A Survey of Wearable Biometric Recognition Systems

Jorge Blasco, Department of Electrical and Electronic Engineering, City University London
Thomas M. Chen, Department of Electrical and Electronic Engineering, City University London
Juan Tapiador, Department of Computer Science, Universidad Carlos III de Madrid
Pedro Peris-Lopez, Department of Computer Science, Universidad Carlos III de Madrid

The growing popularity of wearable devices is leading to new ways to interact with the environment, with other smart devices, and with other people. Wearables equipped with an array of sensors are able to capture the owner's physiological and behavioural traits, and thus are well suited for biometric authentication to control other devices or access digital services. However, wearable biometrics have substantial differences from traditional biometrics for computer systems, such as fingerprints, eye features, or voice. In this paper we discuss these differences and analyse how researchers are approaching the wearable biometrics field. We review and provide a categorization of wearable sensors useful for capturing biometric signals. We analyse the computational cost of the different signal processing techniques, an important practical factor in constrained devices such as wearables. Finally, we review and classify the most recent proposals in the field of wearable biometrics in terms of the structure of the biometric system proposed, their experimental setup, and their results. We also present a critique of experimental issues such as evaluation and feasibility aspects, and offer some final thoughts on research directions that need attention in future work.

CCS Concepts: •**Security and privacy** → **Biometrics;** •**General and reference** → *Surveys and overviews;*•**Computing methodologies** → *Machine learning algorithms;*

Additional Key Words and Phrases: Wearables, biometrics, biosignals, authentication, sensor, ECG, PPG, heart sound, accelerometer, machine learning

ACM Reference Format:
Jorge Blasco, Thomas M. Chen, Juan Tapiador, Pedro Peris-Lopez, 2015. A Survey of Wearable Biometric Recognition Systems *ACM Comput. Surv.* 0, 0, Article 0 (0000), 34 pages.
DOI: 0000001.0000001

1. INTRODUCTION

Wearable electronics was introduced to the public in 1977 in the form of a calculator watch. Before then, various head-mounted electronic devices and wrist wearables had been developed and commercialized with limited success. In the last few years, wearable devices have proliferated and found wide adoption, mainly through affordable fitness bands and general-purpose smartwatches such as Apple Watch and Android Wear. These allow user-installable apps similar to smartphones, which provide a broad range of new applications such as voice calls, contactless payments, opening cars or house doors, measuring vital signs, or facilitating healthcare. According to some estimates, wearable sales will rise to 100 million units by 2020 [Lee et al. 2014].

Equipped with an array of built-in sensors, wearables are very well suited for biometric authentication and offer a number of advantages over traditional biometric

Author's addresses: Jorge Blasco and Thomas M. Chen, Department of Electrical and Electronic Engineering, City University London, Northampton Square, EC1V 0HB, London, United Kingdom; Juan Tapiador and Pedro Peris-Lopez, Department of Computer Science, Universidad Carlos III de Madrid, Av. Universidad 30, 28911, Leganes, Spain.

DOI: 0000001.0000001

systems. An important advantage arises from the fact that wearable systems, by their nature, are always with the user, while traditional biometric systems are generally placed at a fixed location. Wearable biometric systems can effectively perform continuous authentication of the wearer. Another advantage is that the wearer is not required to share his biometric traits, generally considered to be very sensitive information, with a third party for storage, since all data can be stored inside the wearable device.

However, the adoption of wearables for biometrics also introduces new challenges. First, wearable devices can be easily lost or stolen due to their portable nature. More generally, owners can be subject to a new range of threats that do not usually affect traditional biometric systems. Second, wearable devices tend to use cheaper sensors and hardware than traditional biometric systems. Consequently, sensor readings have more noise, and combined with natural variability in the subject's state, accuracy is more of an issue for biometric applications. Furthermore, the authentication system will generally run in an insecure (and perhaps poorly managed) platform such as a smartphone. Finally, wearability incurs some costs in terms of computational power restrictions. Wearable devices have limited computational capabilities and must optimize the usage of their resources to maximize battery life while providing a quick response to biometric challenges.

This paper is intended for readers with some basic background in traditional biometrics systems who want to understand the specific issues that arise in the wearable domain. For surveys on traditional biometric methods, we refer the reader to [Jain et al. 1999; Maltoni et al. 2009; Szeliski 2010; Unar et al. 2014]. Our work is also different from previous surveys that focus on smartphone-based biometrics [Hoseini-Tabatabaei et al. 2013] (with different and usually fewer sensors) or medical devices that are invasive or unsuitable for everyday activities [Agrafioti et al. 2011].

In this paper we provide a review of the current state of wearable biometrics focusing on these specific differentiators. The structure of the rest of the paper is based on the functional components of a biometric system. Section 2 describes these components and details the differences between traditional and wearable biometrics. In section 3, we describe and categorize wearable sensors that can be used for biometric applications. Section 4 discusses different techniques available to process raw sensor signals and produce useful data inputs for the pattern recognition algorithms that underlie biometric systems. Section 5 describes and compares different signal similarity and pattern matching techniques used in biometric systems, including multi-modal systems. Our comparison, which includes a complexity analysis, is based on the most popular quality metrics for biometric systems, such as accuracy (H), equal error rate (EER) and false positive rate (FPR). Section 6 discusses additional issues specific to wearable biometrics, including the biosignal quality and the lack of publicly available datasets. This section systematically analyses how existing attack vectors for biometric systems affect wearable biometrics. Finally, Section 7 presents our main conclusions and discusses open problems and ideas for future work.

2. BIOMETRIC SYSTEMS

Biometric recognition can be viewed as a pattern recognition problem in which a user who wants to be authenticated provides a set of physiological and/or behavioural characteristics to match a previously registered signature (or reference). Biometrics takes advantage of the fact that humans have natural diversity and certain traits are unique for each individual.

Biometric systems, whether traditional or not, are usually composed of the three main functional components shown in Figure 1: (i) a sensor or set of sensors that capture raw biometric signals (r); (ii) a signal processing unit that pre-processes and extracts feature vectors from the signals ($P(r) \rightarrow s$); and (iii) a recognition system, which

usually includes a signature (or template) database, and implements a pattern recognition function $B(s)$ [Bow 2002].

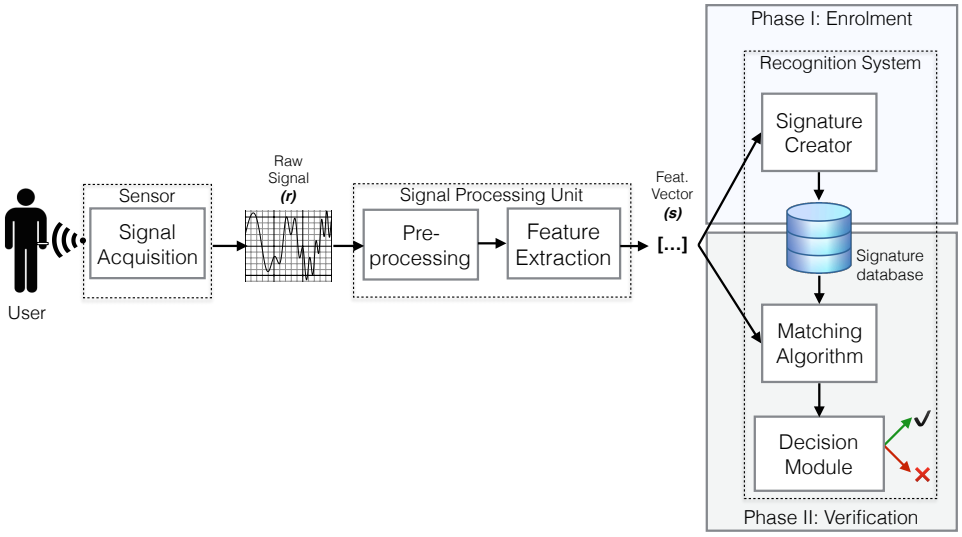


Fig. 1. Phases involved in a biometric verification system.

The matching phase depends on the mode of operation, either verification or identification. Biometric verification systems are configured by a sole user to verify its identity at a later stage. In biometric identification, the system is presented with a biometric signal (r) and must decide who is the owner of that signal from a pool of registered users.

A biometric system should fulfill the following requirements [Yampolskiy and Govindaraja 2010; Jain et al. 2000]:

— Performance: The system should respond promptly to queries with satisfactory accuracy [Ashbourn 2014].
— Acceptance: The system must be accepted by its intended users to be practical. If a sensor or device is not comfortable enough, it will not be used.
— Circumvention: The system should not be easy to circumvent. This implies that the system should be protected against unauthorized access to any of its components.

2.1. Traditional Biometric Systems

Traditional biometric system are often somewhat large and stationary (i.e., deployed at a fixed location). Typical applications involve the identification of users in order to control access to resources such as a computer system, a room, border control, or transportation. In these systems, the user needs to actively present himself to the biometric system to be recognized. For instance, Windows 10 includes a feature named *Windows Hello* [Belfiore 2015] that enables the user to authenticate using his face, iris, or fingerprint.

The stationary nature of these systems offers a series of advantages: (i) the sensors and other systems are less susceptible to deterioration and can be easily replaced; (ii) the different components of the system can make use of more computationally expensive processes, as they can make use of external sources of power; (iii) they can be

generally monitored through other external means (e.g., CCTV), thus increasing the effort required by an adversary; and (iv) they can be used for both identification and verification.

2.2. Wearable Biometric Systems

Figure 2 shows a wearable biometric system in which its primary user is in control of all the system components, including the signature database. A wearable biometric system requires the owner to constantly wear the sensor that captures his biosignals. The signal processing and recognition units can also be embedded in the same wearable device or can be located in a different smart device (e.g., a smartphone). The resources unlocked when the user is successfully recognised by the wearable might include the rest of the services provided by the wearable or a cryptographic key that can be used to prove the identity of the user to other systems [Rathgeb and Uhl 2011]. In any case, the process triggered after authentication is out of the scope of this survey.

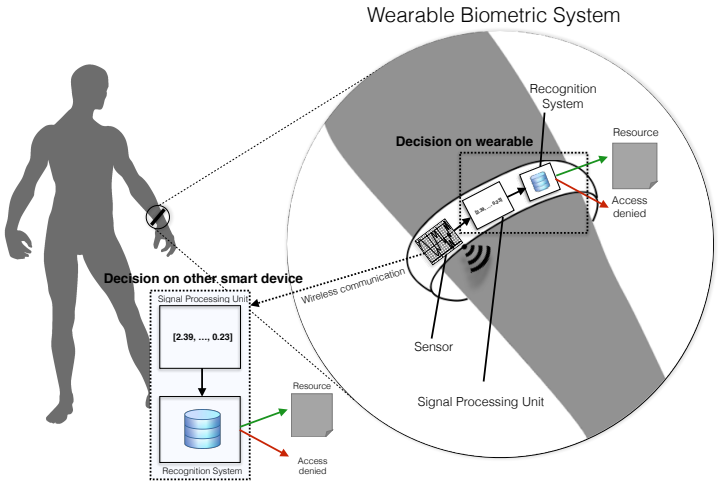


Fig. 2. Wearable biometric system where the decision can be done in the same wearable or allocated to a different smart device such as smart phone.

In this configuration, wearable sensors are capable of reading signals from the subject at any time. This enables the biometric system to continuously authenticate the wearer.

Wearable biometric systems are generally used for identity verification processes. In this case, the biometric traits of the subject never leave the control of the user; they are stored in the wearable or a smart device in his possesion. This avoids other entities accessing the biometric traits of the user provided that the devices are properly configured and protected against external attackers. An example of a commercial product implementing this philosophy is Nymi [Nymi 2015]. Nymi is a biometric verification wristband that includes one electrode in direct contact with the wrist and a second electrode that the user must touch with a finger from the opposite hand. When the user identity is verified, it has access to previously stored security tokens that can be used to authenticate against other devices, such as a car or a lock.

Table I. Differences between traditional and wearable biometric systems.

	Traditional	**Wearable**
Environment	Fixed location. Components can be separate. Allows to implement additional security measures but doesn't protect against a resourceful attacker.	Always with wearer. It can be lost. When this happens the adversary generally gains access to all the system components.
Types of recognition	On-request recognition	On-request & continuous recognition
Biometric processes	Verification & Identification	Verification
Signals	Mostly external to the body. Not suited for some signals that need to be taken with sensors in direct contact with the body	Signals that can only be captured by sensors that are in direct contact of certain parts of the body.
Sensor	Highly accurate and normally in noise-free environments	Inexpensive and subject to noise
Signal Processing Unit	Not constrained in computational capacity or power consumption. Can be placed in a different location	Embedded in the wearable or another smart device. Limited capacity and power.
Matching Unit	Not constrained in computational capacity or power consumption. Can be placed in a different location	Embedded in the wearable or another smart device. Limited capacity and power.
Signature Database	Not controlled by the subject.	Always with the subject. Templates are not shared with other parties.

2.3. Hybrid Biometric Systems

Some biometric systems may not fit in any of the two previously described categories. Some scenarios can require the sensor to be worn by the user, but other system components (for instance, the matching unit and the signature database) will not be in control of the user. We refer to these as *hybrid biometric systems*. One example of such hybrid systems arises in telecare services [Camara et al. 2015a]. Assume a patient who wears sensors that monitor some health-related signal, such as his heart activity. The information (in this case, the ECG signal) is sent to an external server and used for both analysis and biometric identification. The biometric system uses a sensor that is constantly worn by the user, but the matching unit and signature database are controlled by the healthcare provider.

Table I provides a summary of the main elements that differentiate traditional and wearable biometric systems. Hybrid biometric systems, depending on its configuration, can combine characteristics from both categories. The usage of one type of biometric system or another will strongly depend on the scenario, its intended application, and the biometric signal to be used. For example, biometric systems based on signals generated by the heart are easier to implement with wearable biometrics. In the same way, face and gait recognition systems are generally easier to implement with traditional biometric systems.

In some cases, both types of systems can be deployed for the same purpose. For instance, if the scenario requires the biometric system to distinguish between different users, a traditional biometric system could be used straight away. The same kind of authentication could be implemented with a wearable biometric system that protects specific user identifiers through biometric verification.

