UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE CIÊNCIA DA COMPUTAÇÃO

LAURA RODRIGUES SOARES

An ECG-based Biometric Authentication System for Healthcare Internet of Things

Work presented in partial fulfillment of the requirements for the degree of Bachelor in Computer Science

Advisor: Prof. Dr. Jéferson Campos Nobre

Porto Alegre
June 2021

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
Reitor: Prof. Carlos André Bulhões Mendes
Vice-Reitora: Profª. Patricia Pranke
Pró-Reitora de Graduação: Profª. Cíntia Inês Boll
Diretora do Instituto de Informática: Profª. Carla Maria Dal Sasso Freitas
Coordenador do Curso de Ciência de Computação: Prof. Rodrigo Machado
Bibliotecária-chefe do Instituto de Informática: Beatriz Regina Bastos Haro

ACKNOWLEDGMENTS

The completion of both this work and my whole graduation course would not be possible without the aid of many people.

Above all, I would like to thank my parents for supporting me and always encouraging me whenever my morale was low. I would also like to thank my advisor, prof. Jéferson Nobre, for the opportunity to grow as a student and for the partnership I hope will go on for many years.

Many thanks are due to the Institute of Informatics of the Federal University of Rio Grande do Sul, which provided many means to its students to excel in the academic fields, and to the National Council for Scientific and Technological Development (CNPq), for supporting the project this work is part of.

And finally, I thank my friends for all the love and help in these five years. Because of them, some of the direst practical assignments resulted in funny moments and memories that I'll cherish for the rest of my life.

I would not have completed college without all the help from some of the most wonderful people I've met, and for that I'm thankful.

ABSTRACT

The use of Internet of Things technologies in the healthcare environment, (Healthcare Internet of Things - HIoT), can bring improvements in the quality of life of the patients and more convenience for the medical team in charge. HIoT devices have restricted computational power, battery, and network usage, and require specialized technologies to maintain the privacy and security of the biometric information in these circumstances. The usage of biometric signatures in patient authentication, in particular electrocardiogram (ECG) signals, is a promising research trend. Some of the reasons are the high inter-subject variability and the difficulty to forge these signatures. However, most of the existing research initiatives do not take into account the existing resource constraints in HIoT environments. The goal of this work is to develop a biometric authentication system based on the ECG signal to be applied in HIoT devices, using algorithms and technologies of low computational cost to better suit these devices' capabilities. The tests performed show that memory consumption is within the bounds considered acceptable to be applied in constrained nodes, even though the accuracy still demands some improvement.

Keywords: Authentication. biometrics. electrocardiogram (ECG). feature extraction. HIoT. security.

Um Sistema de Autenticação Biométrica Baseado em ECG para Internet das Coisas em Saúde

RESUMO

A utilização de tecnologias de Internet das Coisas em ambientes hospitalares, ou *Healthcare Internet of Things* (HIoT), tem o potencial de trazer melhorias na qualidade de vida dos pacientes e maior conveniência para as equipes médicas responsáveis. Dispositivos HIoT possuem restrições de poder computacional, bateria, e uso de rede, necessitando assim de tecnologias especializadas para manter a privacidade e segurança das informações biométricas nessas circunstâncias. O uso da assinatura biométrica do paciente para autenticação, em particular sinais de eletrocardiograma (ECG), é promissor pela sua alta variabilidade e difícil falsificação. Porém, a maioria das soluções existentes não levam em conta a restrição de recursos presente em ambientes de HIoT. O objetivo desse trabalho é desenvolver um sistema de autenticação biométrica baseado em ECG para aplicação em HIoT, empregando tecnologias de baixo custo computacional para se adequar à capacidade destes dispositivos. Testes feitos mostraram que o consumo de memória do sistema ficou dentro dos limites considerados aceitáveis para nodos restritos, apesar de a precisão ainda demandar melhorias.

Palavras-chave: Autenticação, Biometria, Eletrocardiograma (ECG), Extração de Features, Internet das Coisas em Saúde, Segurança.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

BAN	Body Area Network
CoAP	Constrained Application Protocol
DWT	Discrete Wavelet Transform
ECG	Electrocardiogram
EDF	European Data Format
EER	Equal Error Rate
FAR	False Acceptance Rate
FFT	Fast Fourier Transform
FNA	False Negative Authentications
FPA	False Positive Authentications
FRR	False Rejection Rate
HIoT	Healthcare Internet of Things
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IPI	Inter Pulse Interval
RBF	Radial Basis Function
RNG	Random Number Generator
SVC	Support Vector Classifier
SVM	Support Vector Machine
TLS	Transport Layer Security
UDP	User Datagram Protocol
WFDB	Wave Form Database

CONTENTS

1 INTRODUCTION

The use of Internet of Things (IoT) broadens the reach of the Internet and allows seamless communication between different kinds of devices, such as medical sensors, monitoring cameras, home appliances, and several others (GOPE; HWANG, 2015). Within the healthcare environment, this use is called Healthcare Internet of Things (HIoT). HIoT can bring more convenience to the medical team and greatly improve the patient's quality of life (HE; ZEADALLY, 2014). However, HIoT systems have many particularities, such as high privacy requirements, heterogeneous devices and communications, and resource-constrained end-devices and network (WANG, 2018) that demands specific applications. To protect the devices that make up a HIoT system and the physiological data they acquire, a strong authentication system in respect to these particularities is necessary.

Among several possible types of authentication, biometric ones are considered to have an advantage over traditional ones (e.g., passwords). This happens because biometric authentication relies on intrinsic characteristics of subjects that cannot be either lost or stolen (BARROS et al., 2020). In healthcare facilities, such as hospitals and nursing homes, one of the main biometric traits available is the electrocardiogram (ECG). The ECG is universal, of hidden nature, and has high variability between different subjects. These characteristics led the ECG to be the trait of choice for biometric authentication systems in an increasing number of research initiatives over the past few years (PINTO; CARDOSO; LOURENÇO, 2018). A biometric authentication system is composed of an acquisition sensor, a storage module where a template of user information is stored, and a biometric algorithm. The biometric algorithm is responsible for deciding if an identity claim is legitimate or not, using the signal from the sensor and the template from the storage. When based on ECG signal, this user template consists of either fiducial features of the user (measurements between reference points of the heartbeat) or non-fiducial features (where the entire signal is processed).

The rise in the number of works investigating the usage of the ECG signal in biometric authentication systems made it possible for several popular techniques to be analyzed in-depth. Huang et al. (2019) was able to successfully authenticate its subjects with satisfactory accuracy even when running or jumping, while in the past authentication based on ECG was only possible in adults at rest. Peter et al. (2016) developed a resource-friendly authentication protocol to identify sensor nodes attached to the same body for use on low-cost sensors of BAN (Body Area Network) platforms, while most of the existing

filters and feature detectors due to cost and size are not applicable in this environment. However, while the existing literature on the use of ECG signals for authentication is very broad, none of the surveyed works had the same combination of authentication scenario and resource requirements as presented in this work.

