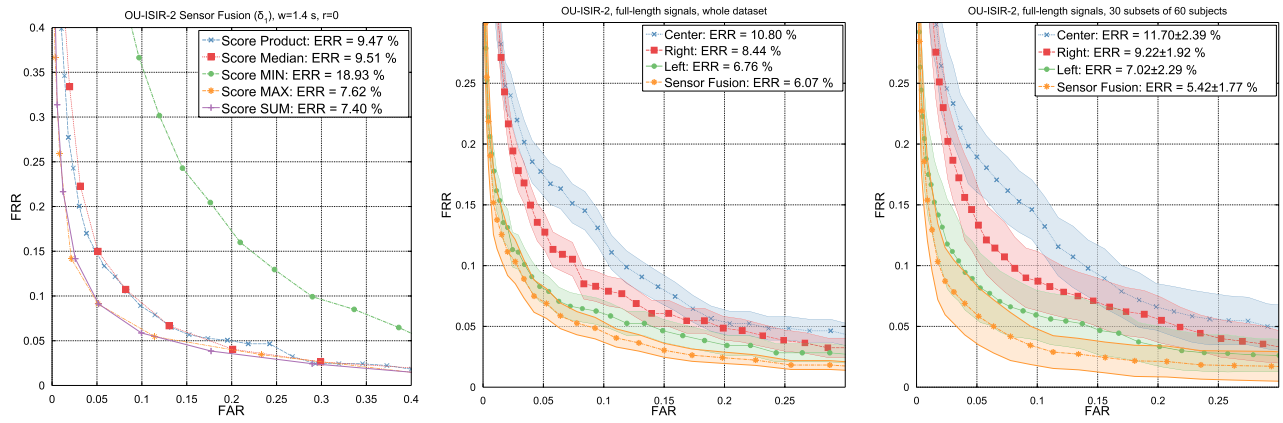


Fig. 6. Evaluation by OU-ISIR-2 dataset: (a) evaluation of fusion techniques; (b) evaluation on full-length signals (whole dataset); and (c) evaluation on full-length signals (30 random subsets of 60 subjects).

single-channel magnitude signals of the same dataset, we obtained ERR values of 15.9%, 14.5% and 14.9% for the center, left and right sensor, respectively. By applying multi-sensor fusion of all three sensors, ERR was further reduced to 13.4%. Considering average EER values of all three sensor locations for both approaches ($16.8 \pm 2.4\%$ and 15.1 ± 0.7 %), our proposed approach outperformed the one evaluated in [10] for approx. 1.7%. Our approach also shows considerably lower variability reflecting stable performance irrespective to sensor location. The results show that the efficiency and reliability of our method is consistently better compared to existing approaches.

C. Performance Evaluation on Smartphone Dataset

Feasibility of applying the proposed approach in real-world scenarios was evaluated on MCGILL dataset containing accelerometer data acquired by 20 subjects performing casual walking in two different days. By doing so, evaluated performance was compared to the approach based on geometric template matching [11], where their TDEBOOST algorithm was efficiently applied to the problem of gait authentication in aggravated circumstances. In order to ensure an objective comparison, authentication procedure is in this case carried out by applying machine learning approach and presented by metrics in the similar way as proposed in [11].

In this case, in order to suppress the influence of sensor orientation, proposed approach was applied to single-channel magnitude signals, calculated as euclidean norm of 3-channel acceleration signals. Prior to gait recognition, walking segments were extracted by applying windowing and thresholding, as proposed in [11]. Gait authentication was relying on 1-nearest neighbour classifier (NN). Classification was evaluated by 100-fold cross-validation. For each run, gallery and probe pattern collections were determined as randomly selected segments of length ω from training data on day 1 and testing data on day 2, respectively, and transformed into feature vectors. We experimented with segment lengths ω of 2.8 s, 4.2 s, 8.4 s and 12.6 s. We ensured that selected segments were not overlapping. For each ω, we extracted all possible segments that meet above mentioned conditions for both gallery and probe patterns. The proposed approach was tested by 10 classifiers in parallel, built by preserving only random $\eta\%$ of gallery patterns having $\eta = 10, 20, \ldots, 100\%$. By classification process, each of probe patterns was classified into one of the corresponding classes.

