Pattern Recognition Letters
journal homepage: www.elsevier.com

A Survey on Biometric Recognition using Wearable Devices

Emanuele Maiorana [a]

[a]Roma Tre University, Via V. Volterra 62, 00146, Rome, Italy

Article history:
Received 10 October 2021
Received in final form 20 January 2022,
Preprint submitted to Elsevier

2000 MSC: 68T10

Keywords: Biometrics, Wearable Devices

ABSTRACT

Thanks to their ability to monitor physical activity and health-related parameters, wearable devices are becoming more and more popular. In addition to what they already offer, an interesting capability achievable through such devices is biometric recognition. The physiological traits recorded by wearable devices may in fact possess distinctive properties which could allow to recognize their legitimate users, and detect unauthorized usage. In this paper, the most recent advances accomplished in this field are reviewed, and a critical analysis on the current state of the art, as well as on the issues still open, is provided.

1. Introduction

The global market of wearable technology is rapidly expanding, with a compound annual growth rate (CAGR) of 12% (Ometov et al., 2021). Earphones, wristbands and smartwatches are the most popular of these devices, with headbands, chestbands, goggles and smart clothing also spreading. The interest in these tools is mainly due to the possibility of using them as activity trackers, monitoring the acquired data for fitness or health purposes. Furthermore, thanks to the possibility of integrating computing and communication capabilities within them, wearable devices can be used to exchange or share data with other equipment in an Internet of Things (IoT) framework, thus enabling value-added services such as smart payment.

In addition to the ways in which wearable technologies are currently employed in real-life scenarios, it has also recently been proposed to use them to perform automatic biometric recognition. Such possibility relies on the ability of wearable devices to capture several physical, behavioral or cognitive traits, from which distinctive features can be extracted and used to discriminate legitimate from unauthorized subjects.

In more detail, wearable instruments can be for instance employed to capture biometric data from subjects other than those who wear them. As an example, this is the case of face-based recognition systems relying on body-worn cameras (BWC), and employed for surveillance, situational awareness, or law enforcement purposes (Almadan and Rattani, 2021). It has yet to be noted that this kind of use of wearable sensors can incur privacy violations, as the interested subjects may not be aware or may not want to be recorded, and could be therefore employed only by certain categories of subjects, such as law officers, and under specific regulations[1].

On the other hand, a much more extensive and diversified use could be achieved by designing biometric systems that employ wearable sensors to recognize their own wearers. Under this framework, the traits of the considered subjects could be collected anywhere and anytime, without asking the interested users to interact with specific fixed infrastructures as in traditional desktop recognition systems, granting a convenient and user-friendly acquisition procedure. Collected data could be then either processed within the employed device, or transmitted to a server where the recognition process have to be carried out. Wearable devices could in fact autonomously dialogue with interconnected systems to allow their users physical access to certain areas or goods, or logical access to specific services. Such possibility could enable the design of novel applications or the improvement of existing ones, such as the recognition of the approaching owner of a car without the need for keys, or the authentication of the applicant for an electronic payment.In addition to a greater ease of use with respect to standard desktop biometric systems, recognition approaches relying on wearable devices could also guarantee improved security, because the physiological traits recorded by wearable sensors typically cannot be captured at a distance, being therefore hard to steal and replicate, and inherently provide liveness detection.

In order to shed light on the state of the art of biometric systems using wearable devices to recognize their owners, this paper covers the most recent advances on the considered topic, and analyzes the associated open issues. An analogous survey has been presented by Blasco et al. (2016), where contributions on wearable biometrics up to 2015 have been categorized using a taxonomy based on the origin and type of the considered

**Corresponding author: Tel.: +39 0657337365
e-mail: emanuele.maiorana@uniroma3.it (Emanuele Maiorana)

[1]https://bja.ojp.gov/program/bwc/topics/privacy

traits, the location of the employed sensors, and the ability to perform continuous recognition. The present contribution updates and improves (Blasco et al., 2016) in the following terms:

- it covers in Section 2 all the biometric traits that can be recorded through wearable devices, and have been proposed till now to recognize their wearer, with half of the mentioned papers published in the past two years. In more detail, a major emphasis is given to studies carried out on data collected with prototypes or commercial off-the-shelf wearable devices, rather than to evaluations relying on medical-grade equipment. This choice is deliberately taken to focus on works where scenarios similar to real-life contexts, in terms of cost of the employed devices and conditions of the involved users, have been taken into account. It is worth remarking that measurements taken through consumer wearable devices are typically not as accurate as those attainable using instruments specifically designed for medical purposes, with consequences on the achievable performance (Bai et al., 2021). The results obtained in works relying on commercial wearable devices are therefore more indicative, with respect to those exploiting medical tools, of the actual recognition capabilities that can be attained in potential practical applications;
- it performs a critical evaluation of the current state of the art on wearable biometrics, analyzing in Section 3 the technology readiness level, expressed in terms of relevant properties of biometric recognition systems, of the approaches presented so far in literature;
- it suggests, in Section 4, aspects and research directions which should be investigated in the future to fully uncover the potential of biometric recognition relying on wearable devices for real-world applications.

It is worth mentioning that other surveys have dealt with the use of wearable devices for biometric recognition, as in (Sundararajan et al., 2019) where, however, aspects related to system networking, rather than on recognition approaches, have been mainly considered. General health-related sensing devices, not necessarily employed for biometric purposes, have been treated by Khan et al. (2020). Lastly, Liu et al. (2021) have reported a list of usable computational techniques, rather than specific approaches for biometric recognition, and did not mention some important biometric traits such as electrodermal activity (EDA), as well as relevant characteristics of the exploited databases.

2. Related Works

Biometric traits recordable by wearable devices and employed to perform recognition only occasionally, i.e., at specific moments, are listed in Section 2.1. Section 2.2 instead reports the approaches allowing to perform continuous recognition. For both classes, a categorization depending on the source of the exploited distinctive information is adopted. For each considered trait, the types of sensors used for its acquisition, namely electrical, optical, acoustic, chemical, or inertial, are specified. Table 1 summarizes the surveyed studies.

2.1. Occasional Recognition

The traits which can be employed for biometric recognition only while the involved subjects perform a specific activity, and those which cannot be acquired continuously due to limitations of current technology, are reviewed in this section.