3. WEARABLE SENSORS FOR BIOMETRICS

Sensors measure the physical properties of the environment and translate them into data that can be handled by a computer system. When used for biometrics, sensors capture physiological and behavioral signals. Biometric signals captured by wearable sensors should be: universal, collectable, distinguishable, biologically constant, and difficult to imitate [Prabhakar et al. 2003; Jain et al. 2004; Yampolskiy and Govindaraja 2010]. Wearable sensors face a number of challenges to meet all of these re-

quirements. They must be located where they do not obstruct the wearer's daily activities. This limits the different signals that can be captured. For instance, sensors to obtain an electroencephalogram (EEG) have been left out of this study because they can obtain brain signals non-invasively [Marcel and Millán 2007] but require the user to wear a device that hinders the execution of everyday activities. Wearable sensors are also restricted in their power consumption. This reduces its accuracy, which is also affected by the noise they capture due to the unobtrusive monitoring performed by the system.

3.1. A Taxonomy for Wearable Sensors

Taxonomies provide insight about how the characteristics of elements that are being categorized are related. We offer a taxonomy that categorizes wearable sensors by five different dimensions (see also Figure 3):

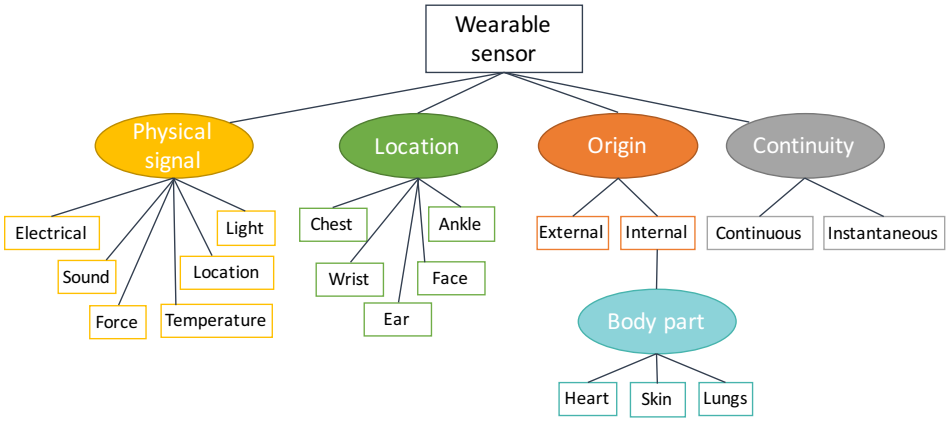


Fig. 3. Wearable sensor taxonomy for biometrics. Only wearable sensors are considered.

— *Origin*: If the signal captured by the sensors has been generated inside the body (e.g., the heart rate), we consider that the sensor reads signals internal to the body. Otherwise, the sensor gets the signal from external sources.
— *Body part*: Only for sensors with an internal source origin, this dimension specifies the part of the body that generates the signal read by the sensor.
— *Physical signal*: The kind of physical signal the sensor reads can be light, electricity, or force, among others. Some physical signals might be only available to sensors that measure signals from inside the body (e.g., the electrical activity of the heart). The same kind of physical signal can be used to measure different properties. For instance, electrodes can be used to measure the electrical activity of the heart, the brain waves, or the electrical activity of muscles in the body.
— *Location*: Describes where the sensor is placed in the body. Commonly used locations include the wrist, chest, and ankle. This dimension is not exclusive, since a sensor can placed in different parts of the body to measure the same physical signal from the same organ (e.g., the electrocardiogram can be measured in the chest or in the wrist among other locations).
— *Continuity*: Specifies if the sensor is able to continuously read the signal (e.g., an electrocardiogram), or if it needs to take instantaneous measures (e.g., a fingerprint).

Table II. Categorization of representative sensors in wearable devices based on our taxonomy.

Device	Sensor	Origin	Body Part	Signal	Location	Continuity
Apple Watch 2015	PPG	•	Vascular	Light	Wrist	△
	Accelerometer	◇	-	Force		△
	Microphone	• ◇	Respiratory	Sound		△
LG HRM Earphones 2014	PPG	•	Vascular	Light	Ear	△
	Accelerometer	◇	-	Force		△
Nymi Band 2015	ECG	•	Heart	Electrical	Wrist	△
	Accelerometer	◇	-	Force		△
CardioLeaf FIT	ECG	•	Heart	Electrical	Chest	△
Garmin Fenix 3 HR 2015	PPG	•	Vascular	Light	Wrist	△
	Accelerometer	◇	-	Force		△
	GPS	◇	-	Location		△ ■
Microsoft Band II 2016	PPG	•	Vascular	Light	Wrist	△
	Accelerometer	◇	-	Force		△
	GPS	◇	-	Location		△ ■
	Ambient Light	◇	-	Light		△
	Skin temp.	◇	-	Temperature		△
	UV ligth	◇	-	UV radiation		△
	Galv. Skin response	•	Skin	Electrical		△
	Microphone	• ◇	Respiratory	Sound		△
	Barometer	◇	-	Force		△

• Internal
◇ External
■ Instantaneous
△ Continuous

Depending on this dimension, the sensor can or cannot be used to build continuous authentication systems [Traore 2011].

Our taxonomy does not attempt to provide a categorization of devices that can be used for biometric recognition, since a single device may integrate multiple sensors to perform the biometric recognition or other activities. Table II presents a categorization of a variety of sensors found in commercial wearable devices based on our taxonomy. Most of the analysed devices are worn on the wrist and include at least one internal and external sensor. This is due to its optimal characteristics: it gives access to different signals, it can be easily worn, and the subject can interact with it.

For each sensor, we describe each of its dimensions. In most of the cases, the sensors embedded in the listed devices are not being used for biometric applications. However, in Section 5 we discuss how these same sensors can be used for biometric purposes and, therefore, we have decided to include them here in our examples. Due to its wearability, most of the sensors are able to provide continuous measurements. This is a major difference with respect to traditional biometric systems, where the user authenticates once.

In the rest of this section we describe the most predominant wearable sensors currently available. Sensors have been categorized using the *physical signal* dimension of our taxonomy.

3.2. Light Sensors

These sensors provide the amount of light sensed in the environment. Depending on the sensor resolution, they can be used to measure just the intensity of light–as, for example, in the case of photoplethysmographic (PPG) sensors–, or provide full images, such as in the case of fingerprint readers or cameras.

3.2.1. Photoplethysmographic Sensor. A PPG sensor measures blood volume changes within the microvascular bed of the tissue [Tamura et al. 2014]. PPG sensors use a light source to illuminate the tissue. Photodetectors within the sensor measure the variations in the intensity of absorbed or reflected light when blood perfusion varies [Allen 2007].

Raw PPG waveforms (Figure 5a) are used to continuously monitor biosignals such as the arterial blood oxygen saturation (SpO_2), heart rate (bpm) [Aoyagi and Miyasaka 2002], blood pressure, and stroke volume [Romano and Pistolesi 2002]. The unique characteristics of each person vascular system can lead to unique features being present in the PPG signal waveform, as found by [Lee and Kim 2015; Reşit Kavsaoğlu et al. 2014].

PPG sensors have become very popular thanks to fitness trackers and smartwatches such as Fitbit Charge HR [FitBit 2015], Apple Watch [Apple 2015], and some earphone models that measure the heart rate from the ear [LG Electronics 2014]. PPG sensors are also available in the form of open hardware platforms [World Famous Electronics 2012; Alves et al. 2013].

3.2.2. Fingerprint reader. Fingerprint readers capture the ridge pattern of a finger.

The fingerprint pattern is a physiological signal with a large body of research works describing its usefulness as a biometric measure. This survey focuses on newer and less consolidated biometric sensors. For a more detailed description of the different fingerprint scan and matching techniques the reader is referred to Maltoni et al. [2009].

Fingerprint readers are being increasingly deployed in most modern smartphones to provide authentication features and enable mobile payments. However, at the time of writing this survey fingerprint readers have not made it into any wearable devices.

3.2.3. Camera. Digital cameras are embedded in smartphones, smartglasses, and many other commodity electronic devices. A digital camera pointing to a person can capture physiological features such as the face or other body features [Kim and Hong 2008; Tao and Veldhuis 2006; Kittler et al. 2005; Bowyer et al. 2008; Introna and Nissenbaum 2010].

The main biometric domains of digital cameras are gait and face recognition. Artificial vision techniques can be used to detect gait and other behavioural information [Sarkar et al. 2005]. Face recognition techniques have been widely studied in the past and are commercially available in many smartphones and computer systems. A detailed review of proposals focused on face recognition is given in [Jafri and Arabnia 2009]. Camera-based biometric systems require the camera to be placed distant from the person to be recognized, which hinders its wearability.

3.3. Force Sensors

This kind of sensors measure the force that affects the measurement device, whether it is originated by movement (3-axes accelerometer), the Coriolis force (gyroscope), the Earth magnetic field (magnetometer), or air pressure (barometer).

3.3.1. Three Axes Accelerometer. An accelerometer measures the force that is affecting the object it is attached to. Accelerometers are widely used in smartphones and other electronic devices to detect device orientation and serve as input in motion-based games. Commonly used accelerometers measure g-force (1 g is 9.81 m/s^2) in the three axis: x, y and z (Figure 4a).

Miniaturization has enabled the construction of inexpensive and tiny accelerometers that can be embedded in almost any electronic device, including smartphones, smartwatches, and a variety of fitness trackers that can be worn on the wrist, hips, or ankles. Forces measured by an accelerometer when they are produced by muscu-

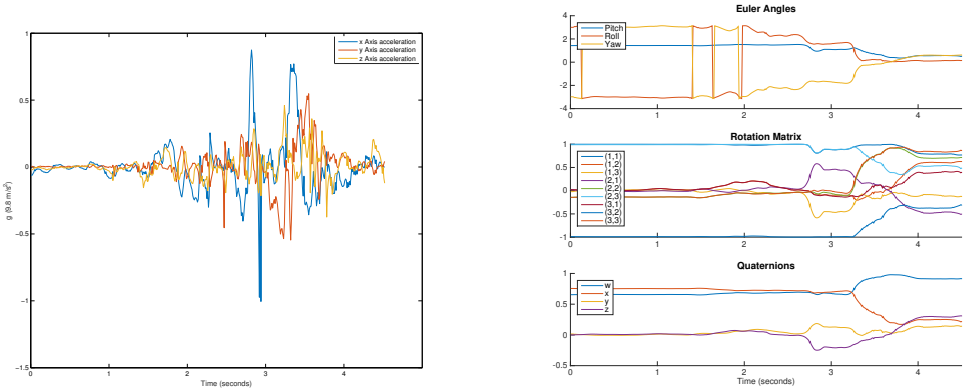
lar induced movement of a body part are signals that depend on the user physiology and behaviour. In most works, accelerometer data has been used to recognise subjects based on their gait patterns [Lu 2014; Meharia and Agrawal 2015; Ho et al. 2012; Nickel et al. 2012].

3.3.2. Magnetometer. A magnetometer measures the strength of the magnetic field in the three (x, y, and z) axes. This data can be used to derive the strength and direction of the Earth's magnetic field. Digital magnetometers are small and inexpensive, and thereby suitable for embedding in almost any electronic device, including smartphones, smartwatches, and fitness trackers such as the Microsoft Band [Microsoft 2016].

Electrical activity of the human body does not generate perceptible changes in the magnetic field. However, the measure offered by a magnetometer can be used to derive the heading of the subject wearing it. In this way, the magnetometer can be used as a behavioural biosignal measurement device.

3.3.3. Gyroscope. Gyroscopes measure attitude and rotation. Attitude is the orientation of the gyroscope relative to a point in space. By measuring changes in attitude, gyroscopes can also measure its rotation rate. The orientation of a body provided by a gyroscope can be represented in three different representations (shown in Figure 4b):

— *Euler angles* measure the rotation angle of the device against three different axis that pass through the gyroscope.
— A *rotation matrix* describes the rotation of a body in the Euclidean space as a matrix.
— *Quaternions* are a numeric system described by Hamilton in 1843. A quaternion is composed of four values: three of them represent the coordinates for the axis of rotation and the last value represents the angle rotated through [Shoemake 1985].



(a) 3 Axis accelerometer. (b) Gyroscope.

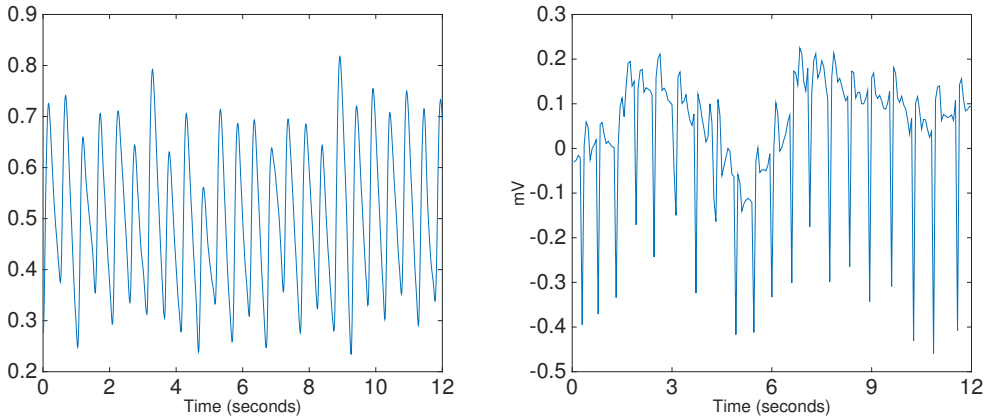
Fig. 4. Motion data generated in a smartphone while pulling it out of the pocket.

Gyroscopes are generally embedded in the same chip as accelerometers. Depending on its positioning, a gyroscope can measure the attitude of different body parts, providing behavioural biometrics about the subject.

3.4. Electrical Sensors

In humans, an electrical sensor measures the electrical activity of some parts of the body (e.g., electrocardiogram for the heart) or how a current changes when it is applied to the body (skin conductance).

3.4.1. Electrocardiogram sensor. An electrocardiogram (ECG) sensor consists of at least two metal electrodes that must be in direct contact with the skin. ECG sensors measure the electric activity of the heart (Figure 5b) [Catalano 2002].



(a) Sample PPG signal.

(b) Sample ECG signal.

Fig. 5. PPG and ECG signals extracted from Physiobank database [Goldberger et al. 2000; Saeed et al. 2011].