The results of NN-based classifier in terms of accuracy are shown in Fig. 7. In order to get better insight into authentication performance, we also consider average precision and recall values for particular subjects. These are shown in Fig. 8 for ω equal to 2.8 s as in [11] when performing classification using NN.

The performance of the proposed approach can be directly compared with the approach proposed by [11]. They reported the following accuracy values: 42.0% when applying TDEBOOST trained with AdaBoost.M1, additionally improved to 63.0% when introducing label smoothing post-processing step, and 42.4% when applying NN classification to 2000 randomly selected signal segments of length $\omega = 2.8$ s. On the other side, by our authentication approach, NN-based classification of gait patterns having $\omega = 2.8$ s resulted in the accuracy of 64.5%. Thus, it outperforms TDEBOOST in all cases, namely for 22.1% when applied in the similar conditions and for 1.5% by their best-case classification task including additional data post-processing. As expected, the accuracy of our approach is further improved by increasing value ω. Considering parameter η, overall accuracy differs for less than 10% between $\eta = 10\%$ and $\eta = 100\%$.

Average precision and recall values shown in Fig. 8 also reflect very interesting results for particular subjects. Obtained values can be compared with the results reported in [11]. Considering the threshold equal to 0.6 for both precision and recall, close to the accuracy of both approaches, there are 7 and 3 subjects out of 20 where TDEBOOST has precision and recall greater than threshold, respectively. By applying our approach, there are 11 subjects where precision and 14 subjects having recall greater than predefined threshold. However, it is very interesting that both algorithms poorly classified subjects 4, 12 and 14. As stated in [11], this is related to the drastic change in clothing. These limitations, as well as IMU configuration of smartphones, the possibility of an arbitrary positioning and orientation, allowing for authentication performed directly on multi-channel accelerometer data in this particular case, are out of the scope of this paper and will be tackled within further investigations.

Obtained results reveal that the proposed gait authentication approach shows its great potential also in realistic situations involving aggravated conditions for authentication,

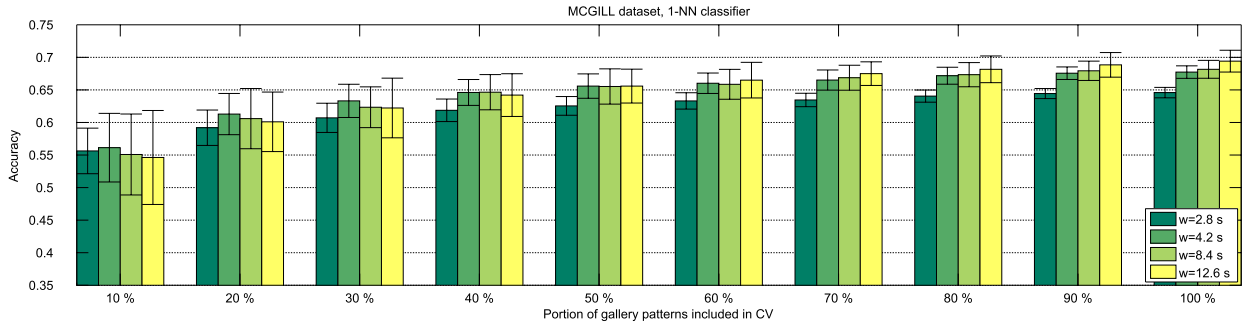
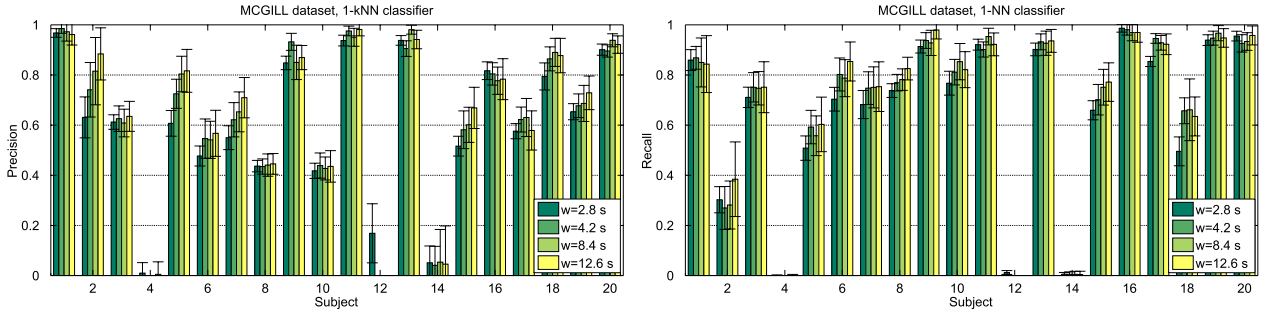