This work develops a biometric authentication system based on ECG signals, using low-cost techniques and algorithms, to be applied in the restricted scenario of HIoT devices. The proposed system's decision algorithm is based on Euclidean distance, a similarity metric of linear cost, and uses fiducial feature extraction from the ECG signal in order to reduce the amount of computation necessary to the authentication process. The system is then evaluated in means of computational cost, where the memory usage is mostly satisfactory, and of accuracy. The results are presented using widely adopted metrics for the evaluation of biometric systems, and discussed in detail.

The remainder of this work is organized as follows. Chapter 2 has detailed information about key concepts necessary for a better understanding of the proposed system, as well as research initiatives in which similar works are presented. In Chapter 3 further information about the scope of this work is presented, as well as the system requirements and an outline of the proposed solution. Chapter 4 has technical details about the implementation of the system, and the performance evaluation in means of accuracy and computational cost is discussed. At last, Chapter 5 presents the final considerations and future work inside this project.

2 STATE OF ART AND KEY CONCEPTS

In this chapter, several important concepts about biometric authentication systems, particularly the ones making use of the Electrocardiogram (ECG) signal, are discussed. Then, an overview of the research initiatives proposing similar systems is presented. This review of the existing literature has the purpose of investigating the most appropriate techniques to be applied in the scenario of this work, as well as the areas in which further research is due.

2.1 Background

A biometric authentication system consists roughly of three components: an acquisition module, usually a sensor used for measurement of the biometric trait of choice, a storage module, and a biometric algorithm (JAIN; ROSS; NANDAKUMAR, 2011). The biometric algorithm is responsible for taking data from the sensor, pre-processing it, extracting the relevant features, and deciding either if it matches with a template in the storage module, or not. The pre-processing phase usually consists in denoising the acquired signal, e.g. using bandpass filters, and preparing it for feature acquisition, e.g., by selecting the important parts in the chosen length (PINTO; CARDOSO; LOURENÇO, 2018). The system, then, consist mainly of a decision algorithm comparing the signal measured from the user to a template stored in a database, and appointing the user either as legitimate, in case access to the system will be granted, or as an impostor and the access will be denied.

The main goal of this work is to investigate authentication mechanisms to be applied in resource-constrained environments specifically in healthcare facilities, which led the ECG to be the selected biometric trait since it will be widely available in this circumstance. Examples of resource-constrained devices are Healthcare Internet of Things (HIoT) sensors. What makes a device to be considered resource-constrained will be further discussed in Section 3.1.

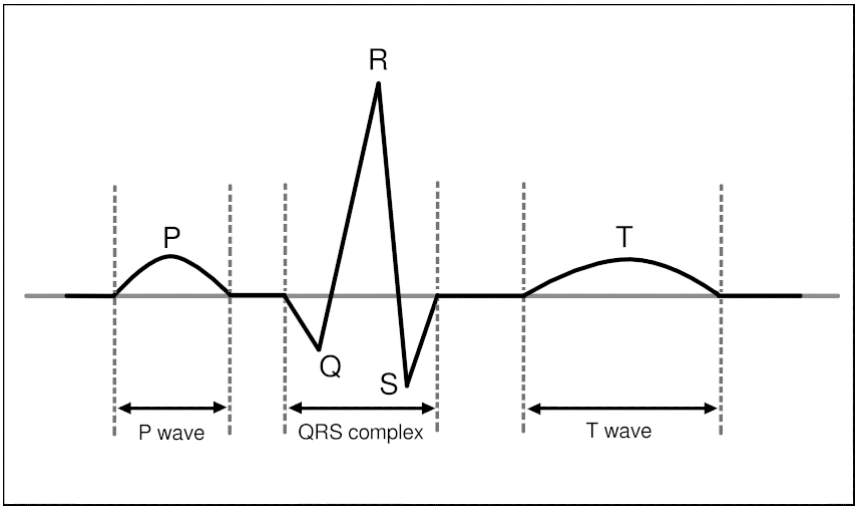
In the remainder of this Section, several key concepts about the ECG, the biometric trait of choice, will be presented. Then, the difference between signal acquisition settings will be discussed. Finally, the concept of Euclidean distance is presented and its computational complexity is discussed.

2.1.1 Electrocardiogram (ECG)

The ECG is the recording of the electrical activity of the heart, captured from a sensor in contact with the body, and usually segmented based on peak reference points (BARROS et al., 2020). It varies from person to person due to factors like heart geometry and other individual attributes, such as age and weight (HOEKEMA; UIJEN; OOSTEROM, 2001), which makes the ECG a suitable choice for a biometric recognition system.

A heartbeat is usually a cyclic repetition of five structures, the P, Q, R, S, and T waves, corresponding to the phases of depolarization and repolarization of the heart muscles. A sample of an ECG signal depicting these deflections is shown in Figure 2.1. In normal conditions, the atrial depolarization corresponds to the P wave, the ventricular depolarization to the QRS complex, and the ventricular repolarization to the T wave (BIEL et al., 2001). One heartbeat is defined as the interval between onset points of two consecutive P waves, but the beat duration is usually computed measuring two consecutive R-peaks since the R-peak detection is much simpler (CHANDRA; SHARMA; SINGH, 2018). The heart rate is the number of beats in one minute.

Figure 2.1 – A sample of ECG signal



Source: The author

Several situations can lead two separate ECG recordings from the same person to be slightly different. Some of the most common causes are cardiac conditions, such as Arrhythmia, as well as physical exercise, fatigue, and even gain of weight and pregnancy. These changes in the ECG signal of a single subject are called intra-subject variabil-

ity (PINTO; CARDOSO; LOURENÇO, 2018), and should not prevent the subject from successfully authenticating to a biometric system. In turn, inter-subject variability corresponds to the variations of heartbeats between different subjects and should be properly recognized as such by the biometric algorithm, in order to prevent an impostor from obtaining unauthorized access to the system.

It is possible to compare the whole heartbeat segment (non-fiducial approaches), but these methods usually require much more computation and are not resource-friendly in the overall. Thus, the predominant characteristics of the ECG can be translated into features and used for user authentication. Algorithms of feature detection usually find local maximum and minimum points for the P, Q, R, S, and T-peaks, which are used to calculate several features such as P, QRS, and T amplitude, each wave duration, and the R-R interval. More features related to the duration of each wave can be derived by detecting each onset and offset point.

The work proposed by Biel et al. (2001) is one of the pioneers of ECG usage in human identification. In it, the authors used the standard 12-Leads (or channels) configuration for medical acquisitions and generated a total of 360 features (30 per lead). They used correlation matrices to show the strong correlation from the same feature in different leads, therefore reducing the test set to a single lead. Further correlation helped to eliminate the features with little variability, to a final set of 10 total features. Then, a classifier with a test set of 50 subjects used these 10 features to achieve the same accuracy performance as the whole set of 360 features. After this research, several other works were based on it and explored the use of feature sets for human identification and authentication, like the work of Lugovaya (2005) and of Singh and Singh (2012).