2.1.1. Behaviour

The first wearable devices proposed to perform biometric recognition are inertial measurement units (IMUs) such as accelerometers and gyroscopes, worn by subjects while carrying out specific tasks. Gait is the most commonly investigated activity, with IMUs placed on arms, wrists, hips, thighs, and ankles (De Marsico et al., 2019). In addition to kinematic aspects, also kinetic information has been recently exploited, using custom insoles to measure the applied forces (Ivanov et al., 2020). Other exploited activities comprise typing (Rahman et al., 2020) and handwriting (Griswold-Steiner et al., 2019). IMUs have been also used to recognize people while executing generic gestures (Yoneda and Weiss, 2017), observing that activities involving large body movements are less distinctive, with respect to those requiring little body movements (Elkader et al., 2018). Obviously, all such approaches cannot be performed in the absence of any movement.

2.1.2. Voice

Recognizing people using their voice is an activity often performed by humans, and also one of the approaches most commonly adopted in automatic authentication systems. The availability of microphones in wearable devices such as smart glasses can be exploited to recognize who wears them as in (Peng et al., 2017), where the recognition performance achievable with either voice or gestures have been compared.

2.1.3. Muscle

Wearable devices can be exploited to detect, at the skin surface, the electric potential generated by cells in skeletal muscles, when activated by external or neurological stimuli. The collected signal, that is, the electromyogram (EMG), can be exploited to perform biometric recognition. A custom armband has been employed in (Raurale et al., 2021) to capture such electrical signals, and to recognize subjects performing specific gestures. It is also possible to sense the activity related to isometric contractions of finger muscles, without any observable gesture, as proposed by Jiang et al. (2021).

2.1.4. Fingerprint

Fingerprint is the trait most commonly employed for desktop and mobile biometric recognition, and it can also be captured by commercial wristbands with capacitive scanners such as Nymi[2] and Flywallet[3]. Yet, the employed paradigm requires users to touch the device while being recognized, with authentication validity then lasting as long as the wristband is worn.

2.1.5. Vein

Commercial products such as Biowatch[4] have been designed to capture wrist subcutaneous vein structures. A near-infrared (NIR) illuminator and a NIR camera are needed to acquire vein pattern images (Uhl et al., 2020). Limitations of current imaging technology allows to take proper recordings only when the optical sensor is far enough from the wrist. The recognition process can be thus performed only when the device is initially worn. Hence, although in principle continuous recognition could be achieved collecting vein patterns with wearable devices, solutions that can do that have yet to be developed.

[2] `https://www.nymi.com/`
[3] `https://www.flywalletpay.com/en`
[4] `https://biowatchid.com/`

Table 1: Summary of state-of-the-art approaches using biometric traits acquired through wearable devices for automatic people recognition.

Recognition Type	Origin	Trait	Paper	Database: Subjects	Database: Sessions	Database: Release	Device	Multiple conditions	Time for recognition	Feature	Comparator	Recognition Modality	Performance: EER/HTER	Performance: CIR
Occasional	Behavior	Gait	De Marsico et al. (2019)	175	2 in 6 months	Private	Commercial	No	5 steps	Time signal	DTW	OS Ident. & Ver.	8.3%	75.2%
			Ivanov et al. (2020)	59	1	Private	Prototype	No	15 s	Learned	CNN	CS Identification	-	93.3%
		Typing	Rahman et al. (2020)	49	1	Public[5]	Commercial	No	10 s	Statistical	MLP	CS Verification	6.9%	-
		Handwriting	Griswold-Steiner et al. (2019)	53	1	Private	Commercial	No	250 s	Learned	CNN+RNN	CS Verification	7.8%	-
		Gesture	Yoneda and Weiss (2017)	18	1	Private	Commercial	Yes	50 s	Statistical	RF	CS Id., OS Ver.	15.3%	88.3%
	Voice	Speech	Peng et al. (2017)	32	1	Private	Commercial	No	1 command	MFCC	SVM	CS Verification	4.9%	-
	Muscle	EMG	Raurale et al. (2021)	5	4 in 4 weeks	Private	Prototype	Yes	15 s	Statistical	MLP	CS Verification	6.0%	-
			Jiang et al. (2021)	22	3 in 9 days	Private	Prototype	No	3 s	Statistical	SVM	CS Verification	14.9%	-
Continuous	Heart	ECG	Ye et al. (2011)	5	over 6 months	Private	Commercial	Yes	6 heartbeats	Wavelet	SVM	CS Identification	-	70-100%
			Pourbabaee et al. (2018)	33	over 6 weeks	Private	Commercial	Yes	10 heartbeats	Learned	CNN	CS Identification	-	95.9%
			Chandrashekhar et al. (2020)	90	1	Public[6]	Commercial	Yes	1 heartbeat	MFCC	RF	CS Ident. & Ver.	1%	99%
			Lehmann and Buschek (2020)	20	6 in 6 days	Private	Commercial	Yes	3 heartbeats	Statistical	RF	CS Verification	21.9%	-
		PPG	Luque et al. (2018)	43	1	Private	Prototype	No	1 s	Learned	CNN	OS Verification	10.0%	-
			Sancho et al. (2018)	56	2 in 2 days	Public[7,8]	Prototype	No	30 hearbeats	Time signal	L2 dist.	OS Verification	21.5%	-
			Cao et al. (2020)	7	6 in 50 days	Private	Prototype	Yes	4 heartbeats	Statistical	RF	CS Identification	-	90-97%
			Donida Labati et al. (2020)	42	1	Public[8]	Prototype	No	20 s	Spectrogram	SVM	CS Ident. & Ver.	7.0%	94.8%
			Retsinas et al. (2020)	20	> 20 days	Public[9]	Commercial	Yes	10 min	Learned	CNN	CS Identification	-	55.8%
			Lee et al. (2020)	12	4 in 4 days	Public[10]	Prototype	No	8 s	Learned	CNN	CS Identification	-	95.7%
			Hwang et al. (2021)	100	3 in 17 days	Public[11]	Prototype	No	20 heartbeats	Learned	CNN+RNN	CS Identification	-	87.1%
			Yadav et al. (2021)	32	1	Public[11,12]	Prototype	Yes	8 heartbeats	Wavelet	LDA	CS Verification	2.61%	-
		PCG	Spadaccini and Beritelli (2013)	206	1	Public[13]	Prototype	No	4 s	PSD	GMM	CS Verification	13.6%	-
			Cheng et al. (2020)	40	1	Private	Prototype	No	1 heartbeat	Statistical	L2 dist.	CS Identification	-	97.5%
		SCG, GCG	Maiorana and Massaroni (2021)	10	1	Private	Commercial	Yes	5 s	Spectrogram	CNN	CS Identification	-	99.9%
	Respiration	BR	Chauhan et al. (2017)	10	3 in 7 days	Private	Commercial	Yes	1 breath	GFCC	GMM	CS Verification	5-15%	-
			Raji et al. (2020)	10	1	Private	Prototype	Yes	1 min	Statistical	MLP	CS Identification	-	99.8%
	Brain	EEG	Chuang et al. (2013)	15	1	Private	Commercial	Yes	5 s	Time signal	Cos. dist.	OS Verification	32.2%	-
			Nakamura et al. (2018)	15	2 in 15 days	Private	Prototype	No	60 s	PSD, AR	Cos. dist.	OS Verification	17.2%	-
			Arnau-Gonzalez et al. (2021)	21	3 in 2 weeks	Public[14]	Commercial	Yes	5 s	MFCC, AR	HMM	OS Verification	26.2%	-
	Eye	Iris	Li and Huang (2017)	10	1	Private	Prototype	No	10 pictures	Gabor feat.	Bin. dist.	OS Verification	0.0%	-
		EOG	Suzaki et al. (2019)	2	3 in 3 days	Private	Prototype	No	10 min	Statistical	n/a	n/a	n/a	n/a
	Skin	EDA	Piciucco et al. (2021)	17	2 in 1 week	Private	Commercial	Yes	10 s	Spectrogram	CNN	CS Identification	-	94.9%
		Odor	Yang and Lee (2018)	10	1	Private	Prototype	No	3 s	PCA	L2 dist.	CS Identification	-	96%
		Temperature	Enamamu et al. (2017)	30	6 days	Private	Commercial	No	3 s	Statistical	MLP	CS verification	2-5%	-
	Subcutan. tissues	MSP	Kim et al. (2018)	150	1	Private	Prototype	No	20 s	Optical val.	L2 dist.	OS Verification	0.2%	-
		Conduction	Schneegass et al. (2016)	10	1	Private	Prototype	No	23 s	MFCC	CNN	CS Ident. & Ver.	6%	97%
		Bioimpedance	Cornelius et al. (2012)	46	1	Private	Prototype	No	9 s	Statistical	SVM	CS Ident. & Ver.	17.5%	80%
		HBC	Nie et al. (2015)	20	8 in 4 days	Private	Prototype	No	n/a	S21 gain	SVM	CS Ident. & Ver.	0.24%	98%
		Antenna sens.	Saadat et al. (2021)	6	3 in 3 days	Private	Prototype	No	30 s	AR	MLP	CS Identification	-	98%