Medical ECG equipment generally uses three, five, or ten electrodes placed across the chest, wrists, and ankles. This configuration is not suitable for wearable devices. Fitness chest straps and ECG t-shirts [Clearbridge Vitalsigns 2016] use just two electrodes positioned across the chest to measure ECG and capture the heart beat. In a similar way, ECG sensors can be worn on the wrist [Mills and Homayoun 1994]. As opposed to chest straps, wristband ECGs cannot be used to obtain a continuous signal without interfering with daily activities. The unique features of each persons' heart are captured by the ECG signal, providing a physiological signal that has been used in several biometric studies [Derawi 2015; Pasero et al. 2015; Sidek et al. 2014; Camara et al. 2015a]. However, it remains an open challenge to validate if these features remain constant over long periods of time or change due to ageing.

3.4.2. Galvanic skin response sensor. A galvanic skin response (GSR or skin conductance) sensor measures the electrical conductance of the skin [Nourbakhsh et al. 2012]. GSR sensors can be placed in any part of the body but require direct contact with the skin. A GSR sensor is composed of two electrodes placed about an inch apart. The GSR sends a small, human imperceptible, amount of electrical current through one electrode and measures the intensity of the current received on the other.

The skin conductance varies depending on the amount of moisture (induced by sweat) in the skin. Sweating is controlled by the sympathetic part of the nervous system, so it cannot be directly controlled by the subject. The skin conductance can be used to determine body response against physical activity, stress or pain. The body response against these stimulus differs from person to person [Kurniawan et al. 2013].

3.5. Temperature Sensors

Skin temperature sensor works in a way similar to an infrared camera. A thermopile captures infrared energy and transforms it into a digital signal that represents the temperature. Skin temperature sensors are usually placed in a very short distance or in direct contact with the skin.

The skin temperature value depends on the part of the body where the measurement is made [Ramanathan 1964; Venable et al. 2013]. The miniaturization of technology has allowed the development of small skin temperature sensors that can be embedded in almost any electronic device, but they are generally deployed in high-end fitness trackers such as the Microsoft Band.

3.6. Sound Sensors

A microphone translates sound waves that travel through air into an electrical signal. Microphones are generally inexpensive and can be produced in very small sizes, so they can be embedded in almost any electronic device.

Microphones can be produced with different sensitivities to capture different sounds. For the purpose of biometrics, most commercial microphones are prepared to capture human voice at a reasonable distance (60 db at 1 meter). A person's voice is defined by the physiological characteristics of his respiratory system [Atkinson 1978]. However, voice can sometimes be mimicked so it is also considered a behavioural biometric signal [Revett 2008]. Vocabulary, style, syntax, and other features of speech are also considered behavioural biometric attributes. In addition to standard microphones, medical microphones such as digital stethoscopes can gather low power sounds emitted by the heart when placed in the chest [Wang et al. 2009].

3.7. Location Sensors

The Global Positioning System (GPS) consists of 32 (originally 24) satellites and any number of GPS receivers located on the Earth's surface [Braasch and Van Dierendonck 1999]. A GPS receiver uses the signal from four different line-of-sight satellites to triangulate the location of the device offering its coordinates (longitude and latitude).

GPS receivers provide only behavioural information about the subject's location. GPS receivers can be embedded in almost any electronic device, but are generally included in high-end smartwatches [Garmin 2015] and fitness trackers. Prolonged usage of the GPS antenna can rapidly drain small batteries [Bulusu et al. 2000].

4. SIGNAL PROCESSING UNIT

Measurements obtained by sensors are generally affected by noise and changes in physical conditions. The signal processing unit receives a raw signal r, amplifies it (if required), and extracts a feature vector s that can be used by the rest of the biometric system.

4.1. Pre-Processing

Sensor configuration, differences in timing measurements, and the technical limitations of sensors introduce noise and errors in the captured biosignals. Pre-processing attempts to reduce noise and errors, normalizes the data, and prepares the raw signal for the feature extraction process. The use of specific pre-processing techniques greatly depends on the domain and scenario. The most common pre-processing techniques are normalization, smoothing, interpolation, and segmentation. For a more detailed description of them, we refer the reader to [Wei 1994; Thévenaz et al. 2000; Ifeachor and Jervis 2002].

4.2. Feature Extraction and Selection

The goal of feature extraction is to reduce the noise, redundancy, and dimensionality of a signal so that classification operates on only significant information. With feature extraction, a signal can be compared to others in the time, frequency, and other domains defined by the extracted features. There are two main approaches for extracting features from raw data [Guyon 2006]. The domain-driven approach extracts features from the data by using knowledge from the problem domain. The automatic-driven approach uses statistics and other techniques to automatically extract features. The number of extracted features generally determines the computational cost of the matching process. Increasing the number of features may also introduce unnecessary noise that reduces the accuracy of the matching algorithm [Kira and Rendell 1992]. Section 4.2.3 describes some of the mechanisms often used to evaluate and reduce the dimensionality of features in biometric processes.

4.2.1. Domain-based features. Domain knowledge-based features are able to summarise the relevant information in a raw signal into a reduced set of features. These features can be based on fiducial points of the signal or other domain characteristics. Examples of domain-based features are ECG [Biel et al. 2001] and PPG [Gu et al. 2003] fiducial points, fingerprint patterns, and specific iris characteristics [Unar et al. 2014]. However, not all features derived from domain knowledge might be good for the biometric classification problem, so in some cases a feature selection step is required.

4.2.2. Statistical features. Statistical features such as the mean, standard deviation, maxima and minima can be extracted from almost all signals independently of its domain. Frequency of biosignals can also be used as a feature when transformed to the frequency domain. Indeed, this approach has been used with ECG [Plataniotis et al. 2006], heart sound [Fatemian et al. 2010], and gait data [Rong et al. 2007], among other signals.

4.2.3. Feature selection. Feature extraction and selection is not an exact science, even when domain knowledge is available. Certain characteristics of the extracted features can introduce noise or information that might be redundant or misleading. Feature selection methods iterate through the subset of features of a signal to obtain the best subset candidate according to an evaluation function [El Ouardighi et al. 2007]. Feature selection is performed during the design of the biometric system.

Principal component analysis (PCA). PCA is an unsupervised machine learning method to reduce the dimensionality of a feature vector. It does not take into account the class of samples, only the feature values. Given a classification problem with a dataset composed of d-dimensional samples, PCA reduces the dimensionality of the dataset by creating a projection of each dataset sample onto a k-dimensional space, where $k < d$.

PCA uses the d-dimensional training samples to build a covariance matrix, which is later used to extract the *eigenvectors* and values. The more dominant features of the samples are contained in the eigenvectors with highest eigenvalues. Thus, to reduce the dimensionality of the problem, a subset of k of these eigenvectors are selected to represent the transformation matrix for the new dimensional space.

In biometric problems, Irvine et al. [2008] calculate the mean of each of the reduced dimensions in the training data to store a unique vector representing each subject. Additionally, the classification process can be leveraged to other machine learning algorithms such as k-nearest neighbour [Pal and Mitra 2012] or SVM [Ye et al. 2011]. The combination of PCA with other machine learning techniques has proven valuable

with ECG [Wang et al. 2008], gait [Nickel et al. 2012], and PPG [Kavsaoğlu et al. 2014] signals.

Linear discriminant analysis (LDA). LDA is a linear transformation technique similar to PCA. However, while the goal of PCA is to get a lower dimensionality with a reduction of information in each sample, the goal of LDA is to generate a projection that maximizes the separation between samples from different classes. In LDA, the eigenvectors and eigenvalues are calculated from a combination of the within-class scatter matrix and the between-class scatter matrix.

Transformation of samples to the new vector space defined by the subset of eigenvectors is performed in the same way as PCA. Further techniques can be used to perform the classification step such as k-nearest neighbour [Wang et al. 2008; Spachos et al. 2011].

Other methods for feature selection and reduction, including mutual information [Peng et al. 2005], correlation [Hall 1999] and fast correlation [Yu and Liu 2003], have been widely used in the literature for all kinds of machine learning problems.

5. MATCHING UNIT

The matching unit receives feature vectors in the time, frequency, or any other domain and outputs a decision. If the biometric system is working in verification mode, the decision has two possible values: genuine user or impostor. When working in identification mode, the decision can have as many values as subjects being identified. Wearable biometric systems generally work in verification mode whether traditional and hybrid systems can be used for both modes.

The location of the matching unit depends on the kind of biometric system. For traditional and hybrid systems, it is located in a traditional workstation, receiving information from multiple sensors (subjects). In wearable systems, it is embedded in the same wearable device as the sensor. Alternatively, it can also be placed in a more computational capable device such as a smartphone.

The matching unit uses similarity and machine learning techniques to produce its decision. A summary of the most used similarity techniques, including its computational complexity, is given on section 5.1. The complexity analysis of each technique is useful to evaluate their suitability when applying them to a wearable scenario. Similarity measurement methods are widely used by machine learning algorithms to measure how different are two biosignals. Section 5.2 reviews the most recent machine learning techniques that have been used to implement wearable and hybrid biometric systems. In multi-modal biometric system, results from all matching techniques must be combined together. Fusion approaches are reviewed in Section 5.3.

5.1. Signal Similarity

The method to computing similarity between two biosignals has a great impact on the results of the matching unit. Distance and correlation functions are generally the basis for quantitative measures of similarity between two signals.

5.1.1. Classic distance functions. Consider two feature vectors $s = \{s_0, s_1, \ldots, s_n\}$ and $t = \{t_0, t_1, \ldots, t_n\}$ where each component of the vectors is mapped to a coordinate of a point in space. The most common distance function is the Euclidean distance, which is a measure in the Euclidean space:

$$d_{euclidean}(s,t) = \sqrt{\sum_{i=0}^{n}(s_i - t_i)^2} \tag{1}$$

The time complexity of the Euclidean distance is $O(n)$. The Manhattan distance is simpler to compute as it requires fewer number of operations:

$$d_{manhattan}(s,t) = \sum_{i=0}^{n} |s_i - t_i| \tag{2}$$

However, its time complexity is also $O(n)$. The Mahalabonis distance takes into account correlations between signal features to generate a distance that does not overweight higher magnitude components of the signals to compare [Mahalanobis 1936]. The Mahalabonis distance is sometimes referred as the normalised Euclidean distance and is given by:

$$d_{mahalanobis}(s,t) = \sqrt{\sum_{i=0}^{n} \frac{(s_i - t_i)^2}{\sigma^2_{s_i,t_i}}} \tag{3}$$

where σ_{s_i,t_i} is the standard deviation of s_i and t_i over the set of all samples (feature vectors). The time complexity of the Mahalanobis distance is dominated by the computation of σ_i. In the first time of computation, complexity is bounded by $O(n \cdot m^2)$ where m is the number of samples available. For further executions, all σ_i are already computed and complexity is $O(n)$.

5.1.2. Dynamic time warping (DTW). DTW measures the distance between two time series. Let s and t be two feature vectors representing two time series of length n and m, respectively, where $s = \{s_1, s_2, \ldots, s_n\}$ and $t = \{t_1, t_2, \ldots, t_m\}$. DTW first constructs an $n \times m$ cost matrix (D) where each element d_{ij} contains the distance $d(s_i, t_j)$, e.g., Euclidean distances. In this way, each matrix element represents the alignment between points s_i and t_j of the two time series. A warping path (W) is a finite set of contiguous matrix elements pairs that starts at (s_1, t_1) and finishes at (s_n, t_m). The warping path defines a possible mapping between the two time series s and t. DTW uses dynamic programming to find the warping path that minimizes the total distance of its mapping elements.More details on DTW can be found in [Kruskal and Liberman 1983]. DTW requires to build a $n \times m$ matrix, so its time complexity is $O(n^2)$ when $n = m$.

5.1.3. FastDTW. To reduce the executing cost of DTW, some strategies introduce constraints to decrease the number of cells that are evaluated in the cost matrix [Sakoe and Chiba 1978; Itakura 1975].

FastDTW initially reduces the resolution of the time series by averaging adjacent data points (coarsening). FastDTW finds the minimum path using the regular DTW algorithm over the reduced resolution data. The obtained minimum distance warp path is used to project a new minimum distance warp path over a version of the data with a higher resolution. The warping path is refined by searching the neighbours of the projected path. This process continues until the path reaches the original resolution.

In FastDTW, the cost matrix is only calculated for the neighbour of each resolution data. As the length of the warp path grows linearly with the size of the input, the complexity of FastDTW is $O(ln) = O(n)$, where l is the number of resolution reductions. Additional details about FastDTW can be obtained in [Salvador and Chan 2007].

5.1.4. Correlation. Correlation measures the similarity between two feature vectors as a function of the lag between them. The correlation between two signals of the same length is calculated as:

$$Correlation(s,t) = \frac{\sum_{i=0}^{n}(s_i - \sigma_s)(t_i - \sigma_t)}{\sqrt{\sum_{i=0}^{n}(s_i - \sigma_s)^2 \sum_{i=0}^{n}(t_i - \sigma_t)^2}} \tag{4}$$

Table III. Time complexity of feature vector similarity measures

Distance	**Complexity**
Euclidean	$O(n)$
Manhattan	$O(n)$
Mahalanobis	$O(n \cdot m^2)/O(n)$
DTW	$O(n^2)$
FDTW	$O(n)$
Correlation	$O(n)$
Coherence	$O(n \cdot log(m))$

n length of feature vector
m number of feature vectors

The complexity of a single correlation measure is $O(n)$. The correlation measure can be used to synchronize signals. If d is a delay introduced to one of the signals, it is straightforward to measure the correlation between a signal and a delayed version of the other signal:

$$Correlation(s,t,d) = \frac{\sum_{i=0}^{n}(s_i - \sigma_s)(t_{i-d} - \sigma_t)}{\sqrt{\sum_{i=0}^{n}(s_i - \sigma_s)^2 \sum_{i=0}^{n}(t_{i-d} - \sigma_t)^2}} \quad (5)$$

If differently delayed versions of the signal are compared to each other, different correlation values will be obtained (cross correlation). The complexity of the cross correlation is $O(n^2)$, as $d < n$.

5.1.5. Coherence. The similarity of two signals can also be measured by comparing their frequencies.This requires transforming the feature vector from the time domain to the frequency domain, e.g., by the Fourier or the Discrete Cosine Transform.

The coherence measure can be seen as the counterpart of the correlation measure, but in the frequency domain. The complexity of the coherence function depends on the method for translating the signal to the frequency domain. If the Fast Fourier Transform is used, the complexity of a coherence operation is bounded by $O(n \cdot log(n))$.