In this work, the features used for authentication are the duration of the P, R, and S waves, of the QRS complex, and of the whole PQRST segment. The onset point of the QRS complex is also used, as well as the amplitude of the T wave, ST, and QRS complexes. This features are discussed in detail in Section 3.2.

2.1.2 Signal acquisition

The circumstances of the signal acquisition will determine the quality of the output in terms of noise and reliability. A few acquisition scenarios will be discussed in this subsection.

The acquisition settings for ECG recordings can be sorted into two broad cate-

gories: on-the-person and off-the-person settings (PINTO; CARDOSO; LOURENÇO, 2018). Each has variations in the quality of the output, due to noise and signal loss. On-the-person settings are usually medical acquisitions, performed in a healthcare facility (e.g., a hospital) with 12 sensors attached to the patient body (BIEL et al., 2001), which limits movement but results in high accuracy and less interference in the output. Holter systems are an alternative with fewer electrodes, used to record heart activity in longer periods of time on a daily basis. The off-the-person settings do not require electrodes to be placed in the patient and can be acquired by touching metallic sensors with hands or fingers, but the patient still needs to be in contact with the sensors for the reading, or else the signal will be lost. Wearables sensors are a recent approach for unconstrained, off-the-person ECG signal acquisition, but they also require constant contact with the patient's skin. Despite providing more freedom of movement to the patient, off-the-person methods are more vulnerable to external interferences that can affect the quality of the signal (SILVA et al., 2014) in comparison with the more stable on-the-person settings.

In an initial attempt of the proposed system, ECG data with on-the-person measurement settings will be acquired from the PhysioNet (GOLDBERGER et al., 2000) repository, eliminating, for now, the signal acquisition step of the system. As will be discussed in Section 2.2, several works investigating the use of ECG in biometric authentication systems also rely on PhysioBank datasets to guarantee high user variability, ideal measurement conditions, and even signals with heart conditions that might affect the performance of the biometric algorithm. More about the PhysioNet repository is discussed in Chapter 4.

2.1.3 Euclidean distance

The Euclidean distance is by far the most popular metric-based decision algorithm employed in ECG biometric systems (PINTO; CARDOSO; LOURENÇO, 2018). It is defined as the shortest distance between two points in an n-dimensional space and used as a similarity measurement in several mathematical fields.

In a two-dimensional plane, point p has coordinates (p_1, p_2), while point q has coordinates (q_1, q_2). The Euclidean distance between these points is given by

$$d(p, q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2} \tag{2.1}$$

In higher dimensional planes, the formula can be generalized as

$$d(p,q) = \sqrt{\sum_{i=1}^{n}(p_i - q_i)^2} \tag{2.2}$$

where n is the number of variables in each vector p, q.

The formula in 2.2 can be used to analyze the complexity of the Euclidean distance. It takes n subtractions of the $(p_i - q_i)$ kind, n squares of this result, $n - 1$ further sums for all the terms, and one final square root calculation. Therefore, the algorithm is at most linear $O(n)$, which is ideal for a resource-constrained environment if implemented in a low-cost language with the right programming structures.

2.2 Related Work

In the work of Choi, Lee and Yoon (2016), the ECG signal was acquired by the authors using mobile sensors. The noise removal step of the pre-processing phase was performed using band-pass filters. Eight fiducial features are then extracted (amplitude of the P, Q, R, S, and T waves, and the interval between PQ, QS, and ST peaks). Then, the authors evaluated the performance of several template-matching techniques. The classifier that performed the best was a Radial Basis Function (RBF) kernel-based Support Vector Machine (SVM), which was able to achieve 95.99% of accuracy in a single-beat authentication. The accuracy was even higher when applied in a real-life scenario using an authentication window of 15 seconds instead of the 3 seconds of the single-beat scenario.

The work of Huang et al. (2019) obtained the ECG both in PhysioBank (MIT-BIH Arrhythmia and MIT-BIH Noise Stress Test databases) and using wearable sensors, transmitted it to a processing device via a wireless channel, and denoised it using Singular Value Decomposition. The extracted features are the time length from P-peaks to R-peaks, the QR interval duration and its amplitude, and the RS interval and its amplitude, detected using a sliding window algorithm. To measure the similarity between the acquired signal and the template stored in a database, Huang et al. (2019) uses Kullback-Leibler divergence to calculate a K value, and the subject is successfully authenticated if this value is below a given threshold. Their approach is evaluated in subjects in different situations, such as walking, running, and jumping, and was able to achieve an accuracy score of 96.21, 93.24, and 83.12, respectively, after the denoising process.

The aim of Ko et al. (2019) is to propose an adjusted method for ECG feature extraction based on the QRS complex, to be used in authentication systems. A template-matching classifier is not part of their solution, but a few of them are used in the evaluation of the proposed scheme. First, the adjusted Q^i, R, and S^i features are compared visually using graphs and tables. Then, they present an evaluation of the features using logistic regression models, SVC, Naive Bayes, decision trees, and random forests. Random forests achieved the best test accuracy, with 92.68%.

Tan and Perkowski (2017) used data from PhysioNet's databases MIT-BIH and Human-ID in their work, as well as data acquired from a mobile phone. They then applied a fast Fourier transform (FFT) bandpass filter for noise removal. For the feature extraction phase, the authors used both fiducial and non-fiducial features of the ECG to propose a two-stage classifier, in order to improve overall accuracy. Non-fiducial approaches for feature extraction use the entirety or segments of the signal to extract waveform morphology information, in circumstances where fiducial features detection is unreliable (PINTO; CARDOSO; LOURENÇO, 2018). In the work of Tan and Perkowski (2017), discrete wavelet transform (DWT) is used for the non-fiducial feature extraction. The fiducial feature detection is made using a combination of the method proposed by Pan and Tompkins (1985) with a shifting window algorithm. Finally, the accuracy is evaluated using two different classifier algorithms. First, a probabilistic random forest classifier is used for the fiducial features, and then a one-to-many template matching classifier based on wavelet coefficients is used for the non-fiducial features. The two-stage classifier algorithm was capable of achieving 99.52% of authentication accuracy in a dataset with 184 subjects.

The challenge in Peter et al. (2016) is to have two different sensors attached to the same body authenticating to each other, provided they can acquire the same features from measuring the ECG of the subject, in a resource-constrained environment. The authors used the data acquired by their own custom hardware setup, complete with a sensor board and a MATLAB interface embedded to a Raspberry Pi. The selected feature for comparison was mainly the Inter Pulse Interval, obtained through the detection of Q, R, and S-peaks using the Pan and Tompkins (1985) algorithm. They tested False Negative Authentications (FNA) and False Positive Authentications (FPA) with different noise rates and deviation tolerance and were able to achieve 0% FNA and 0% FPA.

Camara et al. (2018) used the ECG signal acquired from low-cost ECG sensors in a BITalino board as input on the design of a Random Number Generator (RNG), to be employed in tasks such as session key generation or providing random numbers for

authentication protocols. The final product is the highly entropic bits extracted from the ECG signal, to be used as seeds for a key generation algorithm in a later authentication phase. The ECG signal is pre-processed using Wavelet Decomposition for the randomness extraction, and, due to the nature of the proposed application, there is no need for any template matching technique. They measured the quality of the extracted random bits by calculating the Hamming distance between the random numbers generated by each subject and concluded that the probability of an adversary to predict the values was zero.