2.2. *Continuous Recognition*

Several human characteristics recordable by wearable devices possess distinctive features even when the involved subjects do not perform a specific activity, and can be thus exploited to perform continuous recognition. Most of such traits are controlled by the autonomic nervous system (ANS), and their usage for authentication purposes is consequently referred to as *cognitive biometrics* (Revett and de Magalhães, 2010).

2.2.1. *Heart*

The heart is the source of many biometric traits recordable by wearable devices and usable in recognition systems. The signal most commonly associated with heart activity is the electrocardiogram (ECG), obtained placing electrodes on a subject's skin to detect small electrical changes resulting from cardiac muscle depolarization and repolarization during each heartbeat. The vast majority of ECG studies for biometric recognition have exploited medical equipment for data acquisition, with multiple electrodes placed on the chest, wrists, and ankles. Nevertheless, recent approaches have collected ECG through wearable devices with only one or two electrodes, using chestbands (Lehmann and Buschek, 2020), armbands (Martinho et al., 2018), and also electronic textiles, that is, fabrics with embedded electronics (Ye et al., 2011; Pourbabaee et al., 2018). Commercial wristbands (Chandrashekhar et al., 2020) instead requires the involved subjects to touch the device with the opposing hand to acquire the desired ECG data, as it happens for the Nymi device or the Apple Watch[15].

Heart activity can be also described by a photoplethysmogram (PPG) using pulse oximeters, which illuminate at close distance the skin with either green, red, or infra-red (IR) light, and measure changes in the received radiation (Sancho et al., 2018). Since IR light is absorbed by the blood in vein vessels depending on levels of vasodilation, vasoconstriction, and oxygenation, both variations in blood volume pulse (BVP) due to the cardiac cycle (Yadav et al., 2021), and oxygen saturation (SpO2) using two different wavelengths (Donida Labati et al., 2020), can be measured by wearable devices exploiting optical PPG techniques. Furthermore, coarse metrics describing the cardiovascular activity (Ekiz et al., 2021) such as the heart rate (HR) and heart rate variability (HRV), and measures associated to the physical exertion during an activity such as the calories burned (Vhaduri et al., 2021) or the metabolic equivalent of task (MET), can be easily derived from PPG recordings. Typically, sensors capturing transmitted light are placed on fingertips (Hwang et al., 2021), while reflected light can be exploited by sensors placed on the wrist (Cao et al., 2020).

Acoustic devices (Spadaccini and Beritelli, 2013) have been employed to collect phonocardiograms (PCGs), with distinctive information extracted from the two main sounds of a cardiac cycle, the low-pitch S1 at the closing of mitral and tricuspid valves (systole) and the high-pitch S2 at the closing of aortic and pul-

[5] WISDM: https://www.cis.fordham.edu/wisdm/dataset.php
[6] ECG-ID: https://physionet.org/content/ecgiddb/1.0.0/
[7] MIMIC II: https://peterhcharlton.github.io/RRest/mimicii_dataset.html
[8] PRRB: https://peterhcharlton.github.io/RRest/capnobase_dataset.html
[9] PersonID: https://robotics.ntua.gr/person-id/
[10] IEEEPPG: https://zenodo.org/record/3902710#.YVoK333OM2w
[11] BioSec: https://www.comm.utoronto.ca/~biometrics/PPG_Dataset
[12] DEAP: https://www.eecs.qmul.ac.uk/mmv/datasets/deap/
[13] HSCT-11: http://www.diit.unict.it/hsct11/
[14] BED: https://zenodo.org/record/4309472#.YUsORX3OMuU
[15] https://www.apple.com/watch/

monic valves (diastole). Digital stethoscopes are traditionally placed on the chest to record PCGs, with small sound sensors recently used to improve acceptability (Cheng et al., 2020).

Besides electrical, optical, and acoustic devices, also IMUs have been used to extract discriminative information from cardiac cycles, detecting the vibrations caused by heart compressions and transmitted throughout the body, producing seismocadiograms (SCGs) using accelerometers or gyrocardiograms (GCGs) with gyroscopes (Maiorana and Massaroni, 2021).