5.1.6. Time Complexity. Table III describes the time complexity of each of the studied similarity functions. Most them are linear in complexity. This makes their execution faster, but also imposes some constraints to the input vectors such as being of the same length. More complex similarity measures (DTW and coherence) avoid these drawbacks, but with a much higher computational cost.

When designing a wearable biometric system, it is necessary to measure the amount of comparisons that will be executed per query. If not selected accordingly, the similarity function can become a bottleneck that reduces the acceptability of the system.

5.2. Machine Learning Algorithms

Machine learning algorithms used in biometrics try to solve two different problems. Biometric identification (traditional and hybrid systems) is seen as a multi-class classification problem. Biometric verification (mostly found in wearable systems) are seen as one-class classification problems. Although there are some algorithms specific for each problem, some multi-class classification problems can be adapted to solve one-class classification problems.

The output of matching learning algorithms executed by the matching unit is generally a numerical value that measures the degree of similarity between the queried signal and a registered subject. After obtaining this result, a threshold t is usually applied to determine the final decision. Varying t adjusts the false positive and false

negative rates (FPR and FNR respectively)[1], generating what is called a receiver operating characteristic (ROC) curve [Hanley and McNeil 1982]. In these cases, the equal error rate (EER) is used as a measure reflecting the quality of a biometric system. The EER is the point in the ROC curve where the FPR is equal to the FNR. In general terms, the lower the EER the better acceptance and protection against circumvention.

This section describes the machine learning approaches that have been used to build wearable and hybrid biometric systems. Traditional biometric systems have not been included in this analysis. Reviewed proposals are summarized in Table IV. For each machine learning technique, the table lists related references; biosignal; kind of biometric approach (identification or verification); experimental parameters (subjects, samples and features); their results (equal error rate, accuracy, and false positive rate) if provided; and whether they are part of a multi-modal system. If experiments were done with different parameters, the results best fitting the biometric signal requirements (uniqueness, constancy, and so on) are selected. The rest of this section provides a brief explanation of each of the machine learning techniques. For details on the fundamentals of these techniques, the reader is referred to [Bishop et al. 2006].

Proposals have been categorized as wearable or hybrid depending on the characteristics of the system described in each of the works. Proposals that use a wearable devices for sensing and wearables or smart personal devices to execute the decision have been categorized as wearable systems. Works that use sensors that are medical-grade wearables or traditional workstations as the matching unit have been categorized as hybrid.

The majority of the analysed works have been categorised as hybrid. This is due to the fact that researchers generally use workstations to perform (offline) training and validation. The widespread adoption of emerging platforms such as Arduino, Intel Eddison and other IoT and wearable development platforms can help researchers to easily test their proposals in a wearable scenario.

5.2.1. Naive Bayes (NB). Naive Bayes uses the well known Bayes theorem to build a probabilistic model of the subject's features. The intuitive idea of a naive Bayes classifier is that future observations of a feature vector belonging to a subject will follow the same probabilistic distribution of feature vectors that were given for training for the same subject, and that the value of a feature is independent of the value taken by other features. Naive Bayes can be directly used to build biometric identification systems (with one class per subject), but must be modified when training data only belongs to one class (biometric verification), which is the usual use case in wearable scenarios. This is usually achieved by introducing a threshold; a specific sample is rejected as belonging to the registered subject if the calculated probability is below that threshold.

As in most machine learning techniques, the size of the training dataset has a substantial impact on the results. In the case of naive Bayes [Sugimori et al. 2011] and [Ho et al. 2012] studied the same signal and matching algorithm but obtained very different results. In fact, the number of subjects in [Sugimori et al. 2011] was too small (five) to consider their results representative.

[1]Some authors prefer using false acceptance rate FAR and false rejection rate FRR instead

Table IV. Summary of machine learning techniques proposed for biometrics (if part of a multi-modal system, all ML techniques used are listed.

Wearable Systems												
ML tech.	**Proposal**	**Signal**	**Mode**	**Sensor**	**M.U.**	**Multi**	**EER**	**H**	**FPR**	**Subjects**	**Samples**	**Feat.**
NB	[Cornelius et al. 2012]	Skin cond.	V	WSD	WSD	No	-	0.85	-	2-5	3680	7
	[Cornelius et al. 2014]	Skin cond.	I	WSD	WSD	No	0.127	-	-	8	1078	48
SVM	[Casale et al. 2012]	3 axys acc.	V	WSD	WSD	No	-	-	0.01	20	2800	18
	[Hestbek et al. 2012]	3 axys acc.	I	WSD	WSD	No	0.1	-	-	36	14400*	12
GMM	[Cornelius et al. 2014]	Skin cond.	V	WSD	WSD	No	0.127	-	-	8	1078	48
	[Shi et al. 2011]	GPS	V	WSD	WSD	Yes	-	0.99*	0.25*	50	2400	3
	[Lu 2014]	3 axys acc.	V	WSD	WSD	Yes	0.14	-	-	12	1 hour	87
	[Meharia and Agrawal 2015]	3 axys acc.	V	WSD	WSD	X	-	0.8	0.14	10	50	-
KNN	[Derawi 2015]	ECG	I	WSD	WSD	No	0.01	-	-	30	3690	4
ANN	[Pasero et al. 2015]	ECG	I	WSD	WSD	No	-	0.8*	0	40	328	-
	[Lee and Kim 2015]	PPG	I	WSD	WSD	No	-	0.96*	0.04	10	708	22
Hybrid Systems												
ML tech.	**Proposal**	**Signal**	**Mode**	**Sensor**	**M.U.**	**Multi**	**EER**	**H**	**FPR**	**Subjects**	**Samples**	**Feat.**
NB	[Sidek et al. 2014]	ECG	I	WM	WSD	No	-	0.99	-	18	108	48
	[Ho et al. 2012]	3 axys acc.	V	WSD	SV	No	-	0.69	0.30	32	640	-
	[Sugimori et al. 2011]	3 axys acc.	I	WSD	SV	No	-	0.98	-	5	100	2
BN	[Sidek et al. 2014]	ECG	I	WM	WSD	No	-	0.98	-	18	108	48
	[Singh et al. 2012]	ECG	V	WM	SV	Yes	0.11	-	-	78	6006	20
ANN	[Sidek et al. 2014]	ECG	I	WM	WSD	No	-	0.99	-	18	108	48
	[Beritelli and Capizzi 2013]	Heart sound	V	WSD	SV	No	-	0.86*	-	50	400*	32
KNN	[Reşit Kavsaoğlu et al. 2014]	PPG	I	WSD	SV	No	-	0.94	-	30	900*	20
	[Sidek et al. 2014]	ECG	I	WM	WSD	No	-	0.99	-	18	108	48
	[Nickel et al. 2012]	3 axys acc.	I	WSD	WSD	No	-	0.82	-	36	20h	52
	[El-Bendary et al. 2010]	Heart sound	I	WM	SV	No	-	0.93	-	40	10	*
	[Rasmussen 2014]	Skin cond.	V, I	WSD	SV	No	0.12*	0.88	0.02	80*	4000	-
	[Bugdol and Mitas 2014]	ECG	I	WSD	SV	Yes	-	0.44	-	30	150	33
	[Camara et al. 2015a]	ECG	I	WM	SV	No	-	0.9612	0.039	18	-	48
SVM	[Ho et al. 2012]	3 axys acc.	V	WSD	SV	No	-	1.0	-	36	640	-
	[Sugimori et al. 2011]	3 axys acc.	I	WSD	-	No	-	0.98	-	5	100	2
	[Ye et al. 2011]	ECG	I	WSD	SV	No	-	1.0	0.0	5	4800*	26
GMM	[Wahid et al. 2012]	Heart sound	V	WM	SV	No	-	0.86*	-	80	160	24
	[Zhao and Shen 2011]	Heart sound	I	WM	SV	No	-	1.0	0.0	30	90	-
	[Fatemian et al. 2010]	Heart sound	I	WM	SV	Yes	0.35*	-	-	21	126	-
HMM	[Nickel et al. 2011]	3 axys acc.	I	WSD	SV	No	0.10	-	-	48	1344	26
DT	[Sugimori et al. 2011]	3 axys acc.	I	WSD	-	No	-	0.98	-	5	100	2

*	Estimated from data in reference
-	Data not provided in reference
V	Verification mode
I	Identification mode
WM	Wearable medical grade sensor
WSD	Wearable or other smart-device such as a smartphone
SV	Server or workstation that is not constrained in computing power

5.2.2. Bayesian network (BN). A Bayesian network represents a probabilistic model of a problem as a directed acyclic graph (DAG). In biometric systems, the signal features $s = \{s_1, s_2, \ldots, s_n\}$ and subjects $U = \{u_1, u_2, \cdots, u_n\}$ are represented as nodes of the graph (one node per signal feature and one node for the subjects). Directed edges in the Bayesian network that connect two nodes are associated with a probability p and represents the conditional probability that the source of the edge will happen given that the destination node of the edge happens. Naive Bayes is a special case of Bayesian network where the node representing the subject can only have children and features are independent (nodes representing features have the subject node as their only parent).

The probability of a signal belonging to a specific user is calculated chaining the conditional probabilities of each of the nodes connected to the subject node. To assign a query signal to a specific subject, the same process as in Naive Bayes is carried out. The decision is based on the class with higher probability.

Sidek, Mai and Khalil [2014] studied both naive Bayes and Bayesian network with the same training. Results obtained in both cases were very similar in accuracy.

5.2.3. Artificial neural networks (ANN). An ANN mathematically simulates the structure of biological neural networks [Haykin and Network 2004]. A neural network is composed of one input, one output and several hidden layers of neurons. Each neuron in the neural network has a fixed number of inputs and produces one output. The neurons in the input layer receive the outside stimulus (the biosignal feature vector) as input. Each neuron in the neural network produces its output by applying a combination of functions (propagation, activation and transfer) to the neuron inputs. During the training phase, the network is presented with samples from the training set and the weights of the propagation function are adjusted depending on the output of the neural networks and label of each training register. The neurons in the output layer generate the output value of the neural network, which has different applications depending on the problems where the network is being used. In biometrics, it can be used to determine the identity of the subject that produced the input signal.

Artificial neural networks have been used in both wearable and hybrid biometric systems. Pasero et al. [2015] used ANN to verify the identity of 40 subjects, achieving an accuracy of 80% with no false positives. Lee and Kim [2015] used a similar approach to verify identities based on the subject PPG signal. Their results were better (accuracy of 96%) but their subject population was not very representative (only 10 subjects). In Sidek et al. [2014] a multi-layer perceptron (MLP) to tell apart ECGs was compared against Naive Bayes, Bayesian networks, and k-nearest neighbour. The MLP was found to perform as well as naive Bayes and k-nearest neighbour, but the number of samples is not very representative. Gautam [2013] used a MLP to distinguish the heart sound of ten different subjects. The MLP has ten neurons in the hidden layer and achieved an accuracy of 0.90. Beritelli and Capizzi [2013] used a probabilistic neural network to distinguish subjects by their heart sound. Authors reported an accuracy of 86% with 50 different subjects.

5.2.4. K-nearest neighbour (KNN). KNN is a so-called lazy learning method that stores feature vectors in the training dataset, and all processing is delayed until classification. When the system is queried with a new signal, the feature vector is compared with all stored samples using a distance function (see Section 5.1.1). The system returns the class with the nearest k neighbours to the query signal. K-nearest neighbour can be adapted to verification problems by reducing k to 1 and establishing a threshold t to perform the decision based on the similarity measure obtained.

KNN its a very extended technique due to its simplicity and effectiveness. These reasons also account for this popularity as a matching and decision algorithm for wearable

biometric proposals. Independently of the signal used for classification, KNN obtains very good accuracy results in most proposals. However, one of the drawbacks is this algorithm is generally more computationally expensive than others because it requires comparing the query sample with all the stored feature vectors.

5.2.5. Support vector machines (SVM). SVM is a statistical learning method that builds a hyperplane that optimally separates the different classes of training samples [Hearst et al. 1998]. The separation hyperplane is chosen to have the maximum possible distance between the closest points of each class (said to maximize the margin between classes). There are some cases where no hyperplane can be determined without misclassifying any of the training classes. In this case, SVM chooses a hyperplane that splits the examples with the minimum possible number of misclassified samples while trying to maximize the distance between the nearest correctly classified training samples. The effectiveness of SVM depends on the kernel selected and the soft margin parameter C. The former specifies the process to calculate the hyperplane. The latter describes the influence of a single sample in the hyperplane. SVM was originally intended for multi-class classification (biometric identification) but can be adapted to be trained for one-class classification problems only [Schölkopf et al. 1999]. In this cases, C is the parameter that defines how strict is the SVM when adapting to the training dataset samples.

In [Casale et al. 2012; Hestbek et al. 2012] researchers used the accelerometer to verify the identity of subjects while performing gestures. They were only able to verify the identity of the subject while walking in a very constrained environment. Dandachi et al. [2013] proposed a multimodal system consisting of accelerometer, gyroscope, and GPS positioning to verify a subject's identity. Their results were promising but involved only three subjects. Ho et al. [2012] obtained a 100% accuracy using accelerometer data, but their classification strategy was not exactly a biometric system. It was a mix of identification and verification; their system accepts several subjects, but classified them in two classes: enrolled or not enrolled. Ye et al. [2011] obtained similar results with the ECG signal, but with a very limited population of individuals (5 subjects).

5.2.6. Gaussian mixture model (GMM). GMM is a probabilistic model that assumes that all the samples from the same class (subject) can be generated by a weighted sum of a finite number of Gaussian distributions. The weights of each distribution and their parameters are obtained through different fitting methods, e.g., expectation-maximization (EM) algorithm [Dempster et al. 1977] being the most common in the literature. GMM generates one model per class in the classification problem and outputs the likelihood that the sample used as input belongs to the GMM class. GMMs can be used for both verification and identification purposes. In a verification system a probability threshold must be established to select samples as valid for that GMM model. In a biometric identification system, the query sample is passed though all subject's GMMs and the one with more likelihood is selected.

GMM has been widely used in voice recognition systems [Reynolds and Rose 1995]. This is why most of its uses related to biometric identification have focused on sounds emitted by the body, specifically the heart [Wahid et al. 2012; Zhao and Shen 2011; Fatemian et al. 2010]. Experiments achieved accuracy between 0.86 and 1.0 with medium-sized populations of subjects (between 10 and 80 subjects). GMM has also been used for verification purposes using the accelerometer and skin conductance as signals [Cornelius et al. 2014; Lu 2014; Meharia and Agrawal 2015; Shi et al. 2011] with worst results. Equal error rate and false positive rates were above 0.14 in all cases.