The goal of the work of Seepers et al. (2015) was also to use ECG as a source of entropy for heartbeat-based security keys. They used the MIT-BIH Arrhythmia dataset, as well as the Rest-and-Exercise dataset from the BioSec ECG database. There is no template matching algorithm, and instead, the measurement of several IPI (Inter Pulse Interval), called ImPI, is used to generate a secure key to be employed in the communication between the two sensor devices without the need of a key-exchange protocol. The least significant bits of the ImPI signal are used as an entropy source for enhancing the security of the key, and the measured ImPI entropy bits are evaluated using Key Strength metrics and Hamming Distance.

Table 2.1 shows a summary of the surveyed existing works in a similar scope as this work. While several of them have similar authentication scenarios (a decision algorithm authenticating a user to a system through template-matching), not all of them have resource-constrained environments to work with. Very few present the proposed system performance in computational cost. The work of Peter et al. (2016) have similar resource requirements as this work, but the authentication scenario varies greatly. Therefore, further work is necessary to achieve the requirements of the proposed authentication system, using the most low-cost techniques and achieving suitable accuracy.

Table 2.1 – Overview of related works

Author	Signal Acquisition	Feature Extraction	Decision	Results
Choi, Lee and Yoon (2016)	By the authors using mobile sensors	Fiducial features extraction by R-peak detection	Support Vector Machine (SVM)	ACC(%) 95.99 EER(%) 4.46
Huang et al. (2019)	MIT-BIH Arrhythmia, MIT-BIH NST, by the authors using wearables	Fiducial features extraction using a sliding window algorithm	Kullback-Leiber divergence	ACC(%) 96.21 (walking)
Ko et al. (2019)	Not informed	Adjusted (Q^i*S^i) for fiducial feature detection	Random Forests (for the Q^i*S^i performance evaluation)	ACC(%) 92.68
Tan and Perkowski (2017)	MIT-BIH Arrhythmia, MIT-BIH Normal, Human-ID, by the authors using mobile sensors	Pan–Tompkins for fiducial features and Discrete Wavelet Transform for non-ficudial features	Random Forests for fiducial features, and One-to-Many for non-fiducial features	ACC(%) 99.54 (combined methods)
Peter et al. (2016)	By the authors using a custom sensor board	Pan-Tompkins for fiducial features detection	Simple comparasion of IPI values from different sensors	FNA(%) 0 FPA(%) 0
Camara et al. (2018)	By the authors using a low-cost ECG sensor	Wavelet Decomposition for entropy extraction	-	Hamming Distance
Seepers et al. (2015)	MIT-BIH Arrhythmia, BioSec ECG	Least significant bits of ImPI for entropy extraction	-	Hamming Distance

3 PROPOSED SOLUTION

In this chapter the scope of the broader project this work is part of is presented, and further requirements for a possible solution are elaborated. Then, the fiducial feature set used for user authentication in the proposed system is discussed in greater details. At last, the decision algorithm based on Euclidean distance that will be used for the template-matching is presented step-by-step and discussed as well.

3.1 Requirements

This work is intended as an initial step towards a lightweight ECG-based biometric authentication system to be applied in resource-constrained devices inside a healthcare environment. The ECG is the biometric trait of choice due to its wide availability in this environment, since most medical equipment already generates ECG signal for diagnosis purposes (BIEL et al., 2001). In this way, the authentication functionality could be integrated into the sensor without demanding further computation, mainly in patients limited to hospital beds. This resource optimization is important due to the mentioned limitation in the computational capability of the target devices, e.g., HIoT sensors.

Most IoT systems are a three-layer architecture divided in sensor layer, server, and gateways responsible for the communication between them (WANG, 2018), and HIoT are no exception. The sensor node is where the computational resources are the most scarce. The goal of the proposed system is to be resource-friendly enough to be applied to the sensor node of the biometric system, therefore, there is the need for the decision algorithm to be as less costly as possible.

For the classification of resource-constrained environments, there is the need of a common and succinct terminology that can roughly translate each device's capabilities (BORMANN; ERSUE; KERANEN, 2014). This terminology is available in RFC7228, published by the IETF for informational purposes. In this work, classes that divide the constrained devices regarding data and code size are proposed. Class 2 (C2) devices are said to have around 50 KiB for data (RAM size) and 250 KiB of code size. These devices, while benefiting from resource-friendly applications and protocols, would be able to communicate with the Internet using the same protocol stack as other devices (such as notebooks and servers). Class 1 (C1) devices have roughly 10 KiB or more of data size and around 100 KiB of code size. They cannot easily employ the full protocol

stack (such as HTTP and TLS) but are capable of using protocols specifically developed for constrained devices, such as the Constrained Application Protocol (CoAP) over User Datagram Protocol (UDP). C1 devices can be integrated into an IP network if careful with resource usage in its applications. The last class, Class 0 (C0), consists of the devices in the lower bound of the C1 class, with less than 10 KiB for RAM size and less than 100 KiB for code size. C0 devices, which comprises the majority of HIoT sensors, mostly do not communicate directly with the Internet in a secure manner and rely on the help of gateways. They can be preconfigured with a very small dataset and send off basic health indicators. The three classes (C0, C1, and C2) cover broadly the requirements of most HIoT devices. Further analysis will need more information about the sensor's specifications and full operational scenario.

Since the scope of this work will be handling on-the-person sensors in a medical acquisition setting, the accuracy of the ECG measurement is expected to be satisfactory. The noise-to-signal ratio is higher in this circumstance (PINTO; CARDOSO; LOURENÇO, 2018), so the denoising part of the pre-processing phase can be accomplished with simple bandpass filters which do not require extensive computation. This work will focus on the feature extraction and decision algorithm, and the acquisition of the signal, as well as the denoising step from the pre-processing phase, will be left out of the scope for now.

The final goal of the proposed system is to be employed in real-world scenarios. Therefore, it is desirable that the testing dataset would have a high degree of intra-subject variability as well as inter-subject variability, so the system can be tested to work properly even in the circumstances in which the biometric signature of a subject is slightly altered.

3.2 Feature Set Selection

Fiducial approaches in biometric authentication systems require the detection of fiducial points in the ECG signal, such as the P, QRS, and T waveforms. The noisier the input signal, the greater the difficulty in locating these features after filtering. However, for the scope of this project, on-the-person sensors in medical acquisition settings will be used, therefore making the fiducial feature detection and extraction attainable with less costly methods. Also, in this scenario, the medical equipment often produces the features for clinical diagnostic purposes, which could be reused in the authentication system.