2.2.2. Respiration

Breathing is an act controlled by the brain to supply oxygen to the blood and to remove carbon dioxide. Several studies highlight the existence of distinctive features in people's breathing rate (BR) (Vhaduri et al., 2021). While this trait has been typically acquired using acoustic devices such as microphones or earphones (Chauhan et al., 2017), also chestbands with pressure sensors have been employed to measure changes in the cross-sectional rib cage areas, caused by oscillations of lung volumes during inspirations and expirations (Raji et al., 2020).

2.2.3. Brain

Brain activity is the cognitive biometric trait *par excellence*. Discriminative features can be derived from non-invasive electrical measurements, known as electroencephalogram (EEG), taken on the subjects' head scalp. Such signals depend on the activity of pyramidal neurons in the outermost brain cortex layers, and possess different characteristics depending on the performed mental task. While most of studies on EEG biometrics have been performed using medical-grade acquisition devices, with dozens of electrodes and a low signal-to-noise ratio, relatively inexpensive sensors such as the single-electrode Neurosky MindSet (Chuang et al., 2013), or the Emotiv EPOC+ wireless headset with 14 channels (Arnau-Gonzalez et al., 2021), have been also employed. Moreover, innovative designs have been proposed to improve the collectability of EEG data, as in (Nakamura et al., 2018) where an in-ear sensor with two EEG channels has been used for people recognition.

2.2.4. Eye

Custom wearable devices have been build to capture biometric traits from the human eye. Cognitive signals in the form of electroocoulograms (EOGs), i.e., electric measurements of eye movements taken by sensing the voltage difference between cornea and retina, and depending on the subjects' eye blinking patterns, have been analyzed by Suzaki et al. (2019) placing electrodes on eyeglasses nose pads. Li and Huang (2017) have also proposed to collect the highly-distinctive characteristics of the iris at a close range by placing an IR camera over eyeglasses, although such approach severely hinders sight.

2.2.5. Skin

Our skin possess unique characteristics that can be used for biometric recognition purposes. A prominent skin-dependent cognitive trait, typically collected through wristbands, is the electrodermal activity (EDA), also known as galvanic skin response (GSR) (Blasco and Peris-Lopez, 2018). Injecting a small amount of direct current (DC), EDA measures the resistance of an electrical path along skin surface over time. The collected values reflect changes in the eccrine sweat gland activity, controlled by the sympathetic branch of the ANS, therefore dependent on subjects' cognitive and emotional states on a subconscious level, making EDA a reliable measure of physiological arousal and stress. Typically, high-frequency EDA components are indicated as *phasic*, while low-frequency ones are referred to as *tonic* (Piciucco et al., 2021).

Skin sweat glands, more specifically apocrine ones, are also responsible for the secretion of chemical compounds producing odorant substances. Body odor has been investigated as a cognitive biometric trait too, exploiting wearable electro-chemical sensors usually placed close to armpits (Yang and Lee, 2018). The ANS also controls thermoregulatory processes by leveraging on blood flows, with direct effects on skin temperature. This latter is another cognitive characteristics easily recordable by wearable devices such as wristbands, from which distinctive features can be extracted (Enamamu et al., 2017).

2.2.6. Subcutaneous tissues

Besides the outer one, also subcutaneous tissues have been explored to derive distinctive features. Instead of cognitive traits depending on the ANS, physical properties are considered in these cases. In fact, anatomical characteristics such as bones, tendons, and ligaments greatly differ across individuals, and can be exploited for recognition purposes. The uniqueness of subcutaneous tissues have been for instance analyzed using multispectral skin photomatrix (MSP), an optical technique similar to PPG, yet using a wide set of wavelengths to illuminate a body portion such a wrist, and estimate the properties of tissues at different depths by measuring photon absorption of different lights (Kim et al., 2018). The absorption of acoustic signals has been evaluated as a potential biometric trait by Schneegass et al. (2016), analyzing the frequency changes made by the human skull to sounds released and received by smart glasses.

Similarly to EDA, a characterization of the properties of subcutaneous tissues can be obtained in terms of biompedance (Cornelius et al., 2012), that is, the body response to an externally applied electric current. Differently from EDA, where a DC current is used to create superficial circuits, alternating current (AC) is instead employed in this case, possibly using several electrodes to apply different frequencies, typically ranging from 1 kHz and 100 kHz (Cornelius et al., 2012).

Also body sensor networks have been investigated for biometric recognition. Within the context of human body communication (HBC) based on capacitive coupling, where the human body is used as a transmission medium to exchange messages between two sensors, the S21 transmission gain parameters has been employed by Nie et al. (2015) as a biometric identifier, leveraging on the uniqueness of body responses to different frequencies, ranging from 300 KHz up to 750MHz, when transmitting from one palm to the other. Even antenna sensitivity has been explored as a biometric trait, measuring the return loss of wearable patches working at 2.45 GHz, with the interaction depending on the subject's body tissues (Saadat et al., 2021).

3. Technology Readiness Assessment

As shown in Section 2, several physiological traits have been proposed to recognize the users of wearable devices. Unfortunately, not all these characteristics have been tested with the same level of detail. The following sections provides an overview about the maturity of the research on wearable biometrics, taking into account the most important aspects which have to be addressed before deploying real-world applications.

3.1. Universality and Distinctiveness

Universality and distinctiveness are the core capabilities a biometric trait should possess to be used in a recognition system. In order to evaluate these properties, datasets with samples taken from multiple subjects are typically collected, and authentication performance estimated over them. The size of such datasets is highly relevant to infer reliable information about the treated characteristics, especially for systems tested in identification modality. Unfortunately, the number of subjects involved in studies on wearable biometrics is rarely adequate. As shown in Table 1, more than 30 users have been considered only in works on voice, handwriting, ECG, PPG, PCG, temperature, and bioimpedance, while more than a hundred of subjects have been exploited only in a handful of studies on gait (De Marsico et al., 2019), PPG (Hwang et al., 2021; Vhaduri and Poellabauer, 2019), PCG (Spadaccini and Beritelli, 2013), and MSP (Kim et al., 2018). Until appropriate tests will be carried out on databases with a large number of subjects, the reliability of studies on wearable biometrics will remain questionable.

It has also to be observed that, even if tested over small databases, several traits have shown very limited distinctiveness, with equal error rates (EERs) often greater than 10%. Such behavior is mainly due to intrinsic characteristics of the considered traits, but also to limitations of the employed wearable devices. In fact, as already remarked, the accuracy of these latter is typically much lower than that of medical equipment (Vhaduri et al., 2021), and also than that of mobile devices such as smartphones (Yoneda and Weiss, 2017), with negative consequences on the feasibility of extracting effective features from the collected data.