Fig. 7. Evaluation by MCGILL dataset: overall recognition accuracy of the classification using nearest neighbour classifier on non-overlapping random subsets by 100 rounds of cross validation.



(a) (b)

Fig. 8. Evaluation by MCGILL dataset: precision (a) and recall (b) after the classification of gait patterns using nearest neighbour classifier (training on the collection of gallery patterns and testing on the collection of probe patterns).

that were covered by evaluation on MCGILL dataset. As a result of the slight improvement in terms of performance, corresponding contribution to the unique and permanent representation of gait patterns of the proposed approach in comparison with the existing approaches can be assumed.

VII. Security Implications

In the context of security relevant aspects [7], proposed accelerometer-based gait authentication approach reveals significant contribution in terms of performance and collectability and sufficiently addresses permanence and uniqueness. However, the issue of gait affecting factors is far from being resolved adequately and still represents an open challenge that is encouraged to be addressed systematically in further research activities.

Another important biometric factor that needs to be considered is circumvention performed with either spoofing or avoidance as possible attack or countermeasure. There has already been an interesting research performed right on this topic published in [20] with results measured through the performance of their authentication approach. Authors have reported that a minimal effort impersonation attack does not significantly increase the chances of impostors being accepted whether the attacker with the knowledge of the closest math can be serious threat to the biometric system. Since the experiments were performed by one of the earliest approaches with higher EER in comparison with the proposed one, the anticipation that at least similar assumptions hold for our approach is reasonable. Furthermore, avoidance is still major drawback of all acceleration-based gait authentication approaches since only natural gait pattern is permanent as biometric trait, including the manageable deviations due to the slight influence of gait affecting factors. The problem is that the user can consciously affect the gait pattern (i.e. drastically or randomly changing the way of walking) if one does not want to be identified. Currently, there are several lines of work that address circumvention issues, i.e. by merging accelerometer data with cryptographic techniques to eliminate attacks [40].

VIII. Conclusion and Future Work

In this paper, we presented a novel and efficient approach for gait authentication based on higher-order statistics. Statistical analysis of gait patterns is achieved by transformation of acceleration signals in feature space relying on higher-order cumulants. Approach was evaluated using three datasets, with first two datasets as a part of currently the largest available gait-related biometric dataset OU-ISIR [10], obtained by experiments in controlled conditions covering many gait-related factors, and the third dataset, MCGILL [11], obtained by experiments involving casual walking and acquisition of accelerometer signals using smartphones. Applying our proposed approach on OU-ISIR datasets, EER values of 6% to 12% reveal reliable performance of the proposed approach regardless to the number of subjects involved in the authentication scenario or sensor location and with its additional improvement by introducing multi-sensor data fusion. Compared with the latest most efficient approach [10] using the same dataset, our approach has shown better performance. The ERR values have improved by 3.5%, 1.7% and 3.4% when considering large number of subjects, sensor location and multi-sensor fusion, respectively. Furthermore, the evaluation on the MCGILL dataset has outperformed the well-accepted approach based on geometric template matching [11] by 22.1% when applied in the similar conditions and 1.5% by their best-case classification task. Based on these facts we believe that our proposed approach indicates an important step towards

improving the accelerometer-based gait authentication, since it represents one of the most reliable and efficient available gait authentication approaches that are currently available.

Nevertheless, the proposed gait authentication approach still holds potential for further development, especially in terms of improving its efficiency and accuracy by real-life authentication problem relying on data acquired by smartphones. In the first place, the biggest challenge is to further examine several factors that affect gait pattern and their influence on the uniqueness and permanence in the context of the proposed approach. Besides that, possibility of circumvention will be investigated thoroughly. The proposed approach will be also deployed as a service which will allow real-time operability and efficient integration into existing cloud platforms and will be available to end-users. Last but not least, biometric fusion of the proposed approach with established biometric systems will also be examined.