A subset of the features used in the work from Biel et al. (2001) was selected for

evaluation in the system proposed in this work. This subset of features is either related to the duration of a fiducial event, or to their amplitude. These features are the duration of the P, R, S waves and QRS complex, the onset of the QRS complex and the time interval of the whole PQRST segment. Features in the amplitude class are the T wave amplitude, the amplitude between the S and the T-peak, and the amplitude of the QRS complex. The set of selected features is depicted in Table 3.1.

Table 3.1 – Selected feature set

Interval Features	Representation	Amplitude Features	Representation
P-QRS-T duration	$PQRST^{D}$	QRS amplitude	QRS^{A}
QRS onset	QRS^{on}	T amplitude	T^{A}
QRS duration	QRS^{D}	ST amplitude	ST^{A}
P duration	P^{D}		
R duration	R^{D}		
S duration	S^{D}		

An important class of angle-related features was left out of the scope of this work, which appears both in Biel et al. (2001) work (the ST segment slope) and in the work of Singh and Singh (2012) (Q, R and S angles). These features will be added in future corrections (see Section 4.4), with the goal of a more stable feature set consistent to changes in the heart rate of a subject.

3.3 Template matching algorithm

One of the main goals of this work is to investigate an authentication algorithm as inexpensive as possible in terms of computational cost while maintaining an acceptable accuracy in order to be suitable for real-life applications.

In authentication tasks, the goal of the system is either accept or reject an identity claim from a user registered in the database. This is easily attainable with metric-based algorithms, which are less costly than the alternative machine learning classifiers employed in identification tasks, that must sort out the correct identity through a classification process (PINTO; CARDOSO; LOURENÇO, 2018).

For use in this work, part of the authentication strategy proposed by Singh and Singh (2012) and based on Euclidean distance was evaluated due to the similarity in the chosen feature set. The complete authentication algorithm employed in the proposed system works as it follows.

A matrix $P_{(i)}$ of feature vectors for user i is populated with m vectors of d features.

The m vectors are extracted from the heartbeats in a signal excerpt of size t. More about the method for feature extraction and parsing is described in Subsection 4.2.2. In a system with n users, there are n different template matrices in the user database, where i = 1, 2,..., n. A sample vector Q with d features f' is acquired from the test vectors list.

$$P^{(i)} = \begin{pmatrix} f_{1,1} & f_{1,2} & . & . & f_{1,d} \\ f_{2,1} & f_{2,2} & . & . & f_{2,d} \\ . & . & . & . & . \\ f_{m,1} & f_{m,2} & . & . & f_{m,d} \end{pmatrix} \tag{3.1}$$

The distance between sample vector Q and each jth vector of i user's matrix $P^{(i)}$ is then measured using the Euclidean distance formula, where j = 1, 2,..., m.

$$d(Q, j) = \sqrt{\sum_{k=1}^{d} (f_k - f'_k)^2} \tag{3.2}$$

Afterward, following the algorithm proposed by Singh and Singh (2012), a final distance score between Q and the $P^{(i)}$ matrix is then generated by calculating the mean of all the m distance values. Following this algorithm, the smaller the value of the distance score between Q and $P^{(i)}$, the greater the probability of Q to belong to user i as well. The final step, then, consists in the comparison of the calculated distance score with a system threshold (T). The user will be successfully authenticated if the distance score is smaller than T, and rejected otherwise. This T value is chosen as to allow as few as possible false acceptances, while also keeping false rejections to a minimum. Further evaluation of the T value is presented in Section 4.3, and its precision is evaluated using the Equal Error Rate metric.

4 EVALUATION

This chapter focuses on the evaluation of the methods discussed in Chapter 3. For the experiments, the ECG-ID dataset was selected from PhysioBank, since it fitted the system requisites for variability and had already denoised signals. More about the ECG-ID dataset and the signal preparation step of the pre-processing phase can be found in Section 4.1. Then, further information about the development of the fiducial feature detector, the feature extractor, and the decision algorithm is presented in Section 4.2. The experiments using the decision algorithm and the database of user's features generated in Section 4.2 are presented in Section 4.3, with graphs depicting the results both of the accuracy and computational cost of the system. The obtained results are discussed at last in Section 4.4.

4.1 Dataset

This section describes the selection of the dataset, the signal preparation step of the pre-processing phase applied to it, and the assembling of the user database of templates to be used in the experiments.

The selected dataset for testing and evaluating the proposed system was the ECG-ID[1] from PhysioNet. PhysioNet (GOLDBERGER et al., 2000) provides access to a large collection of recorded physiologic signals, as well as related open-source software for processing and analysis of these signals. Both the datasets and the related software are developed and contributed by the biomedical research community. The records are stored in standard formats, such as the European Data Format (EDF) and the MIT format.

The MIT format is used in the ECG-ID dataset and is the standard for most of the data from PhysioNet. A few key concepts from this standard format are necessary for better understanding the remainder of this section. These are records, signals, samples, and annotations. A record contains a continuous recording from a single subject and is comprised of several files (signal files and annotation files, mostly). Signals, while commonly understood to be functions of time and physical variables, here will be defined as a finite sequence of integer samples. A single record usually contains several signals, that may came from different leads or be multi-channel or have filtered versions available. Samples are obtained by digitalizing a continuously observed function at a fixed sampling

[1] https://physionet.org/content/ecgiddb/1.0.0/

frequency in Hz. The time interval between adjacent samples is called a sample interval, and all sample intervals are of equal duration inside a given signal. The integer value of each sample is usually interpreted as voltage. Annotations are labels used to describe events in records, such as features (P, R, T-peaks, waveform delimiters), anomalies, and comments. The annotations are usually stored in separate files.

While several of the available datasets focus on the study of cardiac conditions, the ECG-ID database is focused on the use of ECG for biometric recognition (LUGOVAYA, 2005). It contains 310 ECG recordings of about 20 seconds each from 90 subjects, acquired using limb-clamp electrodes from Lead I (the channel acquired from electrode placement on the wrists). The number of recordings per subject varies from 2 to 20.