3.2. Collectability and Acceptability

Collectability and acceptability of biometric approaches typically depend on the technology employed to record the considered traits, and improve with the usage of comfortable and unobtrusive commercial devices. Table 1 shows that prototype acquisition devices, often relying on Bitalino (Blasco and Peris-Lopez, 2018) or Arduino platforms (Yang and Lee, 2018), have been employed in most of the performed studies. Yet, commercial devices have been used to record behavioural characteristics from gait (De Marsico et al., 2019) or gestures (Yoneda and Weiss, 2017), heart signals such as ECG (Pourbabaee et al., 2018), PPG (Retsinas et al., 2020), and SCG (Maiorana and Massaroni, 2021), respiration (Chauhan et al., 2017), EEG (Arnau-Gonzalez et al., 2021), EDA (Piciucco et al., 2021), and temperature (Enamamu et al., 2017). Interestingly, more than one of these traits can be simultaneously acquired using a single device, as it happens with Fitbit[16] and Empatica E4[17].

3.3. Permanence

An aspect often neglected in biometric studies regards the permanence of distinctive features in the employed traits. Actually, it is well-known that recognition results computed by comparing data from distinct sessions are notably worse than those accomplished on single-session datasets (Sancho et al., 2018), mainly due to aging effects occurring in all biometric traits. When dealing with wearable biometrics, the permanence of distinctive features may be also affected by personal habits such as those concerning diet, and by the dependency of the collected data on the placement of on-body sensors, being it is very unlikely to attach them always at the very same position.

Longitudinal tests have been conducted in at least one paper for most of the traits mentioned in Section 2. When data captured during more than a session are available, the results in Table 1 are referred to cross-session comparisons. It has yet to be observed that time spans larger than one week between acquisition sessions have been considered only for gait (De Marsico et al., 2019), EMG (Raurale et al., 2021), ECG (Ye et al., 2011), PPG (Retsinas et al., 2020; Cao et al., 2020; Hwang et al., 2021), and EEG (Arnau-Gonzalez et al., 2021). For the other characteristics, there is no evidence that recognition could be reliably accomplished one week after enrolment. It is also worth remarking that, even when recordings from multiple sessions are available, tests have been often performed by randomly dividing data into training and testing subsets, without considering any temporal information (Pourbabaee et al., 2018; Nie et al., 2015; Lee et al., 2020). Such approach does not allow to properly take into account longitudinal aspects, and should be therefore avoided.

Beyond checking whether their distinctive features remain stable over time, biometric traits acquired to perform continuous recognition should also be tested to assess whether it is actually feasible to recognize a subject regardless of the specific activity carried out. Although biometric traits have been often collected considering different conditions, only a limited set of well-coded activities such as sitting, standing, lying down, or walking, has been typically taken into account (Luque et al., 2018; Retsinas et al., 2020). In such controlled scenarios, tests are performed with the assurance of having available, as enrollment data, acquisitions taken in the same conditions encountered during recognition. If this is not the case, notable performance worsening typically happens (Maiorana and Massaroni, 2021). In order to generalize the proposed approaches, multi-conditions scenarios can be handled using a two-stage recognition process, during which the performed activity has to be first classified, and then a recognition model specific for that condition is employed (Yoneda and Weiss, 2017). It has also to be observed that physiological data could exhibit different characteristics even when collected in sessions characterized by the same recording conditions, as it happens for example after making a physical effort (Blasco and Peris-Lopez, 2018).

Conversely, recordings taken in the wild, without requiring the involved subjects to perform specific activities, have been considered only for ECG (Ye et al., 2011; Pourbabaee et al., 2018; Lehmann and Buschek, 2020), PPG (Yadav et al., 2021), and EDA (Piciucco et al., 2021) traits. Notable variations in the achieved recognition performance can be obtained in such unsupervised scenarios, due to the possible discrepancies of physiological characteristics employed for enrolment and authentication. Furthermore, in addition to the performed activity, several traits recorded by wearable devices may be also dependent on the subject's emotional state, and such influence is worthy of proper investigation, as done for PPG by Yadav et al. (2021).

[16] https://www.fitbit.com

[17] https://www.empatica.com/research/e4/

Table 2: Summary of state-of-the-art approaches using multi-modal biometric traits acquired through wearable devices for automatic people recognition.

Traits	Paper	Database			Devices		Multiple	Time for	Fusion	Feature	Comparator	Recognition	Performance	
		Subjects	Sessions	Release	Type	Number	conditions	recognition	level			Modality	EER/HTER	CIR
ECG, PPG, EMG, EDA, BR, Temp.	Diaz Alonso et al. (2016)	25	2	Private	Prototype	6	No	1 min	Feature	Statistical	SVM	CS Identification	-	92%
PPG, BR, Temp.	Mosenia et al. (2017)	37	1	Public[7]	Prototype	3	No	1 min	Feature	Statistical	SVM	CS Verification	2.6%	-
ECG, PPG, EDA	Blasco and Peris-Lopez (2018)	25	1	Public[18]	Prototype	3	Yes	20 s	Feature	Statistical	GMM	OS Verification	1.9%	-
ECG, PPG	Martinho et al. (2018)	53	2 in 8 weeks	Private	Prototype	2	Yes	1 heartbeat	Decision	Time Signal	L2 dist.	OS Verification	13%	-
ECG, BR, EDA	Bianco and Napoletano (2019)	37	1	Public[19]	Commercial	2	No	60 s	Feature	Learned	CNN	CS Identification	-	90.5%
Gait, PPG	Vhaduri and Poellabauer (2019)	400	over 17 months	Private	Commercial	1	Yes	5 min	Feature	Statistical	OC-SVM	OS Verification	20-30%	-
Gait, PPG, BR	Vhaduri et al. (2021)	10	1	Private	Commercial	2	Yes	10 min	Feature	Statistical	OC-SVM	OS Verification	19.5%	-
Gait, PPG, EDA, Temp.	Ekiz et al. (2021)	74	over 5 days	On request	Commercial	1	Yes	1 min	Feature	Statistical	CNN+RNN	CS Verification	9.3%	-

3.4. Data Processing

As for most pattern recognition systems, the typical processing pipeline of wearable biometric recognition includes preprocessing, feature extraction, and classification. During preprocessing, the acquired traits, typically temporal sequences of multidimensional data, are first filtered, with common choices for this stage including notch filters, followed by band-pass Butterworth filters to cancel DC components and frequencies above the range of interest.