REFERENCES

[1] M. W. Whittle, *Gait Analysis: An Introduction*, 4th ed. London, U.K.: Harrison, 2007.

[2] A. Muro-de-la-Herran, B. Garcia-Zapirain, and A. Mendez-Zorrilla, "Gait analysis methods: An overview of wearable and non-wearable systems, highlighting clinical applications," *Sensors*, vol. 14, no. 2, pp. 3362–3394, Jan. 2014.

[3] R. Vera-Rodriguez, J. S. D. Mason, J. Fierrez, and J. Ortega-Garcia, "Comparative analysis and fusion of spatiotemporal information for footstep recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 35, no. 4, pp. 823–834, Apr. 2013.

[4] G.-Z. Yang and M. Yacoub, *Body Sensor Networks*. London, U.K.: Springer-Verlag, 2006.

[5] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[7] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to Biometrics*. New York, NY, USA: Springer-Verlag, 2011.

[8] P. Gupta and T. Dallas, "Feature selection and activity recognition system using a single triaxial accelerometer," *IEEE Trans. Biomed. Eng.*, vol. 61, no. 6, pp. 1780–1786, Jun. 2014.

[9] O. Banos, J.-M. Galvez, M. Damas, H. Pomares, and I. Rojas, "Window size impact in human activity recognition," *Sensors*, vol. 14, no. 4, pp. 6474–6499, Jan. 2014.

[10] T. T. Ngo, Y. Makihara, H. Nagahara, Y. Mukaigawa, and Y. Yagi, "The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication," *Pattern Recognit.*, vol. 47, no. 1, pp. 228–237, Jan. 2014.

[11] J. Frank, S. Mannor, J. Pineau, and D. Precup, "Time series analysis using geometric template matching," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 35, no. 3, pp. 740–754, Mar. 2013.

[12] D. Gafurov, E. Snekkenes, and P. Bours, "Improved gait recognition performance using cycle matching," in *Proc. IEEE 24th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, Apr. 2010, pp. 836–841.

[13] M. O. Derawi, P. Bours, and K. Holien, "Improved cycle detection for accelerometer based gait authentication," in *Proc. 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Oct. 2010, pp. 312–317.

[14] H. Sun and T. Yuao, "Curve aligning approach for gait authentication based on a wearable accelerometer," *Physiological Meas.*, vol. 33, no. 6, p. 1111, 2012.

[15] C. Nickel and C. Busch, "Classifying accelerometer data via hidden Markov models to authenticate people by the way they walk," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 28, no. 10, pp. 29–35, Oct. 2013.

[16] A. Samà, F. J. Ruiz, N. Agell, C. Pérez-López, A. Català, and J. Cabestany, "Gait identification by means of box approximation geometry of reconstructed attractors in latent space," *Neurocomputing*, vol. 121, pp. 79–88, Dec. 2013.

[17] M. Derawi and P. Bours, "Gait and activity recognition using commercial phones," *Comput. Secur.*, vol. 39, no. 2, pp. 137–144, Nov. 2013.

[18] T. Hoang and D. Choi, "Secure and privacy enhanced gait authentication on smart phone," *Sci. World J.*, vol. 2014, May 2014, Art. ID 438254.

[19] S. Sprager and D. Zazula, "A cumulant-based method for gait identification using accelerometer data with principal component analysis and support vector machine," *WSEAS Trans. Signal Process.*, vol. 5, no. 11, pp. 369–378, 2009.

[20] D. Gafurov, E. Snekkenes, and P. Bours, "Spoof attacks on gait authentication system," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 491–502, Sep. 2007.

[21] N. T. Trung, Y. Makihara, H. Nagahara, R. Sagawa, Y. Mukaigawa, and Y. Yagi, "Phase registration in a gallery improving gait authentication," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–7.

[22] N. T. Trung, Y. Makihara, H. Nagahara, Y. Mukaigawa, and Y. Yagi, "Performance evaluation of gait recognition using the largest inertial sensor-based gait database," in *Proc. 5th IAPR Int. Conf. Biometrics (ICB)*, Mar./Apr. 2012, pp. 360–366.