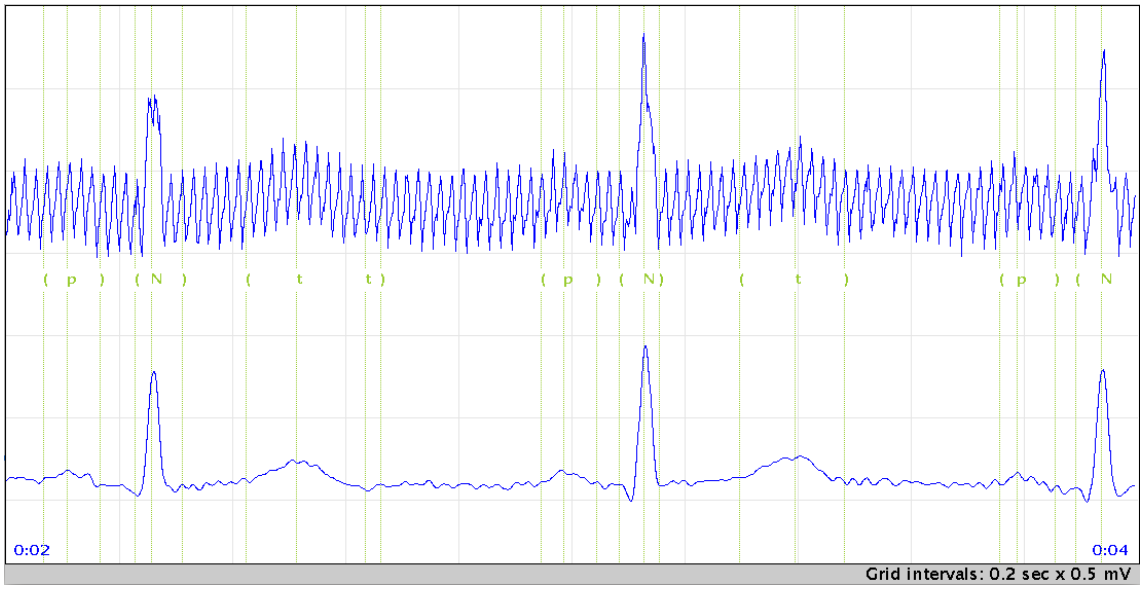
Several reasons lead the ECG-ID to be the dataset of choice. One of the main reasons is the intervals the authors introduce in the recordings of the same subject. Subject number one, for instance, has 20 recordings obtained periodically for over 6 months. These intervals between recordings greatly approaches the conditions of the recordings of a real system, where the user will generate a slightly different recording over time. In other widely used databases, such as the MIT-BIH Normal and Arrhythmia, the recordings for each subject are performed continually for long periods of time, e.g. for half an hour. Furthermore, the ECG-ID database provides both original and filtered signals for each recording, eliminating the need for extra filtering in the proposed work.

As stated in Section 3.1, a degree of intra-subject variability is necessary in the stored templates in the user database, so the system can be evaluated as closely as possible to a real-scenario application. Therefore, the selection criteria for the assembling of the user base of the proposed system was the number of records per subject available in the dataset. We selected the subjects from the ECD-ID database with a satisfactory number of recordings to provide the desired degree of intra-subject variability. Of the 90 total subjects, 25 had at least 4 recordings each and were pre-selected to be analyzed further. In cases in which more than 4 records were available, the selected 4 to be used in the feature extraction phase were selected randomly. The imposters set followed similar selection criteria. In order to be as diverse as possible, 15 imposters were picked randomly of the 16 subjects with a total of 3 recordings.

4.1.1 Signal preparation phase

The input ECG signal needs to be as clear as possible in order to accurately extract the necessary features for authentication. Some of the recordings of the pre-selected 25 subjects had far too much noise to be of any use, even after the filtering process. An example of such a case can be found in Figure 4.1. In this case, the noise caused the S point to be completely filtered out of the signal, which led to erroneous extraction of fundamental features such as the ST amplitude.

Figure 4.1 – Noisy signal makes it impossible to detect S point

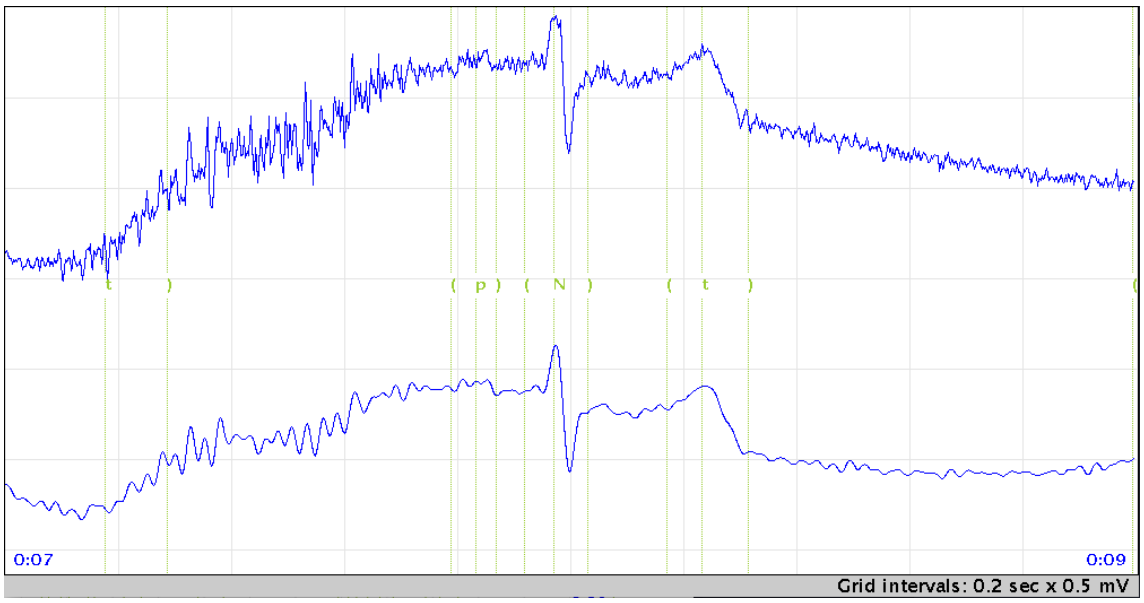


Source: The author

In other cases, some of the selected record from one of the pre-selected 25 subjects was found to be corrupted by a noise peak or measurement errors, which caused the feature detection application described in the next session to be unreliable. In both cases of excessively noisy records and of records corrupted by errors, the defective record was switched for another of that subject's records, if available. In the cases that more records were not available, further analysis of the defective recording was made. A few records, such as shown in Figure 4.2, could be corrected by snipping out the corrupted length and saving the rest of the record. Auxiliary software from the PhysioNet database was employed in this task, to copy excerpts of records to new records. E.g., in Figure 4.3, the first 1.2 seconds of the record was removed, and the remaining of the record could be used. In cases in which the recording could not be properly processed even with further manipulation, the subject was discarded. This led to a final set of 20 users, with four

recordings of 20 seconds each, to be handed to the feature extraction phase.

Figure 4.2 – Noise peak generated in measurement



Source: The author

4.2 Implementation

This section describes in detail the development of the program for fiducial feature detection and extraction employed for the assembling of the testing database, and of the decision algorithm. It also describes the functionality of the auxiliary software used for accessing and manipulating the ECG records detailed in Section 4.1, as well as to aid on the detection of key fiducial points.

Since this work uses datasets from PhysioNet, a few of the software from the repository were used for reading and manipulating this data. The main software component available is the the WFDB Software Package, a large collection of specialized software for manipulating the datasets, open-sourced and available under the GNU General Public License, version 2. Its library has functions to develop specialized software for physiologic data processing, and to evaluate one's own ECG analyzer performance according to well-known standards for ambulatory electrocardiographs, such as the ones from the ANSI (American National Standards Institute). It is written mostly in C but provides related packages for use in Python, Java, and more, as well as a MATLAB toolbox.