The treated signals are then commonly divided into overlapping frames, whose duration can be fixed or depending on specific signal characteristics, such as the cardiac cycle for heart-related signals. Individual frames are then separately processed to extract distinctive information, traditionally in the form of hand-crafted features. For instance, statistical features such as the mean, maximum, minimum, and standard deviation over predefined intervals have been often computed (Lehmann and Buschek, 2020). The power spectral density (PSD) over selected frequency ranges (Nakamura et al., 2018), together with its derivations such as mel-frequency cepstral coefficients (MFCCs) (Schneegass et al., 2016), Gammatone Frequency Cepstral Coefficients (GFCC) (Chauhan et al., 2017), or spectrogram (Donida Labati et al., 2020), have been also employed. Time-dependent representations have been instead used by either directly exploiting the collected waveforms (Sancho et al., 2018), employing modelizations such as the autoregressive (AR) one (Saadat et al., 2021), or resorting to time-frequency domains such as wavelets (Ye et al., 2011).

Comparison between enrolment and probe data have been performed relying on classical machine learning approaches such as support vector machines (SVMs) (Jiang et al., 2021), decision trees like random forest (RF) (Cao et al., 2020), hidden Markov models (HMMs) (Arnau-Gonzalez et al., 2021), Gaussian mixture models (GMM) (Chauhan et al., 2017), dynamic time warping (DTW) (De Marsico et al., 2019), or even simple distance computations (Nakamura et al., 2018). However, more and more frequently, deep learning strategies are being exploited to process biometric traits acquired using wearable devices. In this case, discriminative features are automatically derived either from the original signals (Hwang et al., 2021), or from intermediate representations (Schneegass et al., 2016). Common learning architectures include multi-layer perceptrons (MLPs) (Enamamu et al., 2017), convolutional neural networks (CNNs) (Luque et al., 2018), or combinations of CNNs and recurrent neural networks (RNNs) (Hwang et al., 2021). In most cases, custom CNN architectures have been used in the proposed studies (Pourbabaee et al., 2018), with fine tuning from networks trained for image classification tasks only recently exploited (Piciucco et al., 2021). Data augmentation has been also employed to improve the generalizability of the learned representations (Yoneda and Weiss, 2017; Hwang et al., 2021).

[18]https://www.dropbox.com/s/lei4a27fcgp0ygr/LowCostSensorsBiometrics.zip?dl=0
[19]https://osf.io/c42cn/

3.5. Multi-modality

Even if biometric traits captured by wearable devices can hardly guarantee recognition performance comparable with traditional approaches, multi-modality can be easily exploited in wearable biometrics. A summary of the most relevant multi-biometric proposals is given in Table 2. In most cases, the employed biometric traits are fused at feature level, either combining features extracted from individual characteristics, or jointly feeding them to CNNs. It is worth remarking that multi-biometric solutions using a single commercial device to simultaneously collect multiple physiological signals have been proposed (Vhaduri and Poellabauer, 2019; Ekiz et al., 2021).

3.6. Throughput

A relevant aspect of biometric systems using wearable devices is the time required to perform recognition. As mentioned in Section 3.4, the collected data are commonly divided into frames employed as authentication probes. Frame duration is typically in the order of some seconds, a bit less in case individual heartbeats are considered. In case the recognition rates achievable using such short segments are not satisfying, the information derived from multiple frames can be jointly exploited, for instance by fusing, through majority voting, the decisions taken over consecutive windows (Blasco and Peris-Lopez, 2018; Griswold-Steiner et al., 2019).

It may also happens that frame lenghts in the order of minutes have been used. Such long intervals have been considered to either capture enough discriminative information to perform recognition regardless the performed activity (Retsinas et al., 2020), or to deliberately use only coarse-grained biometric characteristics such as MET, in order to take into account limitations in terms of computational power and battery consumption of wearable devices (Vhaduri and Poellabauer, 2019).

3.7. Recognition Modality

Biometric recognition can be performed as either identification or verification. The former is a typical classification task, in which a probe sample has to be associated to an identity within a set of N users, with information from all the involved subjects acquired during enrolment and employed for 1-to-N comparisons. A closed-set (CS) identification is simulated considering, as probe samples, only traits acquired from the users available during enrolment. Conversely, in case not all probes belong to registered users, open-set (OS) identification is evaluated. In this latter case, the system should have a reject option available, in order to deal with subjects unknown during enrolment (De Marsico et al., 2019). Performance is commonly evaluated in terms of correct identification rate (CIR) in both scenarios.

On the other hand, verification comprises 1-to-1 comparisons, computing the similarity between a probe sample and the traits taken during the enrolment of the claimed identity only, and estimating performance in terms of EER or half-total error rate (HTER). Such task is often carried out employing binary classifiers, in which a model is estimated for each user during enrolment, and a binary decision regarding whether a probe sample can belong to the users' model is taken during recognition. In case this model is created using, as impostors' data, samples from all the available subjects, CS verification is performed. Otherwise, if this model is build using only data taken from the legitimate user, or employing, as impostors' data, samples from subjects not involved with further tests, OS verification is accomplished (Luque et al., 2018).

Real-life scenarios most commonly involve OS identification and verification. Yet, the vast majority of studies on wearable biometrics have been carried out on CS recognition modalities. Actually, OS conditions are much more difficult to manage than CS ones, with OS recognition performance significantly affected by the lower amount of information available during enrolment, which often imposes to use either simple distance-based classifiers (Sancho et al., 2018), or anomaly detectors such as one-class SVM (OC-SVM) (Vhaduri et al., 2021).

3.8. Interoperability

In order to train deep learning approaches, exploited in several recent works on wearable biometrics as mentioned in Section 3.4, a significant amount of data is typically required. Yet, as remarked in Section 3.1, data from a large number of subjects have been used only in few studies. In order to alleviate this potential issue, it could be beneficial to define methods exploiting knowledge derived from data extracted with a device other than the one currently in use. Cross-domain adaptation has been for instance investigated by Lee et al. (2020) for PPG signals. This aspect is still largely under-explored, although its practical applications would be extremely relevant.

3.9. Circumvention

Proper techniques should be designed to protect physiological data collected by wearable devices, especially if they are shared with external infrastructures for recognition purposes. Since information related to the users' health or behavioural aspects can be extracted from the considered traits, it would be recommendable to generate representations from which the original signals cannot be recovered. Furthermore, it could be useful to apply cancelable transformations to employ different versions of the same trait in distinct applications. A template protection scheme based on random projections for PPG signals has been for instance proposed by Cao et al. (2020), yet a proper investigation on how physiological data collected by wearable devices can be effectively secured is still missing.