5.2.7. Hidden Markov model (HMM). HMM is a particular kind of Bayesian network [Ghahramani 2001]. In a HMM, the nodes of the DAG represent the state of a system and a set of observations that configure the state of the system. The system transitions from one state to the other depending on the observations and a set of transition probabilities (edges of the DAG) that are previously unknown. HMM have been widely used in several machine learning problems, but are specially known for its applications to speech recognition [Ghahramani 2001].

[Nickel et al. 2011] trained a HMM for each subject by presenting two classes to each of the HMM. The first class corresponds to samples that belong to the subject's HMM and the second class corresponds to samples belonging to other users. The researchers were able to achieve an average EER of 0.10 with 48 different subjects.

5.2.8. Decision trees (DT). In a decision tree, each node evaluates a feature and tree leafs specify the decision to make. In the biometric domain, decision nodes evaluate the different components of the feature vector, and leafs specify the subject assigned to each biosignal. Decision trees can be generated directly by experts or by inferring their structure from training data. A well known algorithm to generate decision trees given a training dataset is the C4.5 algorithm [Quinlan 2014]. This algorithm follows a simple process to build the decision tree: (i) calculate the feature that provides the highest information gain in the samples; (ii) create a decision node using the attribute that better splits the training dataset in its classes; (iii) create sub-lists of samples using the decision criteria created; (iv) create a decision tree for all the sub-lists starting at that decision node. The algorithm stops when all samples in a sub-list belong to a specific class. In that case, the algorithm creates a decision node for that class.

Sugimori et al. [2011] found decision trees could identify subjects with high accuracy using accelerometer data. Unfortunately, the subject population was only 5 subjects.

5.3. Multi-Modal Biometrics

Biometric systems rarely achieve perfect accuracy in practice due to many factors, such as noise, incomplete training, or non-ideal machine learning algorithm, resulting in false positives and false negatives. Additionally, a small fraction of the population may not be able to provide a specific biometric signal due to disabilities or health problems. To overcome some of these limitations and improve accuracy, it is natural to imagine combining different biosignals during the recognition process [Hong et al. 1999]. This combination can be performed at any of the stages of the biometric process (Figure 6): sensing, feature extraction, matching, or decision making [Faundez-Zanuy 2005].

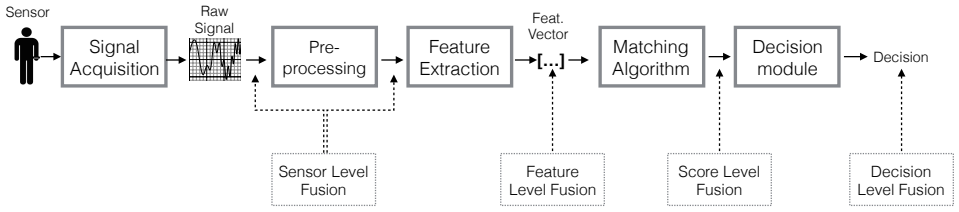


Fig. 6. Location of different fusion levels mapped to different processes in a biometric system.

The benefits of multi-modal biometric systems must be evaluated carefully for a particular application. Processing new biometric traits incurs an overhead in terms of increased computational capabilities required in the system. This sophistication and

Table V. Summary of multi-modal biometric references.

Proposal	Signals	Fusion	Subjects	Samples	EER	H
[Feng et al. 2013]	Magnetometer and gyro.	Feature	31	910	0.112	-
[Mondal and Nandy 2012]	Rotation	Feature	30	30 seconds	-	1.00
[Singh et al. 2012]	ECG, face and fingerprint	Score	78	6084	0.0022	-
[Vildjiounaite et al. 2006]	Accelerometer and voice	Score	31	-	0.021	-
[Fatemian et al. 2010]	ECG and PPG	Decision	21	2070	-	0.97
[Agrafioti and Hatzinakos 2008]	12 lead ECG	Decision	14	655	-	1.00
[Bugdol and Mitas 2014]	ECG and voice	Feature	30	150	-	0.92

- Data not provided in reference

corresponding cost may not be feasible or desirable for wearable devices [Jain and Ross 2004]. Table V summarizes the results reported for different multi-modal biometric approaches.Multi-modal biometric systems based on wearables could also use information from non-wearables sensors to improve their accuracy. These could be behavioural information extracted from the mobile device [Bo et al. 2013] or a biosignal captured from non-wearable sensors [Camara et al. 2015b] among others. In this work we focus only on those that strictly use wearable devices.

5.3.1. Sensor level fusion. In sensor level fusion, the raw signals $(r', r'', r''', \ldots)$ from the different sensors are combined into a single biosignal r. Sensor level fusion can be performed before or after preprocessing the raw signal, but before the feature extraction process. Combined signals at this stage should be highly related. Combining signals from very different domains without loss of information is a very difficult task because the signals can have very different meanings [Joshi et al. 2009].

A widely extended example of this approach is the fusion of 3-axis accelerometer data into a unique signal for analysing gait [Lu 2014; Gafurov et al. 2006a].

5.3.2. Feature level fusion. In feature level fusion, each raw signal used in the multi-modal system is processed independently to generate an independent feature vector $(s', s'', s''', \ldots)$. Then, all feature vectors are combined into one vector s for use in the matching process, e.g., by concatenating the different feature vectors. If some features of the different vectors are closely related, they can also be combined by using a function, instead of concatenation [Joshi et al. 2009].

Agrafioti and Hatzinakos [2008] evaluated the accuracy of feature level fusion against decision level fusion for a 12-lead ECG system. Instead of combining the signal from all ECG leads into one ECG signal, features for each lead are extracted and then combined into a single feature vector (feature level fusion). Their results with 14 subjects show that both fusion approaches increase the accuracy compared to single leads, and decision-level fusion was the most accurate for ECG. Unfortunately, 12-lead ECG is not feasible for wearables. Bugdol and Mitas [2014] added voice features to increase the accuracy of an ECG identification system from 44% to 92%. Feng et al. [2013] studied the usage of accelerometer, magnetometer and gyroscope data to identify users when picking up phone calls. Their results found that accelerometer data introduced noise into the process, reducing the accuracy of the multi-modal system.

5.3.3. Score level fusion. In score level fusion, the output of the matching algorithms for each of the signals is combined. This means that each raw signal is processed to generate a feature vector put into a different matching unit that has been trained only with signals generated from that sensor. Outputs can be combined using weighted sums or other combinatorial operation. The result is passed to the decision module to obtain the final result.

Kumar et al. [2008] tried particle swarm optimization (PSO) [Kennedy 2010] to obtain the optimal weights for combining the outputs from different matching algorithms

for fingerprint and hand geometry images. Their approach obtained better results than an analogous biometric system using decision level fusion (see next section). Another example of score level fusion, Singh et al. [2012] combined ECG with facial and fingerprint recognition to improve the EER from 11% to 1%.

5.3.4. Decision level fusion. Decision level fusion combines the decisions from each of the matching units. This kind of multi-modal fusion is particularly appropriate when some subjects are unable to provide one of the biometric signals required by the system. Decision level fusion is usually carried out by a voting system. Depending on the confidence and accuracy of each of the sub-systems, decisions can be combined using a weighted voting system.

Veeramachaneni et al. [2005] described a decision level fusion algorithm taking into account the cost of wrong decisions to adapt in real time, thereby improving flexibility. The fusion could also be configured to be strict, i.e., all sub-systems must agree on the classification output. This improved the security against impersonation attacks but increased the number of false negatives. In verification mode, the system could be configured to accept the subject identity if any of the sub-systems gives a positive output. In this case, the system improved its usability but reduced its resilience against attacks. Decision fusion algorithms can also be generated through machine learning. Giot and Rosenberger [2012] experimented with genetic programming [Koza 1992] to generate the fusion function, but results were only slightly better than weighted sums.

Agrafioti and Hatzinakos [2008] found that combining 12-lead ECG signals at decision level performed better than fusion at the feature level. Fatemian et al. [2010] also showed that the accuracy of ECG as a biometric improved when combined with the PPG signal at decision level.

6. OPEN ISSUES

The analysis of current proposals included in Table IV has led us to identify some key issues that hinder the applicability of the obtained results. Rather than a criticism of current works, we believe these are opportunities for researchers to address and solve some of the still open problems in the wearable biometrics area. We group these issues into four major groups: (i) biosignal quality; (ii) time complexity; (iii) datasets; and (iv) vulnerability to attacks.

6.1. Biosignal Quality

Biometric signals should be distinguishable, permanent, collectable, and difficult to imitate. Table VI quantifies the set of requirements for the biosignals that can be captured with the sensors relevant to this survey.

To measure distinguishability, we quantify the best results obtained in terms of accuracy H (number of times the system outputs the correct decision), false positive rate FPR, and equal error rate EER. Results from Table VII show that the choice of machine learning classifier is not critical. Choosing useful features and obtaining good quality data are more important factors affecting classification results. Most of the signals studied achieve a high accuracy, low false positive or equal error rates. However, only 5 out of 25 works performed experiments with 50 or more subjects. Some signals are used to improve the accuracy of others (GPS and gyroscope with the accelerometer) as they do not provide enough information to distinguish between users. Experiments with ultraviolet, ambient light, skin temperature, and barometer have not been reported in the literature yet.

Permanence is quantified by reviewing whether researchers tested their proposals with biosignals taken more than a month apart. The effects of ageing have only been studied for well established biometrics that cannot always be implemented in wearable

Table VI. Signal quality summary (results from best proposals in each category).

Signal	Distinct			Permanent	Collectable	Imitability	
	EER	H	FPR	Tested	Tested	Human	Synthetic
PPG	-	0.96*	-	x	✓	x	x
ECG	0.01	1.0	0.0	✓	✓	x	x
Accelerometer	0.1	1.0	0.01	x	✓	✓	x
Gyroscope	-	-	0.02[1]	x	✓	x	x
Magentometer	-	-	-	x	✓	x	x
GPS	-	0.99*	0.02[1]	x	✓	x	x
Ambient light	-	-	-	x	✓	x	x
Skin temperature	-	-	-	x	✓	x	x
UV light	-	-	-	x	✓	x	x
Skin conductance	0.12*	0.88	0.02	x	✓	x	x
Heart sound	0.35*	1.0	0.0	x	✓	x	x
Barometer	-	-	-	x	✓	x	x

-	No data available
*	Estimated from data in reference
[1]	Multi-modal with sensor or feature fusion level
x	Not tested
✓	Tested

devices [Lanitis 2010]. Only Da Silva et al. [2013] tested the accuracy of a biometric system based on ECG four months after the template readings. Results showed an increase from 1% to 9.1% in the EER.

In this survey, only sensors that can read biosignals without interfering with daily activities have been considered. Therefore, we presume all signals are feasible to collect. Nevertheless, in most of the experiments, ECG and PPG biometric signals have been captured with medical grade devices and in very controlled environments. The recent development of cheap sensors and platforms such as Bitalino [Alves et al. 2013] or Angel Sensor [Seraphim Sense 2016] will help to collect results with a more general purpose hardware. However, it remains to be seen if signals acquired in much more noisy environments and with low-precision hardware are still good enough for wearable biometrics.

As can be deduced from table IV, most research on wearable biometrics has been focused on signals that are originated in the heart. PPG, ECG and heart sound are used in 14 out of 25 proposals, being ECG and PPG the most used ones in most recent works. The other widely used sensor is the accelerometer. It is used in 7 proposals. Other signals are used on a small set of multi-modal proposals to improve the accuracy of the biometric system. This is expected for some sensors that provide low information such as light sensors. We foresee that other features such as the skin temperature will play major roles when their sensors and their usage in biometrics are studied further. Our research has shown also that that hybrid systems generally achieve better results than wearable systems. This could be attributed to the quality of the sensors or the differences in the classification problems. Multi-class classification problems (identification) are generally easier than one-class classification problem (verification), due to the availability of samples from all classes during training. Another issue that has arisen during our literature review is that biometric verification is not always tested in the same way. Some of the works reviewed claim to be doing biometric verification, but they use genuine and impostor samples for training. This is not a realistic setup, as in most wearable environments the enrolment (training) will be done only with genuine samples.

Table VII. Summary of machine learning techniques used in wearable biometric proposals.

Algorithm	Verification	Identification	Learning comp.	Query comp.
Naive Bayes	•	✓	$O(n \cdot m)$	$O(m)$
Bayesian network	•	✓	$O(n \cdot m^2)$	$O(m^2)$
ANN	•	✓	$O(n \cdot m^2)$	$O(m^2)$
KNN	✓	✓	$O(1)$	$O(n) \cdot O(distance_{func})$
SVM	•	✓	$O(n^2 \cdot m)$*1	$O(m)$
GMM (with EM)	✓	✓	$O(n \cdot m \cdot k)$*2	$O(m \cdot k)$
HMM		✓	$O(s^2 \cdot m)$	$O(m)$
Decision trees (C4.5)		✓	$O(n \cdot m^2)$	$O(m)$

*1 Using algorithm optimizations [Bordes et al. 2005]. Complexity is $O(n^3 \cdot m)$ without optimizations.

*2 With k the number of mixtures and using algorithm optimizations in [Verbeek et al. 2003]. Complexity is $O(n \cdot m \cdot k^2)$ without optimizations.

• Requires adaptation

n Number of samples in training dataset

m Number of features in each sample

k Number of gaussian distributions

s States of the HMM

6.2. Time Complexity

In general terms, current biometric systems are being evaluated only in terms of their accuracy or EER. However, for wearable devices, a very accurate algorithm that drains the battery quickly or takes too much time to make a decision is not feasible.

The matching process is one of the most computationally expensive tasks in a biometric system, along with pre-processing and feature extraction. Table VII offers a summary of the computational complexity of previously described machine learning algorithms. The complexity of machine learning algorithms greatly depends on the implementation and some of its parameters. Parameters affecting computational complexity are also listed in the table. In the cases where complexity depends on the implementation, the optimal implementation has been selected. When analysing the complexity of the machine learning algorithms, special emphasis has to be put on the complexity of the query process. Generally, the training or enrolment process is executed only once.