[23] H. Lu, J. Huang, T. Saha, and L. Nachman, "Unobtrusive gait verification for mobile phones," in *Proc. ACM Int. Symp. Wearable Comput.*, 2014, pp. 91–98.

[24] T. T. Ngo, Y. Makihara, H. Nagahara, Y. Mukaigawa, and Y. Yagi, "Orientation-compensative signal registration for owner authentication using an accelerometer," *IEICE Trans. Inf. Syst.*, vol. E97-97, no. 3, pp. 541–553, 2014.

[25] M. Müller, "Dynamic time warping," in *Information Retrieval for Music and Motion*. Berlin, Germany: Springer-Verlag, 2007, pp. 69–84.

[26] D. Gafurov, K. Helkala, and T. Søndrol, "Biometric gait authentication using accelerometer sensor," *J. Comput.*, vol. 1, no. 7, pp. 51–59, 2006.

[27] A. Swami, G. B. Giannakis, and G. Zhou, "Bibliography on higher-order statistics," *Signal Process.*, vol. 60, no. 1, pp. 65–126, 1997.

[28] J. M. Mendel, "Tutorial on higher-order statistics (spectra) in signal processing and system theory: Theoretical results and some applications," *Proc. IEEE*, vol. 79, no. 3, pp. 278–305, Mar. 1991.

[29] C. L. Nikias and J. M. Mendel, "Signal processing with higher-order spectra," *IEEE Signal Process. Mag.*, vol. 10, no. 3, pp. 10–37, Jul. 1993.

[30] D. Zazula and A. Holobar, "An approach to surface EMG decomposition based on higher-order cumulants," *Comput. Methods Programs Biomed.*, vol. 80, no. 1, pp. S51–S60, Dec. 2005.

[31] U. R. Acharya, S. V. Sree, and J. S. Suri, "Automatic detection of epileptic EEG signals using higher order cumulant features," *Int. J. Neural Syst.*, vol. 21, no. 5, pp. 403–414, 2011.

[32] R. J. Martis, U. R. Acharya, C. M. Lim, K. M. Mandana, A. K. Ray, and C. Chakraborty, "Application of higher order cumulant features for cardiac health diagnosis using ECG signals," *Int. J. Neural Syst.*, vol. 23, no. 4, pp. 1350014-1–1350014-19, 2013.

[33] J. Inglada and G. Mercier, "A new statistical similarity measure for change detection in multitemporal SAR images and its extension to multiscale change analysis," *IEEE Trans. Geosci. Remote Sens.*, vol. 45, no. 5, pp. 1432–1445, May 2007.

[34] S. Sprager and D. Zazula, "Impact of different walking surfaces on gait identification based on higher-order statistics of accelerometer data," in *Proc. IEEE Int. Conf. Signal Image Process. Appl. (ICSIPA)*, Nov. 2011, pp. 360–365.

[35] C. W. Therrien, *Discrete Random Signals and Statistical Signal Processing*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1992.

[36] C. L. Nikias and A. P. Petropulu, *Higher-Order Spectra Analysis*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1993.

[37] T. Öberg, A. Karsznia, and K. Öberg, "Basic gait parameters: Reference data for normal subjects, 10–79 years of age," *J. Rehabil. Res. Develop.*, vol. 30, no. 2, pp. 210–223, Jan. 1993.

[38] A. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern Recognit.*, vol. 38, no. 12, pp. 2270–2285, Dec. 2005.

[39] L. Rong, Z. Jianzhong, L. Ming, and H. Xiangfeng, "A wearable acceleration sensor system for gait recognition," in *Proc. 2nd IEEE Int. Conf. Ind. Electron. Appl. (ICIEA)*, May 2007, pp. 2654–2659.

[40] T. Hoang, D. Choi, and T. Nguyen, "Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme," *Int. J. Inf. Secur.*, pp. 1–12, Jan. 2015, doi: dx.doi.org/10.1007/s10207-015-0273-1.

Sebastijan Sprager, photograph and biography not available at the time of publication.

Matjaz B. Juric, photograph and biography not available at the time of publication.