4. Research Directions

Given the current state of the art, future research on wearable biometrics should focus on acquisition devices to be employed, data to be collected, and processing to be performed.

In order to improve collectability, acceptability, and accuracy of recorded data, technological developments in wearable technology must be constantly monitored, in order to identify solutions that may ameliorate the existing ones, or that implement innovative data acquisition methods (Perez and Zeadally, 2021). For instance, novel commercial products have been recently introduced to make brain signals recording easier and more comfortable, using headbands[20] or earbuds [21]. Extremely compact devices, such as the recently introduced smart rings[22], could be also exploited for recognition purposes. Desired features of devices to be considered for wearable biometrics include the ability to collect multiple traits and long battery life, as in passive health tags[23]. Wearable sensing technologies such as electronic patches and smart tattoos (Alberto et al., 2020) could also be particularly interesting for wearable biometrics.

Concerns about uniqueness, permanence, and interoperability may be better addressed once new public databases will be available. The collected data should possess several properties which are currently rarely encountered in the already employed collections, such as being taken from a large number of subjects, during multiple acquisition sessions spanning several weeks, considering multiple subject conditions and emotional states, and recorded through multiple commercial devices, each possibly acquiring more than a single trait.

Furthermore, algorithms designed to perform recognition in open-set conditions, that are the ones most likely applicable to real-life scenarios, have to be investigated. Such studies are especially needed to design OS verification systems where deep learning strategies are employed. Toward this aim, novel training strategies, such as those involving siamese networks, have yet to be explored for wearable biometrics. Longitudinal studies have to be performed to evaluate the stability over time of distinctive characteristics, and to design template update strategies improving the achievable recognition rates for prolonged recognition. Efficient artifact detection and removal could improve activity-independent continuous recognition. Presentation attacks against wearable devices, and techniques for their detection, are still unexplored research areas. Effective template protection methods would be also extremely useful to protect the physiological signals recorded by wearable device. Transfer learning and domain adaptation should be investigate to achieve device interoperability. Designing algorithms that take into account the storage and computing capacity of low-power wearable devices (Torti et al., 2021), in order to hopefully perform on-board processing of the collected signal, is another goal that should be pursued.

5. Conclusions

Wearable biometrics is an active research area with interesting applications for real-life scenarios. Current state-of-the-art research has already shown that several traits could be exploited to effectively perform continuous recognition of the owners of the employed devices. Nevertheless, investigation in this field is still in its infancy, and in-depth studies are required to fully

[20] `https://brainbit.com/`
[21] `https://www.emotiv.com/blog/the-future-of-work-is-here-now/`
[22] `https://ouraring.com/`
[23] `https://www.spirehealth.com/`

reveal its potential, with the aim of improving collectability and accuracy by exploiting advances in wearable device technology, analyzing permanence and evaluating interoperability by collecting new datasets, and improving recognition performance and security by designing novel processing paradigms.

References

Alberto, J., et al., 2020. Fully untethered battery-free biomonitoring electronic tattoo with wireless energy harvesting. Scientific Reports 10.

Almadan, A., Rattani, A., 2021. Towards on-device face recognition in body-worn cameras, in: IEEE IWBF.

Arnau-Gonzalez, P., Katsigiannis, S., Arevalillo-Herraez, M., Ramzan, N., 2021. BED: A new dataset for EEG-based biometrics. IEEE IoT J .

Bai, Y., Tompkins, C., Gell, N., Dione, D., Zhang, T., Byun, W., 2021. Comprehensive comparison of apple watch and fitbit monitors in a free-living setting. PLoS One 16.

Bianco, S., Napoletano, P., 2019. Biometric recognition using multimodal physiological signals. IEEE Access 7, 83581–83588.

Blasco, J., Chen, T.M., Tapiador, J., Peris-Lopez, P., 2016. A survey of wearable biometric recognition systems. ACM Computing Surveys 49, 1–35.

Blasco, J., Peris-Lopez, P., 2018. On the feasibility of low-cost wearable sensors for multi-modal biometric verification. Sensors 18, 2782.

Cao, Y., Zhang, Q., Li, F., Yang, S., Wang, Y., 2020. PPGPass: Nonintrusive and secure mobile two-factor authentication via wearables, in: INFOCOM.

Chandrashekhar, V., Singh, P., Paralkar, M., Tonguz, O., 2020. Pulseid: The case for robustness of ecg as a biometric identifier, in: IEEE MLSP.

Chauhan, J., Hu, Y., Seneviratne, S., Misra, A., Seneviratne, A., Lee, Y., 2017. Breathprint: Breathing acoustics-based user authentication, in: MobiSys.

Cheng, X., Wang, P., She, C., 2020. Biometric identification method for heart sound based on multimodal multiscale dispersion entropy. Entropy 22, 1–21.

Chuang, J., Nguyen, H., Wang, C., B-Johnson, 2013. I think, therefore i am: Usability and security of authentication using brainwaves, in: FCDS.

Cornelius, C., et al., 2012. Who wears me? bioimpedance as a passive biometric, in: USENIX conference on Health Security and Privacy.

De Marsico, M., Mecca, A., Barra, S., 2019. Walking in a smart city: Investigating the gait stabilization effect for biometric recognition via wearable sensors. Computers & Electrical Engineering 80.

Diaz Alonso, A., Travieso, C., J.B. Alonso, M.D., 2016. Biometric personal identification system using biomedical sensors, in: IEEE CCIS.

Donida Labati, R., Piuri, V., Rundo, F., Scotti, F., Spampinato, C., 2020. Biometric recognition of PPG cardiac signals using transformed spectrogram images, in: IAPR TC4 Workshop on Mobile and Wearable Biometrics.

Ekiz, D., Y.S.Can, Dardagan, Y., Aydar, F., Kose, R., Ersoy, C., 2021. End-to-end deep multi-modal physiological authentication with smartbands. IEEE Sensors Journal 21, 14977–14986.

Elkader, S.A., Barlow, M., Lakshika, E., 2018. Wearable sensors for recognizing individuals undertaking daily activities, in: ISWC.

Enamamu, T., Clarcke, N., Haskell-Dowland, P., Li, F., 2017. Smart watch based body-temperature authentication, in: IEEE ICCNI.

Griswold-Steiner, I., Matovu, R., Serwadda, A., 2019. Wearables-driven freeform handwriting authentication. IEEE TBIOM 1, 152–164.

Hwang, D., Taha, B., Lee, D., Hatzinakos, D., 2021. Evaluation of the time stability and uniqueness in PPG-based biometric system. IEEE TIFS 16.