Most of the algorithms have a complexity that depends linearly on the number of features in each sample $O(m)$. Bayesian networks using the belief propagation technique increase this complexity to $O(m^2)$. In the case of ANNs, the computational complexity does not depend only on the number of samples and features of each sample, but also on the amount of neurons used (k), which must be greater than the number of features (m). As k is bounded by m, we consider that the query complexity is $O(m^2)$. KNN is a very efficient technique during training ($O(1)$), but the querying complexity depends on the distance function used, as the querying signal must be compared to all the reference signals $O(n) \cdot O(distance_{func})$ where $O(distance_{func})$ depends on the used distance function (Table III). Depending on the distance function and amount of signals to compare, it can become a bottleneck in a biometric system. However, wearable systems are presumed to store a small amount of samples from just one subject.

6.3. Datasets

The only dataset that has been used by more than one of the reviewed works is Physionet [Moody et al. 2001]. This dataset is an open archive of biosignals and processing software for biomedical purposes. Although it includes a substantial number of sam-

ples for ECG, PPG and other biosignals, their medical purpose makes them not suitable for wearable scenarios. Signals have been captured with medical grade sensors, and some of the subjects are suffering from conditions that can affect the signal. The other works surveyed used their own datasets. Another dataset, that is available upon request is the one provided by the University of Toronto BioSec Lab [Wahabi et al. 2014]. Their dataset includes ECG and heart sound signals.

Preparing datasets of biosignals is a complex, time consuming, and usually inefficient task. In most of the cases, subjects are recruited using ads in a university or research centre. This limits datasets to a small geographical area and very specific age groups (college-level students). Additionally, the research team must prepare a signal acquisition protocol and pre-process all the signals obtained. A publicly available dataset of biosignals would reduce the workload of researchers in this area and would facilitate a fair comparison of all experiments. However, after years of research the number of available datasets is very limited. This is generally due to the ethics and privacy issues that can arise from sharing them publicly. Depending on the kind of sensors used, these datasets contain very sensitive information in two senses. First, they contain information that can be used to uniquely identify persons, as they are used for biometric purposes. Additionally, depending on the kind of sensor used to capture data, they could also include information that could disclose medical conditions of the volunteers that participated in the study. Providing means to test the suitability of a matching algorithm without disclosing the underlying sensitive information from the subjects is still a research issue. Having such a system could help researchers test their systems without the need of gathering a dataset to test it.

Projects such as Apple's ResearchKit can help to avoid geographical and age biases. ResearchKit is a framework to develop mobile applications to perform research studies. Apps developed with ResearchKit can survey users and gather data from the sensors that are inside the device or connected to it. ResearchKit also eases the data collection process and provides informed consent forms for subjects participating in studies. Nevertheless, it seems that for the moment, these framework is limited only to medical studies.

6.4. Attacks to Wearable Biometric Systems

Another key issue of wearable biometric systems is their security. A biometric system can be compromised by attacking any of its components or the communications between them (see Figure 7). Ratha et al. [2001] identified eight out of the nine different attack points shown in Figure 7 for traditional biometric systems, the ninth being the channel used to store the user's signature during enrollment (number ⑤ in Figure 7). We next discuss potential attacks for the case of wearable biometric systems using these attack points and grouping them into two major categories: components and channels.

6.4.1. Attacking communication channels. Communication channels are subject to four main classes of threats: interception, interruption, modification, and fabrication of messages. While the first one can be accomplished by a passive adversary (i.e., one who can only eavesdrop on the channel), the other three require an active adversary (i.e., one who can stop and inject messages). A wearable biometric system may have up to five communication channel among components (see Figure 7): ② (sensor → signal processing unit), ④ (signal processing unit → matching algorithm), ⑤ (signal processing unit → signature creator), ⑦ (signature database → matching algorithm), and ⑨ (decision module → user). In a real system, the attacker might have access only to a limited number of such channels. For example, the sensor and the signal processing unit are sometimes combined and ② is inside the sensor device, which might be

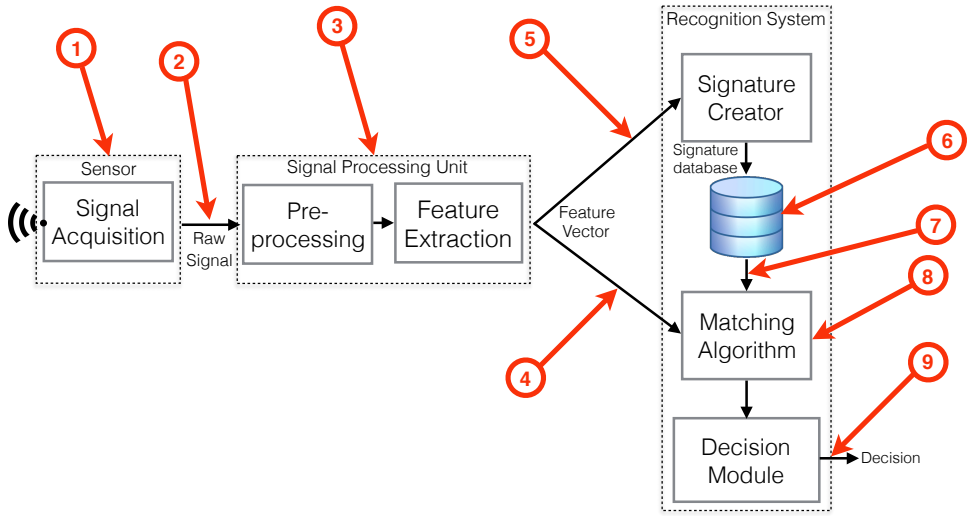


Fig. 7. Attack points of a biometric system.

out of the reach of the adversary. Similarly, ⑦ could be a system channel within the smartphone if the signature database is in the device, or an Internet connection if the database is stored in the cloud.

Interception can take place if the attacker has access to the channel and messages are not encrypted. The goal pursued by capturing messages varies depend on the channel. For example, eavesdropping raw signals on ② or feature vectors in ④ or ⑤ can be needed for a subsequent replay attack. Raw signals can also be used to reduce the search space when looking for another signal that produces the same feature vector [Ratha et al. 2001]. In other cases, it has been proven that some signals leak out valuable information about another signal. For instance, pictures and recordings can provide information about the subject's face or gait [Gomez-Barrero et al. 2014; Liu et al. 2009a]. The threat of interception can be generally mitigated by encrypting the channel. Since most wearable sensors connect to the smartphone using Bluetooth, it is important to securely pair the devices, authenticate both the sensor and the receiving devices and to ensure that communications are always encrypted. In the case of ⑦, when the database is implemented as an external service accessible through an Internet connection, standard security protocols such as TLS can be used.

Interruption on any system channel shown in Figure 7 will translate in a denial of the recognition service. An attacker can achieve this by jamming the channel or by sitting between the sender and receiver (i.e., in a man-in-the-middle setting) and blocking messages between them. Preventing this threat is generally difficult if the attacker has access to the channel and countermeasures (e.g., redundant channels) can be expensive.

Modification and fabrication attacks can pursue different goals. For example, by replaying a valid users' signal over ② or a valid feature vector over ④, an attacker can get authenticated. Similarly, fabricating messages over ⑤ could permanently enroll an attacker in the system. In general, preventing modification and fabrication attacks requires the use of standard message authentication mechanisms and, in some cases challenge-response schemes such as the one proposed in [Jain and Ross 2004] for biometrics.

6.4.2. Attacking components. The components of the wearable biometrics system can be also attacked in a number of ways. The sensor (①) can be presented with fake data that mimics a valid user's signal (e.g., the fake iris on contact lenses or fake fingerprints on gelatin attacks). The software and firmware of the sensor can be also tampered with, even remotely. These attacks can be difficult to prevent and detect (e.g., using code integrity techniques) considering the lack of computational resources available in cheap sensors. These attacks also affect the signal processing unit (③), which can be manipulated to override the feature extraction process. For example, the attacker could be interested in stealing all feature vectors generated by this unit or generating a particular feature vector.

A crucial component of the entire system is the database that stores the user's signatures (⑥). The confidentiality and integrity of such data is paramount. Three common goals for an attacker that involve attacking the database are: (i) stealing signatures; (ii) associate a particular (fake) signature with an already enrolled user; and (iii) enroll a new user and store the associated signatures. Providing protection to the database of signatures has been widely studied in traditional biometrics. However, in the wearable setting this might prove challenging. If the database is stored in the smartphone, it can be compromised by a malicious app with sufficient privileges. Contrarily, keeping it in an external server (i.e., the cloud) or a secure token entail a different set of risks and can make the system too expensive.

Finally, more sophisticated attacks can be launched against the matching and decision units (⑧ and ⑨). Recall that these modules essentially implement a pattern recognition system. Over the last decade, some work (see, e.g., [Barreno et al. 2006; Barreno et al. 2010] for an overview) has studied how an adversary can strategically play against machine learning algorithms to thwart their function. One major objective for the attacker could be to exploit weaknesses in the underlying classifier and construct an invalid signal that would look valid. According to the terminology introduced by Barreno et al. [2010], *exploratory* attacks might provide the attacker with information about the inner workings of the classifier by selectively querying the biometric system with carefully constructed signals. Similarly, in a *causative* attack the adversary can strategically participate in the training process to contaminate the samples so as the system will later recognized him. The interested reader is referred to a recent paper by Biggio et al. [Biggio et al. 2015] in which the authors discuss in detail machine-learning related vulnerabilities of biometric systems, attacks, and potential countermeasures.

6.4.3. Examples of existing attacks and research challenges. Many works justify the lack of research on wearable biometric attacks due to the difficulty to reproduce biometric signals such as the ECG or PPG [Singh et al. 2012; Sidek et al. 2014]. However, this is not necessarily true, as other authors have noted that synthetic generation of these biosignals is feasible but has yet to be studied [Agrafioti et al. 2011; Rasmussen 2014; Cornelius et al. 2014]. This is also related to another important aspect of wearable biometrics security: imitability of the used biosignals. The imitability of a signal depends on two factors: the capacity of the attacker to capture the data necessary to generate a valid signal, and the capacity to generate that signal so it can be read by the biometric system. Imitability has been widely studied in the case of classic biometrics such as the fingerprint or the iris, but it has passed unnoticed in most of the works focused in wearable sensors.

Very few studies have addressed attacks to obtain information about valid signals. In [Gafurov et al. 2006b; Liu et al. 2009a; Liu et al. 2009b; Tanviruzzaman and Ahamed 2014] researchers tested how attacks based on subject observation can reduce the accuracy of the system, increasing the EER up to 10% more. However, the information

about the signal is not enough, as described in [Gafurov et al. 2006b]. Attackers also require specific training to reproduce the biosignal. In another work [Calleja et al. 2015], the authors point a web camera at the subject's skin (forehead) to extract the heart Inter-Pulse Intervals (IPI), which have been proposed as the basis for several authentication protocols. Authors use artificial vision techniques to extract from the camera image the PPG signal of the subject. This same strategy could be used to steal PPG signals from subjects.

Externally observing the subject is not the only way to obtain a valid biometric signal. If the system components use wireless communications, attackers can take advantage of the lack of mutual authentication to create fake system components to steal the readings from the sensor. This kind of attack was used to obtain sensor readings from Gamin wearable devices [Rahman et al. 2016]. Generating a valid signal from one of these readings is just a matter of developing the necessary hardware to reply the captured data.

7. CONCLUSIONS

In this survey, we have reviewed the state of the art on wearable biometric systems. We have described a general model for biometrics and presented a classification of biometric systems depending on its components: sensor(s), signal processing unit, and matching unit. We have provided a taxonomy to classify wearable sensors according to five different dimensions. This classification allows researchers to identify the biometric-related properties of sensors and devices embedding them.

Using these classifications, we have analysed most recent works related to wearable and hybrid biometric systems. Our analysis shows that research in wearable biometrics has several directions for improvement. Very few works analyse the time performance of algorithms that must be executed in smart devices and wearables. Access to new prototyping platforms such as Arduino or Intel Edison can help researchers to evaluate their algorithms in a more realistic setting.

Another problem of current works is the difficulty to carry out a fair comparison because of the lack of publicly available datasets, particularly signals obtained with wearable hardware (i.e., not with medical grade equipment in hospital facilities). Easier access to sensors will also mean that data gathering and experimentation will be easier and faster. It is no longer necessary to buy medical grade equipment to capture biosignals in a non-invasive manner. This development, along with recent proposals of research app frameworks, will help to develop new datasets that will hopefully be made publicly available. While the results obtained in the analysed works look promising, there is a need to further analyse how some signals such as the ECG, PPG, and accelerometer change in the long run.

Finally, we also recommend to further investigate the possible attacks that might be directed at a wearable biometric system. Spoofing seems to be the most dangerous attack and, in some cases, researchers take for granted that some signals cannot be spoofed. Effort should also be devoted to study newly proposed biosignals to avoid assumptions that can generate a false sense of security.

Acknowledgements

This work was partially supported by the MINECO grant TIN2013-46469-R (SPINY) and the CAM Grant S2013/ICE-3095 (CIBERDINE).

References

Foteini Agrafioti, Jiexin Gao, and Dimitrios Hatzinakos. 2011. Heart biometrics: theory, methods and applications. *Biometrics: Book* (2011). http://cdn.intechopen.com/pdfs/16509.pdf

Foteini Agrafioti and Dimitrios Hatzinakos. 2008. Fusion of ECG sources for human identification. *2008 3rd International Symposium on Communications, Control, and Signal Processing, ISCCSP 2008* March (2008), 1542–1547. DOI:http://dx.doi.org/10.1109/ISCCSP.2008.4537472

John Allen. 2007. Photoplethysmography and its application in clinical physiological measurement. *Physiological measurement* 28, 3 (2007), R1.

Ana Priscila Alves, Hugo Silva, Ana Fred, and others. 2013. BITalino: a biosignal acquisition system based on Arduino. In *Proceeding of the 6th Conference on Biomedical Electronics and Devices (BIODEVICES)*.

Takuo Aoyagi and Katsuyuki Miyasaka. 2002. Pulse oximetry: its invention, contribution to medicine, and future tasks. *Anesthesia and analgesia* 94, 1 Suppl (2002), S1.

Apple 2015. *Apple Watch*. Apple. http://www.apple.com/watch/.

Julian Ashbourn. 2014. *Biometrics in the New World: The Cloud, Mobile Technology and Pervasive Identity*. Springer.

James E Atkinson. 1978. Correlation analysis of the physiological factors controlling fundamental voice frequency. *The journal of the acoustical society of America* 63, 1 (1978), 211–222.