The system proposed in this work relied on them for initial R-peak and waveform

Figure 4.3 – Delay in the start of the signal

Source: The author

delimiters detection, and then derived the remaining necessary fiducial points (such as Q and S) by analysing the parts immediately before and after the appointed peaks. After the detection of all the relevant fiducial points, the application developed by the author performed the calculations of the features in Table 3.1, and parsed each of them in the feature vectors organized in matrices per subject in the user dataset.

4.2.1 Fiducial feature detection

The initial detection of the relevant fiducial points is necessary in order to perform the computation and extraction of the selected fiducial features to be stored in each user's template. The QRS detection algorithm proposed by Pan and Tompkins (1985) is still one of the most relevant fiducial feature detectors still used, as previously discussed in Section 2.2. An implementation of this algorithm is available among the WFDB applications (the `ecgpuwave` application), and was employed to provide initial peak detection in order to derive the remaining fiducial points. It can provide waveform delimiters locations for the P and T waves as well, although with less accuracy. The `ecgpuwave` application was implemented in Fortran and requires the installation of a Fortran compiler.

Detectors in the WFDB Software Package usually generate an annotation file that can be read and translated into text format by another application or displayed graphically

Table 4.1 – Output of rdann for a record and an annotation file generated by ecgpuwave

Time(s)	Time (intervals)	Type	subtyp	chan	num
0:00.982	491	(	0	1	0
0:01.040	520	p	0	1	0
0:01.078	539	)	0	1	0
0:01.154	577	(	0	1	1
0:01.188	594	N	0	1	0
0:01.232	616	)	0	1	1
0:01.346	673	(	0	1	2
0:01.418	709	t	0	1	0
0:01.512	756	)	0	1	2

by specialized visualization software. For this translation of annotated information, the `rdann` application was employed in order to convert the `ecgpuwave` output into readable files of detected fiducial points. An example of a converted annotation file can be found in Table 4.1.

The first column contains the time of the annotation in seconds. The second column displays the time of the annotation in sample intervals, which is the time interval between any pair of adjacent samples in a given signal (see Section 4.1 for the difference between record, signal, and samples). The representation in sample intervals is related to the sampling frequency of the record, and is as precise as possible. It will be used in the subsequent computations of the proposed system. The third column has the detected annotation type. It uses '(' and ')' as wave delimiters, and 'p', 't' for the P and T peak, respectively. The 'N' corresponds to the detected R peak and is labeled as such since the detector considers it to be a 'Normal' type beat. Other mnemonics include abnormal beat types (i.e., 'A' stands for an atrial premature beat), following a standard used in various datasets from PhysioBank to document events at specific locations within a recording. The `ecgpuwave` only labels beats as 'N'. The next steps on hardening the system to detect abnormal behaviors in ECG signals is discussed in Section 4.4. The subtyp, chan, and num columns have additional information about each annotation and will not be of use.

The obtained fiducial points provided means to compute a subset of the features related to time intervals, as depicted in Table 3.1. To acquire the required data for computing the remaining relevant points, such as Q and S-peaks, as well as for calculating the amplitude-related features, the `rdsamp` application was used. It reads the selected signal from a specified record and produces a physical value for each sample in text format, since this information was not provided by the previous applications. An excerpt of the output of `rdsamp` is depicted in Table 4.2, in units of sample intervals. This excerpt

Table 4.2 – Output of rdsamp for given a record

Time (intervals)	Physical value (mV)
300	0.180
301	0.165
302	0.155
303	0.145
304	0.135
305	0.130
306	0.120
307	0.115
308	0.105

makes use of the -s flag, to select a single signal from a multisignal record, and the -p flag, to display the values of the second column in physical units (millivolts) instead of the default analog-to-digital converter units (ADU). With the information of the voltage of each sample interval, it was possible to detect the remaining fiducial points necessary for the extraction of the selected feature set.

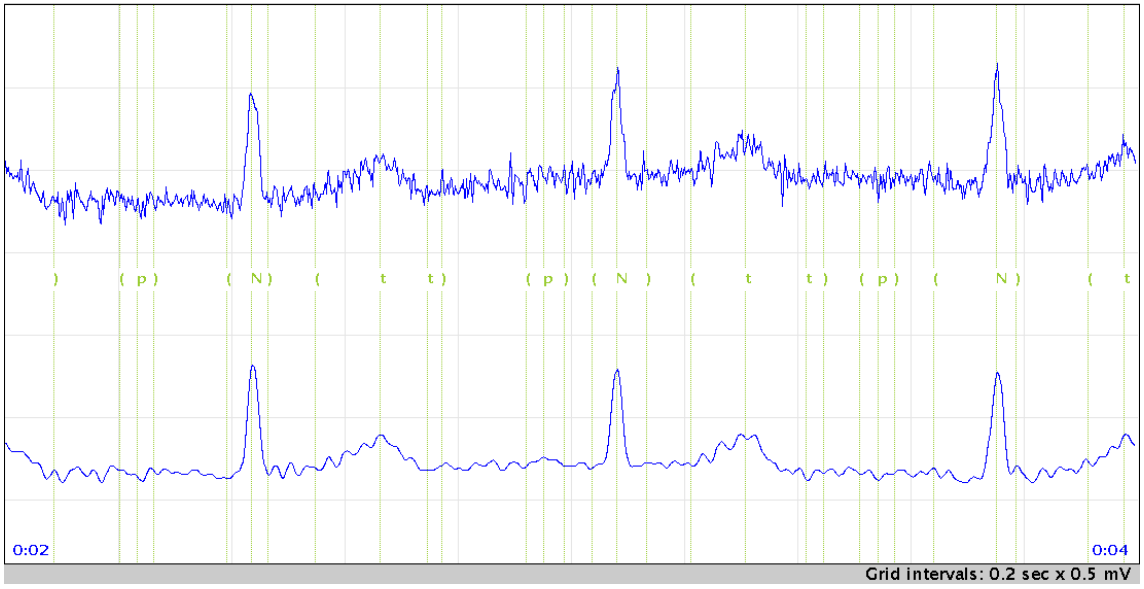
The information of each relevant fiducial point, its time in sample intervals and the corresponding voltage of it, was run through a C program for corrections and computing of further fiducial points. It used the appointed R-peaks as a reference and searched for the lowest voltage values (Q and S-peaks) before and after it. The application also set onset and offset for the R wave, using the baseline value between the P, QRS, and T deflections as reference. The application also corrected misplacement of the T-peak and QRS offset, a common occurrence in the output of the previous feature detector, as shown in Figure 4.4. The newly acquired fiducial points were inserted in the annotation file, following the correct order indexed by sample intervals, and a new column with the corresponding voltage for each of the fiducial points in type was added.

4.2.2 Feature extraction

The new annotation file now has all the necessary information for computing the feature set in Table 3.1. The P wave onset was considered the starting point of the heartbeat for the calculation of the $PQRST^{D}$ and QRS^{on} features. Each set of fiducial points between a P wave onset and a T wave offset in a record generates a feature vector complete with all the discussed features. The full list of feature vectors obtained from a record will then be parsed to populate both the user database and the testing files.