Ivanov, K., et al., 2020. Identity recognition by walking outdoors using multimodal sensor insoles. IEEE Access 8, 150797–150807.

Jiang, X., et al., 2021. Neuromuscular password-based user authentication. IEEE Transactions On Industrial Informatics 17, 2641–2652.

Khan, S., Parkinson, S., Grant, L., Liu, N., McGuire, S., 2020. Biometric systems utilising health data from wearable devices: Applications and future challenges in computer security. ACM Computing Surveys 53, 1–29.

Kim, H., et al., 2018. A wearable wrist band-type system for multimodal biometrics integrated with multispectral skin photomatrix and electrocardiogram sensors. Sensors 18, 1–19.

Lee, E., Ho, A., Wang, Y., Huang, C., Lee, C., 2020. Cross-domain adaptation for biometric identification using photoplethysmogram, in: IEEE ICASSP.

Lehmann, F., Buschek, D., 2020. Heartbeats in the wild: A field study exploring ECG biometrics in everyday life, in: CHI SIGCHI.

Li, Y.H., Huang, P.J., 2017. An accurate and efficient user authentication mechanism on smart glasses based on iris recognition. Hindawi MIS , 1–15.

Liu, S., Shao, W., Li, T., Xua, W., Song, L., 2021. Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey. Digital Signal Processing .

Luque, J., Cortes, G., Segura, C., Maravilla, A., Esteban, J., Fabregat, J., 2018. End-to-end photoplethysmography (PPG) based biometric authentication by using convolutional neural networks, in: EUSIPCO.

Maiorana, E., Massaroni, C., 2021. Biometric recognition based on heart-induced chest vibrations, in: IEEE IWBF.

Martinho, M., Fred, A., Plácido da Silva, H., 2018. Towards continuous user recognition by exploring physiological multimodality: An electrocardiogram (ECG) and blood volume pulse (BVP) approach, in: ISSI.

Mosenia, A., Sur-Kolay, S., Raghunathan, A., Jha, N., 2017. CABA: Continuous authentication based on bioaura. IEEE Tr. on Computers 66, 759–772.

Nakamura, T., Goverdovsky, V., Mandic, D., 2018. In-ear EEG biometrics for feasible and readily collectable real-world person authentication. IEEE Transactions On Information Forensics And Security 13, 648–661.

Nie, Z., Liu, Y., Duan, C., Ruan, Z., Li, J., Wang, L., 2015. Wearable biometric authentication based on human body communication, in: IEEE BSN.

Ometov, A., et al., 2021. A survey on wearable technology: History, state-of-the-art and current challenges. Computer Networks 193.

Peng, G., Zhou, G., Nguyen, D., Qi, X., Wang, Q.Y.S., 2017. Continuous authentication with touch behavioral biometrics and voice on wearable glasses. IEEE Transactions on Human-Machine Systems 47, 404–416.

Perez, A., Zeadally, S., 2021. Recent advances in wearable sensing technologies. Sensors 21.

Piciucco, E., Di Lascio, E., Maiorana, E., Santini, S., Campisi, P., 2021. Biometric recognition using wearable devices in real-life settings. Pattern Recognition Letters 146, 260–266.

Pourbabaee, B., Howe-Patterson, M., Reiher, E., Benard, F., 2018. Deep convolutional neural network for ECG-based human identification, in: CMBES.

Rahman, K., Alam, N., Musarrat, J., Madarapu, A., Hossain, S., 2020. Smartwatch dynamics: A novel modality and solution to attacks on cyber-behavioral biometrics for continuous verification?, in: IEEE ISNCC.

Raji, R., Adjeisah, M., Miao, X., Wan, A., 2020. A novel respiration pattern biometric prediction system based on artificial neural network. Sens. Rev. .

Raurale, S., McAllister, J., Del Rincon, J., 2021. EMG biometric systems based on different wrist-hand movements. IEEE Access 9, 12256–12266.

Retsinas, G., Filntisis, P., Efthymiou, N., Theodosis, E., Zlatintsi, A., Maragos, P., 2020. Person identification using deep convolutional neural networks on short-term signals from wearable sensors, in: ICASSP.

Revett, K., de Magalhães, S.T., 2010. Cognitive biometrics: Challenges for the future, in: ICGS3.

Saadat, W., Raurale, S., Conway, G., McAllister, J., 2021. Wearable antennas for human identification at 2.45 ghz. IEEE TAP in print.

Sancho, J., Alesanco, Á., García, J., 2018. Biometric authentication using the PPG: a long-term feasibility study. Sensors 18, 1525.

Schneegass, S., Y.Oualil, Bulling, A., 2016. Skullconduct: Biometric user identification on eyewear computers using bone conduction through the skull, in: CHI Conference on Human Factors in Computing Systems.

Spadaccini, A., Beritelli, F., 2013. Performance evaluation of heart sounds biometric systems on an open dataset, in: IEEE DSP.

Sundararajan, A., Sarwat, A., Pons, A., 2019. A survey on modality characteristics, performance evaluation metrics, and security for traditional and wearable biometric systems. ACM Computing Surveys 52, 1–36.

Suzaki, K., Shimizu, K., Oguchi, K., 2019. Feasible personal identification by eye blinking using wear able device, in: IEEE CSPA.

Torti, E., D'Amato, C., Danese, G., Leporati, F., 2021. A low power and real-time hardware recurrent neural network for time series analysis on wearable devices. Microprocessors and Microsystems 87.

Uhl, A., Busch, C., Marcel, S., Veldhuis, R., 2020. Handbook of Vascular Biometrics. Springer Nature.

Vhaduri, S., Dibbo, S., Cheung, W., 2021. HIAuth: A hierarchical implicit authentication system for IoT wearables using multiple biometrics. Access .

Vhaduri, S., Poellabauer, C., 2019. Multi-modal biometric-based implicit authentication of wearable device users. IEEE TIFS 14, 3116–3125.

Yadav, U., Abbas, S., Hatzinakos, D., 2021. Evaluation of PPG biometrics for authentication in different states, in: IEEE ICB.

Yang, B., Lee, W., 2018. Human body odor based authentication using machine learning, in: IEEE Symposium Series on Computational Intelligence.

Ye, C., Vijaya Kumar, B., Tavares Coimbra, M., 2011. Human identification based on ecg signals from wearable health monitoring devices, in: ISABEL.

Yoneda, K., Weiss, G., 2017. Mobile sensor-based biometrics using common daily activities, in: IEEE UEMCON.