Marco Barreno, Blaine Nelson, Anthony D. Joseph, and J. D. Tygar. 2010. The security of machine learning. *Machine Learning* 81, 2 (2010), 121–148. DOI:http://dx.doi.org/10.1007/s10994-010-5188-5

Marco Barreno, Blaine Nelson, Russell Sears, Anthony D. Joseph, and J. D. Tygar. 2006. Can machine learning be secure?. In *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2006, Taipei, Taiwan, March 21-24, 2006*. 16–25. DOI:http://dx.doi.org/10.1145/1128817.1128824

Joe Belfiore. 2015. Making Windows 10 More Personal and More Secure with Windows Helloy. https://blogs.windows.com/windowsexperience/2015/03/17/making-windows-10-more-personal-and-more-secure-with-windows-hello/. (2015). Accesssed on April 2016.

Francesco Beritelli and Giacomo Capizzi. 2013. A New Approach to Heart Sounds Biometric Recognition Based on Gram-PNN. (2013), 5–6.

Lena Biel, Ola Pettersson, Lennart Philipson, and Peter Wide. 2001. ECG analysis: a new approach in human identification. *Instrumentation and Measurement, IEEE Transactions on* 50, 3 (2001), 808–812.

Battista Biggio, Giorgio Fumera, Paolo Russu, Luca Didaci, and Fabio Roli. 2015. Adversarial Biometric Recognition : A review on biometric system security from the adversarial machine-learning perspective. *IEEE Signal Process. Mag.* 32, 5 (2015), 31–41. DOI:http://dx.doi.org/10.1109/MSP.2015.2426728

Christopher M Bishop and others. 2006. *Pattern recognition and machine learning*. Vol. 4. springer New York.

Cheng Bo, Lan Zhang, Xiang-Yang Li, Qiuyuan Huang, and Yu Wang. 2013. Silentsense: silent user identification via touch and movement behavioral biometrics. In *Proceedings of the 19th annual international conference on Mobile computing & networking*. ACM, 187–190.

Antoine Bordes, Seyda Ertekin, Jason Weston, and Léon Bottou. 2005. Fast kernel classifiers with online and active learning. *The Journal of Machine Learning Research* 6 (2005), 1579–1619.

Sing T Bow. 2002. *Pattern recognition and image preprocessing*. CRC Press.

Kevin W Bowyer, Karen Hollingsworth, and Patrick J Flynn. 2008. Image understanding for iris biometrics: A survey. *Computer vision and image understanding* 110, 2 (2008), 281–307.

Michael S Braasch and AJ Van Dierendonck. 1999. GPS receiver architectures and measurements. *Proc. IEEE* 87, 1 (1999), 48–64.

Marcin D. Bugdol and Andrzej W. Mitas. 2014. Multimodal biometric system combining ECG and sound signals. *Pattern Recognition Letters* 38 (2014), 107–112. DOI:http://dx.doi.org/10.1016/j.patrec.2013.11.014

Nirupama Bulusu, John Heidemann, and Deborah Estrin. 2000. GPS-less low-cost outdoor localization for very small devices. *Personal Communications, IEEE* 7, 5 (2000), 28–34.

Alejandro Calleja, Pedro Peris-Lopez, and Juan E Tapiador. 2015. Electrical Heart Signals can be Monitored from the Moon: Security Implications for IPI-Based Protocols. In *IFIP International Conference on Information Security Theory and Practice*. Springer, 36–51.

Carmen Camara, Pedro Peris-Lopez, and Juan E Tapiador. 2015a. Human Identification Using Compressed ECG Signals. *Journal of medical systems* 39, 11 (2015), 1–10.

Carmen Camara, Pedro Peris-Lopez, Juan E Tapiador, and Guillermo Suarez-Tangil. 2015b. Non-invasive Multi-modal Human Identification System Combining ECG, GSR, and Airflow Biosignals. *Journal of Medical and Biological Engineering* 35, 6 (2015), 735–748.

Pierluigi Casale, Oriol Pujol, and Petia Radeva. 2012. Personalization and user verification in wearable systems using biometric walking patterns. *Personal and Ubiquitous Computing* 16, 5 (2012), 563–580.

Joseph T Catalano. 2002. *Guide to ECG analysis*. Lippincott Williams & Wilkins.

Clearbridge Vitalsigns 2016. *CardioLeaf FIT Shirt*. Clearbridge Vitalsigns. http://www.clearbridgevitalsigns.com/shirt.html.

Cory Cornelius, Ronald Peterson, Joseph Skinner, Ryan Halter, and David Kotz. 2014. A wearable system that knows who wears it. *MobiSys '14* (2014), 55–67. DOI:http://dx.doi.org/10.1145/2594368.2594369

Cory Cornelius, Jacob Sorber, Ronald Peterson, Joe Skinner, Ryan Halter, and David Kotz. 2012. Who wears me? Bioimpedance as a passive biometric. In *Proc. 3rd USENIX Workshop on Health Security and Privacy*.

Hugo Plácido Da Silva, Ana Fred, André Lourenço, and Anil K Jain. 2013. Finger ECG signal for user authentication: Usability and performance. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on*. IEEE, 1–8.

Ghina Dandachi, Bachar El Hassan, and Anas El Husseini. 2013. A novel identification/verification model using smartphone's sensors and user behavior. In *Advances in Biomedical Engineering (ICABME), 2013 2nd International Conference on*. IEEE, 235–238.

Arthur P Dempster, Nan M Laird, and Donald B Rubin. 1977. Maximum likelihood from incomplete data via the EM algorithm. *Journal of the royal statistical society. Series B (methodological)* (1977), 1–38.

Mohammad Derawi. 2015. Wireless chest-based ECG biometrics. In *Computer Science and its Applications*. Springer, 567–579.

Nashwa El-Bendary, Hameed Al-Qaheri, Hossam M. Zawbaa, Mohamed Hamed, Aboul Ella Hassanien, Qiangfu Zhao, and Ajith Abraham. 2010. HSAS: Heart sound authentication system. *Proceedings - 2010 2nd World Congress on Nature and Biologically Inspired Computing, NaBIC 2010* (2010), 351–356. DOI:http://dx.doi.org/10.1109/NABIC.2010.5716306

A El Ouardighi, A El Akadi, and D Aboutajdine. 2007. Feature selection on supervised classification using Wilks lambda statistic. In *Computational Intelligence and Intelligent Informatics, 2007. ISCIII'07. International Symposium on*. IEEE, 51–55.

S Zahra Fatemian, Foteini Agrafioti, and Dimitrios Hatzinakos. 2010. Heartid: Cardiac biometric recognition. In *Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on*. IEEE, 1–5.

Marcos Faundez-Zanuy. 2005. Data fusion in biometrics. *IEEE Aerospace and Electronic Systems Magazine* 20, January (2005), 34–38. DOI:http://dx.doi.org/10.1109/MAES.2005.1396793

Tao Feng, Xi Zhao, and Weidong Shi. 2013. Investigating mobile device picking-up motion as a novel biometric modality. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on*. IEEE, 1–6.

FitBit 2015. *Charge HR*. FitBit. https://www.fitbit.com/chargehr.

Davrondzhon Gafurov, Kirsi Helkala, and Torkjel Sø ndrol. 2006a. Biometric gait authentication using accelerometer sensor. *Journal of Computers (Finland)* 1, 7 (2006), 51–59. DOI:http://dx.doi.org/10.4304/jcp.1.7.51-59

D. Gafurov, E. Snekkenes, and T. Buvarp. 2006b. Robustness of Biometric Gait Authentication Against Impersonation Attack. *On the Move to Meaningful Internet Systems OTM* (2006), 479–488. DOI:http://dx.doi.org/10.1007/11915034_71

Garmin 2015. *Garming fenix 3 HR*. Garmin. http://www.garming.com/.

Girish Gautam. 2013. Biometric System from Heart Sound using Wavelet based feature set. (2013), 551–555.

Zoubin Ghahramani. 2001. An introduction to hidden Markov models and Bayesian networks. *International Journal of Pattern Recognition and Artificial Intelligence* 15, 01 (2001), 9–42.

Romain Giot and Christophe Rosenberger. 2012. Genetic programming for multibiometrics. *Expert Systems with Applications* 39, 2 (2012), 1837–1847.

Ary L Goldberger, Luis AN Amaral, Leon Glass, Jeffrey M Hausdorff, Plamen Ch Ivanov, Roger G Mark, Joseph E Mietus, George B Moody, Chung-Kang Peng, and H Eugene Stanley. 2000. Physiobank, physiotoolkit, and physionet components of a new research resource for complex physiologic signals. *Circulation* 101, 23 (2000), e215–e220.

Marta Gomez-Barrero, Javier Galbally, and Julian Fierrez. 2014. Efficient software attack to multimodal biometric systems and its application to face and iris fusion. *Pattern Recognition Letters* 36 (2014), 243–253. DOI:http://dx.doi.org/10.1016/j.patrec.2013.04.029

YY Gu, Y Zhang, and YT Zhang. 2003. A novel biometric approach in human verification by photoplethysmographic signals. In *Information Technology Applications in Biomedicine, 2003. 4th International IEEE EMBS Special Topic Conference on*. IEEE, 13–14.

Isabelle Guyon. 2006. *Feature extraction: foundations and applications*. Vol. 207. Springer Science & Business Media.

Mark A Hall. 1999. *Correlation-based feature selection for machine learning*. Ph.D. Dissertation. The University of Waikato.

James A Hanley and Barbara J McNeil. 1982. The meaning and use of the area under a receiver operating characteristic (ROC) curve. *Radiology* 143, 1 (1982), 29–36.

Simon Haykin and Neural Network. 2004. A comprehensive foundation. *Neural Networks* 2, 2004 (2004).

Marti A. Hearst, Susan T Dumais, Edgar Osman, John Platt, and Bernhard Scholkopf. 1998. Support vector machines. *Intelligent Systems and their Applications, IEEE* 13, 4 (1998), 18–28.

Martin Reese Hestbek, C Nickel, and C Busch. 2012. Biometric gait recognition for mobile devices using wavelet transform and support vector machines. In *Systems, Signals and Image Processing (IWSSIP), 2012 19th International Conference on*. IEEE, 205–210.

Chiung Ching Ho, C. Eswaran, Kok-Why Ng, and June-Yee Leow. 2012. An unobtrusive Android person verification using accelerometer based gait. *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia - MoMM '12* (2012), 271. DOI:http://dx.doi.org/10.1145/2428955.2429007

Lin Hong, Anil K Jain, and Sharath Pankanti. 1999. Can multibiometrics improve performance?. In *Proceedings AutoID*, Vol. 99. Citeseer, 59–64.

Seyed Amir Hoseini-Tabatabaei, Alexander Gluhak, and Rahim Tafazolli. 2013. A Survey on Smartphone-Based Systems for Opportunistic User Context Recognition. *Comput. Surveys* 45, 3 (2013), 27:1–27:51. DOI:http://dx.doi.org/10.1145/2480741.2480744

Emmanuel C Ifeachor and Barrie W Jervis. 2002. *Digital signal processing: a practical approach*. Pearson Education.

Lucas Introna and Helen Nissenbaum. 2010. Facial Recognition Technology A Survey of Policy and Implementation Issues. (2010).

John M Irvine, Steven A Israel, W Todd Scruggs, and William J Worek. 2008. eigenPulse: Robust human identification from cardiovascular function. *Pattern Recognition* 41, 11 (2008), 3427–3435.

Fumitada Itakura. 1975. Minimum prediction residual principle applied to speech recognition. *Acoustics, Speech and Signal Processing, IEEE Transactions on* 23, 1 (1975), 67–72.

Rabia Jafri and Hamid R Arabnia. 2009. A Survey of Face Recognition Techniques. *JIPS* 5, 2 (2009), 41–68.

Anil Jain, Lin Hong, and Sharath Pankanti. 2000. Biometric identification. *Commun. ACM* 43, 2 (2000), 90–98.

Anil K Jain, Ruud Bolle, and Sharath Pankanti. 1999. *Biometrics: personal identification in networked society*. Springer.

Anil K Jain and Arun Ross. 2004. Multibiometric systems. *Commun. ACM* 47, 1 (2004), 34–40.

Anil K Jain, Arun Ross, and Salil Prabhakar. 2004. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology* 14, 1 (2004), 4–20.

Tejas Joshi, Somnath Dey, and Debasis Samanta. 2009. Multimodal biometrics: state of the art in fusion techniques. *International Journal of Biometrics* 1, 4 (2009), 393–417.

A Reşit Kavsaoğlu, Kemal Polat, and M Recep Bozkurt. 2014. A novel feature ranking algorithm for biometric recognition with PPG signals. *Computers in biology and medicine* 49 (2014), 1–14.

James Kennedy. 2010. Particle swarm optimization. In *Encyclopedia of Machine Learning*. Springer, 760–766.

Dong-Ju Kim and Kwang-Seok Hong. 2008. Multimodal biometric authentication using teeth image and voice in mobile environment. *Consumer Electronics, IEEE Transactions on* 54, 4 (2008), 1790–1797.

Kenji Kira and Larry A Rendell. 1992. A practical approach to feature selection. In *Proceedings of the ninth international workshop on Machine learning*. 249–256.

J Kittler, A Hilton, M Hamouz, and J Illingworth. 2005. 3D assisted face recognition: A survey of 3D imaging, modelling and recognition approachest. In *Computer Vision and Pattern Recognition-Workshops, 2005. CVPR Workshops. IEEE Computer Society Conference on*. IEEE, 114–114.

John R Koza. 1992. *Genetic programming: on the programming of computers by means of natural selection*. Vol. 1. MIT press.

Joseph B Kruskal and Mark Liberman. 1983. The symmetric time-warping problem: from continuous to discrete. *Time Warps, String Edits and Macromolecules: The Theory and Practice of Sequence Comparison* (1983), 125–161.

a. Kumar, V. Kanhangad, and D. Zhang. 2008. Multimodal biometrics management using adaptive score-level combination. *2008 19th International Conference on Pattern Recognition* (2008), 2–5. DOI:http://dx.doi.org/10.1109/ICPR.2008.4761879

Hindra Kurniawan, Alexandr V Maslov, and Mykola Pechenizkiy. 2013. Stress detection from speech and galvanic skin response signals. In *Computer-Based Medical Systems (CBMS), 2013 IEEE 26th International Symposium on*. IEEE, 209–214.

Andreas Lanitis. 2010. A survey of the effects of aging on biometric identity verification. *International Journal of Biometrics* 2, 1 (2010), 34–52.

Anthony Lee and Younghyun Kim. 2015. Photoplethysmography as a form of biometrie authentication. In *SENSORS, 2015 IEEE*. IEEE, 1–2.

Paul Lee, Duncan Stewart, and Jolyon Barker. 2014. *Deloitte TMT Predictions 2014*. Technical Report. Deloitte.

LG Electronics 2014. *High-speed CAN transceiver*. LG Electronics. http://www.lg.com/.

Jiayang Liu, Lin Zhong, and Jehan Wickramasuriya. 2009a. User evaluation of lightweight user authentication with a single tri-axis accelerometer. *Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services* (2009), 1–10. DOI:http://dx.doi.org/10.1145/1613858.1613878

Jiayang Liu, Lin Zhong, Jehan Wickramasuriya, and Venu Vasudevan. 2009b. uWave: Accelerometer-based personalized gesture recognition and its applications. *Pervasive and Mobile Computing* 5, 6 (2009), 657–675. DOI:http://dx.doi.org/10.1016/j.pmcj.2009.07.007

Hong Lu. 2014. Unobtrusive Gait Verification for Mobile Phones. (2014), 91–98.

Prasanta Chandra Mahalanobis. 1936. On the generalized distance in statistics. *Proceedings of the National Institute of Sciences (Calcutta)* 2 (1936), 49–55.

Davide Maltoni, Dario Maio, Anil K Jain, and Salil Prabhakar. 2009. *Handbook of fingerprint recognition*. springer.

Sebastien Marcel and José del R Millán. 2007. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 29, 4 (2007), 743–752.

Pallavi Meharia and Dharma P. Agrawal. 2015. The Human Key: Identification and Authentication in Wearable Devices Using Gait. *Journal of Information Privacy & Security* 11, 2 (2015), 80–96. http://0-search.proquest.com.wam.city.ac.uk/docview/1698428070?accountid=14510

Microsoft 2016. *Microsoft Band II*. Microsoft. https://www.microsoft.com/microsoft-band.

G.N. Mills and H. Homayoun. 1994. Wrist-worn ECG monitor. (March 1 1994). http://www.google.com/patents/US5289824 US Patent 5,289,824.

Soumik Mondal and Anup Nandy. 2012. Gait based personal identification system using rotation sensor. *Journal of Emerging ...* 3, 3 (2012), 395–402. http://www.researchgate.net/publication/233792801_Gait_Based_Personal_Identification_System_Using_Rotation_Sensor/file/9fcfd50ba42754743d.pdf

George B Moody, Roger G Mark, and Ary L Goldberger. 2001. PhysioNet: a web-based resource for the study of physiologic signals. *IEEE Eng Med Biol Mag* 20, 3 (2001), 70–75.

Claudia Nickel, Christoph Busch, Sathyanarayanan Rangarajan, and M Mobius. 2011. Using hidden markov models for accelerometer-based biometric gait recognition. In *Signal Processing and its Applications (CSPA), 2011 IEEE 7th International Colloquium on*. IEEE, 58–63.

Claudia Nickel, Tobias Wirtl, and Christoph Busch. 2012. Authentication of smartphone users based on the way they walk using k-NN algorithm. *Proceedings of the 2012 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2012* (2012), 16–20. DOI:http://dx.doi.org/10.1109/IIH-MSP.2012.11

Nargess Nourbakhsh, Yang Wang, Fang Chen, and Rafael A Calvo. 2012. Using galvanic skin response for cognitive load measurement in arithmetic and reading tasks. In *Proceedings of the 24th Australian Computer-Human Interaction Conference*. ACM, 420–423.

Nymi 2015. *Nymi Band*. Nymi. https://nymi.com/.

Saurabh Pal and Madhuchhanda Mitra. 2012. Increasing the accuracy of ECG based biometric analysis by data modelling. *Measurement: Journal of the International Measurement Confederation* 45, 7 (2012), 1927–1932. DOI:http://dx.doi.org/10.1016/j.measurement.2012.03.005

E. Pasero, E. Balzanelli, and F. Caffarelli. 2015. Intruder recognition using ECG signal. In *2015 International Joint Conference on Neural Networks (IJCNN)*. 1–8. DOI:http://dx.doi.org/10.1109/IJCNN.2015.7280740

Hanchuan Peng, Fulmi Long, and Chris Ding. 2005. Feature selection based on mutual information criteria of max-dependency, max-relevance, and min-redundancy. *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 27, 8 (2005), 1226–1238.

Konstantinos N Plataniotis, Dimitrios Hatzinakos, and Jimmy KM Lee. 2006. ECG biometric recognition without fiducial detection. In *Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the*. IEEE, 1–6.

Salil Prabhakar, Sharath Pankanti, and Anil K Jain. 2003. Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy* 1, 2 (2003), 33–42.

J Ross Quinlan. 2014. *C4. 5: programs for machine learning*. Elsevier.

M. Rahman, B. Carbunar, and U. Topkara. 2016. Secure Management of Low Power Fitness Trackers. *IEEE Transactions on Mobile Computing* 15, 2 (Feb 2016), 447–459. DOI:http://dx.doi.org/10.1109/TMC.2015.2418774

N. L. Ramanathan. 1964. A new weighting system for mean surface temperature of the human body. *Journal of Applied Physiology* 19, 3 (1964), 531–533.

Kasper B Rasmussen. 2014. Authentication Using Pulse-Response Biometrics. *Ndss* February (2014), 23–26.

Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. 2001. An Analysis of Minutiae Matching Strength. *Audio- and Video-Based Biometric Person Authentication* 2091 (2001), 223–228. DOI:http://dx.doi.org/10.1.1.87.8743

Christian Rathgeb and Andreas Uhl. 2011. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security* 2011, 1 (2011), 1–25. DOI:http://dx.doi.org/10.1186/1687-417X-2011-3

a. Reşit Kavsaoğlu, Kemal Polat, and M. Recep Bozkurt. 2014. A novel feature ranking algorithm for biometric recognition with PPG signals. *Computers in Biology and Medicine* 49 (2014), 1–14. DOI:http://dx.doi.org/10.1016/j.compbiomed.2014.03.005

Kenneth Revett. 2008. *Behavioral biometrics: a remote access approach*. John Wiley & Sons.

Douglas A Reynolds and Richard C Rose. 1995. Robust text-independent speaker identification using Gaussian mixture speaker models. *Speech and Audio Processing, IEEE Transactions on* 3, 1 (1995), 72–83.

Salvatore M Romano and Massimo Pistolesi. 2002. Assessment of cardiac output from systemic arterial pressure in humans. *Critical care medicine* 30, 8 (2002), 1834–1841.

Liu Rong, Zhou Jianzhong, Liu Ming, and Hou Xiangfeng. 2007. A wearable acceleration sensor system for gait recognition. In *Industrial Electronics and Applications, 2007. ICIEA 2007. 2nd IEEE Conference on*. IEEE, 2654–2659.

Mohammed Saeed, Mauricio Villarroel, Andrew T Reisner, Gari Clifford, Li-Wei Lehman, George Moody, Thomas Heldt, Tin H Kyaw, Benjamin Moody, and Roger G Mark. 2011. Multiparameter Intelligent Monitoring in Intensive Care II (MIMIC-II): a public-access intensive care unit database. *Critical care medicine* 39, 5 (2011), 952.

Hiroaki Sakoe and Seibi Chiba. 1978. Dynamic programming algorithm optimization for spoken word recognition. *Acoustics, Speech and Signal Processing, IEEE Transactions on* 26, 1 (1978), 43–49.

Stan Salvador and Philip Chan. 2007. Toward accurate dynamic time warping in linear time and space. *Intelligent Data Analysis* 11, 5 (2007), 561–580.

Sudeep Sarkar, P Jonathon Phillips, Zongyi Liu, Isidro Robledo Vega, Patrick Grother, and Kevin W Bowyer. 2005. The humanid gait challenge problem: Data sets, performance, and analysis. *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 27, 2 (2005), 162–177.

Bernhard Schölkopf, Robert C Williamson, Alex J Smola, John Shawe-Taylor, and John C Platt. 1999. Support Vector Method for Novelty Detection.. In *NIPS*, Vol. 12. 582–588.

Seraphim Sense 2016. *Angel Sensor*. Seraphim Sense. http://angelsensor.com.

Elaine Shi, Yuan Niu, Markus Jakobsson, and Richard Chow. 2011. Implicit authentication through learning user behavior. In *Information security*. Springer, 99–113.

Ken Shoemake. 1985. Animating Rotation with Quaternion Curves. In *Proceedings of the 12th Annual Conference on Computer Graphics and Interactive Techniques (SIGGRAPH '85)*. ACM, New York, NY, USA, 245–254. DOI:http://dx.doi.org/10.1145/325334.325242

Khairul Azami Sidek, Vu Mai, and Ibrahim Khalil. 2014. Data mining in mobile ECG based biometric identification. *Journal of Network and Computer Applications* 44 (2014), 83–91. DOI:http://dx.doi.org/10.1016/j.jnca.2014.04.008

Yogendra Narain Singh, Sanjay Kumar Singh, and Phalguni Gupta. 2012. Fusion of electrocardiogram with unobtrusive biometrics: An efficient individual authentication system. *Pattern Recognition Letters* 33, 14 (2012), 1932–1941. DOI:http://dx.doi.org/10.1016/j.patrec.2012.03.010

Petros Spachos, Jiexin Gao, and Dimitrios Hatzinakos. 2011. Feasibility study of photoplethysmographic signals for biometric identification. In *Digital Signal Processing (DSP), 2011 17th International Conference on*. IEEE, 1–5.

Daisuke Sugimori, Takeshi Iwamoto, and Michito Matsumoto. 2011. A study about identification of pedestrian by using 3-axis accelerometer. *Proceedings - 1st International Workshop on Cyber-Physical Systems, Networks, and Applications, CPSNA 2011, Workshop Held During RTCSA 2011* 2 (2011), 134–137. DOI:http://dx.doi.org/10.1109/RTCSA.2011.64

Richard Szeliski. 2010. *Computer vision: algorithms and applications*. Springer Science & Business Media.

Toshiyo Tamura, Yuka Maeda, Masaki Sekine, and Masaki Yoshida. 2014. Wearable Photoplethysmographic Sensors—Past and Present. *Electronics* 3, 2 (2014), 282–302.

Mohammad Tanviruzzaman and Sheikh Iqbal Ahamed. 2014. Your phone knows you: Almost transparent authentication for smartphones. In *Computer Software and Applications Conference (COMPSAC), 2014 IEEE 38th Annual*. IEEE, 374–383.

Qian Tao and R Veldhuis. 2006. Biometric authentication for a mobile personal device. In *Mobile and Ubiquitous Systems-Workshops, 2006. 3rd Annual International Conference on*. IEEE, 1–3.

Philippe Thévenaz, Thierry Blu, and Michael Unser. 2000. Interpolation revisited. *Medical Imaging, IEEE Transactions on* 19, 7 (2000), 739–758.

Issa Traore. 2011. *Continuous Authentication Using Biometrics: Data, Models, and Metrics: Data, Models, and Metrics*. IGI Global.

J. a. Unar, Woo Chaw Seng, and Almas Abbasi. 2014. A review of biometric technology along with trends and prospects. *Pattern Recognition* 47, 8 (2014), 2673–2688. DOI:http://dx.doi.org/10.1016/j.patcog.2014.01.016

Kalyan Veeramachaneni, Lisa Ann Osadciw, and Pramod K Varshney. 2005. An adaptive multimodal biometric management algorithm. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on* 35, 3 (2005), 344–356.

Adam S Venable, Randall R Williams, and Brian K McFarlin. 2013. Gender differences in skin and core body temperature during exercise in a hot, humid environment.. In *International Journal of Exercise Science: Conference Proceedings*, Vol. 2. 9.

Jakob J Verbeek, Nikos Vlassis, and B Kröse. 2003. Efficient greedy learning of Gaussian mixture models. *Neural computation* 15, 2 (2003), 469–485.

Elena Vildjiounaite, Satu Marja Mäkelä, Mikko Lindholm, Reima Riihimäki, Vesa Kyllönen, Jani Mäntyjärvi, and Heikki Ailisto. 2006. Unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Vol. 3968 LNCS. 187–201. DOI:http://dx.doi.org/10.1007/11748625_12

Saeid Wahabi, Shahrzad Pouryayevali, Siddarth Hari, and Dimitrios Hatzinakos. 2014. On Evaluating ECG Biometric Systems: Session-Dependence and Body Posture. *Information Forensics and Security, IEEE Transactions on* 9, 11 (2014), 2002–2013.

Rasha Wahid, Neveen I Ghali, Hala S Own, Tai-hoon Kim, and Aboul Ella Hassanien. 2012. A Gaussian Mixture Models Approach to Human Heart Signal Verification Using Different Feature Extraction Algorithms. In *Computer Applications for Bio-technology, Multimedia, and Ubiquitous City*. Springer, 16–24.

Haibin Wang, Jian Chen, Yuliang Hu, Zhongwei Jiang, and Choi Samjin. 2009. Heart sound measurement and analysis system with digital stethoscope. In *Biomedical Engineering and Informatics, 2009. BMEI'09. 2nd International Conference on*. IEEE, 1–5.

Yongjin Wang, Foteini Agrafioti, Dimitrios Hatzinakos, and Konstantinos N Plataniotis. 2008. Analysis of human electrocardiogram for biometric recognition. *EURASIP journal on Advances in Signal Processing* 2008 (2008), 19.

William Wu-Shyong Wei. 1994. *Time series analysis*. Addison-Wesley publ.

World Famous Electronics 2012. *Pulse Sensor*. World Famous Electronics. http://pulsesensor.com.

Roman V Yampolskiy and V Govindaraja. 2010. Taxonomy of Behavioral Biometrics. *Behavioral Biometrics for Human Identification* (2010), 1–43.

Can Ye, BVK Kumar, and Miguel Tavares Coimbra. 2011. Human identification based on ecg signals from wearable health monitoring devices. In *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*. ACM, 25.

Lei Yu and Huan Liu. 2003. Feature selection for high-dimensional data: A fast correlation-based filter solution. In *ICML*, Vol. 3. 856–863.

Zhidong Zhao and Qinqin Shen. 2011. A human identification system based on Heart sounds and Gaussian Mixture Models. In *Biomedical Engineering and Informatics (BMEI), 2011 4th International Conference on*, Vol. 2. IEEE, 597–601.