After running through the fiducial feature detector, each of the selected recording

Figure 4.4 – Noisy signal with misplaced T-peaks and QRS offset



Source: The author

discussed in Subsection 4.1.1 resulted in an average of 23 feature vectors. This number depends on the subject's heart rate that impacts the total of beats detected in the 20 seconds segment, varying from 18 to 35 in different subjects.

These 23 feature vectors per record are then run through a parser application written in C, in order to select some of them to be part of the user's template matrix and others to compose the authentication trials in the system evaluation phase. Each user's template matrix stored in the user database of the system is made from 30 feature vectors, obtained from 3 different recordings of each subject.

For the testing and evaluation of the system, a total of 30 testing feature vectors are selected per user. Five of these testing vectors are obtained from each of the same 3 recordings as the database. The remaining 15 testing vectors are obtained from the fourth recording of each subject, in hopes of further hardening the system for recognizing intra-subject variability. This results in a total of 600 legitimate authentication attempts in the evaluation phase, 30 from each of the 20 users in the database.

For the impostor trials, one feature vector is selected from each of the 3 records of each imposter. This amounts to 45 impostor vectors, to be tested against each of the 20 users' template matrices, to a total of 900 illegitimate authentication attempts.

4.2.3 Decision algorithm

The previous subsections discussed the process of assembling the user database to be used in the experiments of the proposed method, as well as the feature vectors for testing to be used in place of data acquired from a sensor in real-time. Now, the final step of the biometric authentication system is to decide if the sample vector matches with the corresponding user's template, in case the sample vector will be considered legitimate, or not, and the authentication attempt will be denied.

The algorithm in Section 3.3 was implemented in C employing optimization techniques, such as loop-unrolling and simplified mathematical expressions. The goal was to make the code as resource-friendly as possible. The program was compiled and assembled using GCC, the standard C compiler for Linux. No optimization flags for code size and execution time were employed in compilation, in order to more accurately assess the resource consumption of the algorithm evaluated.

The results of the experiments performed using the database from the feature extraction program and the decision algorithm is presented in the next section.

4.3 Results

The database assembled in Section 4.1, as well as the legitimate users' and imposters' feature vector tests, were used as input for the metric-based decision algorithm based on Euclidean distance. The goal is the evaluation of the performance of the method, both in means of accuracy and computational cost. A secondary objective is to assess the quality of the database of feature vectors assembled from the ECG-ID dataset using the feature detector developed with aid from the applications in the WFDB Software Package. The results of these tests will help to investigate the need for further work in the phases of signal acquisition, denoising, and feature extraction of the proposed biometric authentication system.

The performance analysis is evaluated in means of accuracy and computational cost. For the accuracy performance, the widely used Equal Error Rate (EER) metric is computed after testing. The computational cost in memory usage is measured using the Massif heap profile tool from the Valgrind framework. Both tests are executed with an Ubuntu 20.04 LTS system with 15,5 GiB of RAM and a quadcore, 2.70GHz CPU.

4.3.1 Accuracy

The analysis of the accuracy of the system consists in selecting a reference threshold T to be applied to the distance score from the authentication algorithm in 3.3. The authentication attempt will be considered legitimate if lower than threshold T, and rejected as illegitimate if greater than T. The goal of the system is to classify as few as possible true attempts as illegitimate, and as few as possible false attempts as legitimate.

The accuracy performance was evaluated following the False Acceptance Rate (FAR) metric for analysis of the illegitimate authentication attempts, and the False Rejection Rate (FRR) metric for the legitimate attempts. These metrics take a number of trials, previously labeled as legitimate or illegitimate, and return the percentage of wrongly decided cases for a given threshold T. The Equal Error Rate (EER) can then be calculated, defined as the value of T in which both FAR and FRR are the same. The formula for these metrics, as defined by Pinto, Cardoso and Lourenço (2018), are displayed in Table 4.3.

Table 4.3 – FAR, FRR and EER metrics

Metric	Definition
False Acceptance Rate	$FAR(T) = \frac{\text{Nº of imposter trials with score}<T}{\text{Total number of imposter trials}}$
False Rejection Rate	$FRR(T) = \frac{\text{Nº of legitimate trials with score}>T}{\text{Total number of legitimate trials}}$
Equal Error Rate	$ERR = FAR(T)$, for T that gives $FAR(T) = FRR(T)$

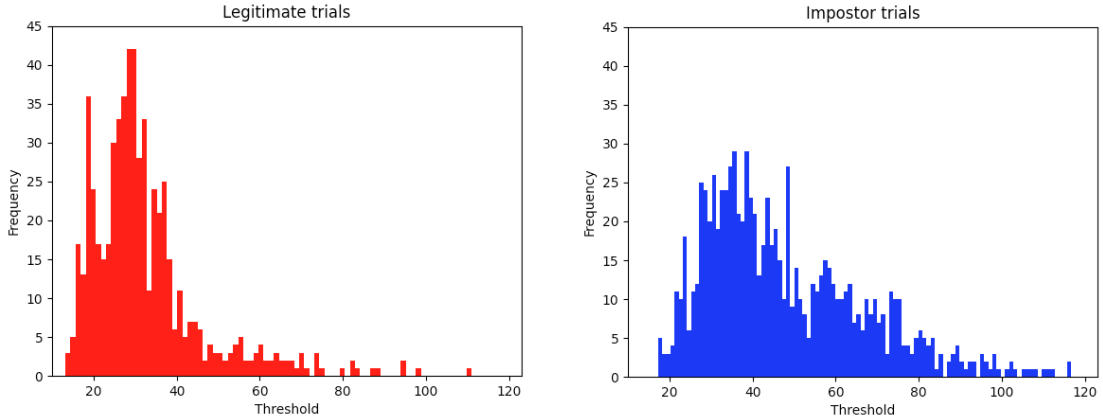
Source: Pinto, Cardoso and Lourenço (2018)

For the proposed system, as previously discussed in Section 4.2.2, the data obtained from 600 legitimate attempts and 900 illegitimate attempts were analyzed. With 20 users in the system's database, these trials correspond to 30 attempts of authentication per user and 45 imposter trials per legitimate user.

A simple histogram of the algorithm computed threshold values for both legitimate and illegitimate trials can be found in Figure 4.5. In the legitimate authentication attempts (Figure 4.5a), the threshold values peaked highly in a short range between 25 and 45. The illegitimate attempts, however, despite varying in a broader range, still have an equally high occurrence in the same score values that would authenticate a user (Figure 4.5b). This means that several impostors would have successfully authenticated to the system with an ECG signal that is not the same as the ones in the database. In an ideal performance, the peaks of the legitimate curve and the illegitimate curve would be far apart from each other.

Graphic visualization of this concept is given by the EER graph in Figure 4.6. This graph takes both FAR and FRR values to each computed threshold and places them

Figure 4.5 – Threshold values per authentication attempt
(a) Legitimate authentication attempts (b) Illegitimate authentication attempts



Source: The author

together. The EER is in 28%, which means that no matter the threshold value selected for the system there would be a substantial amount of both users wrongly rejected and imposters successfully authenticated.

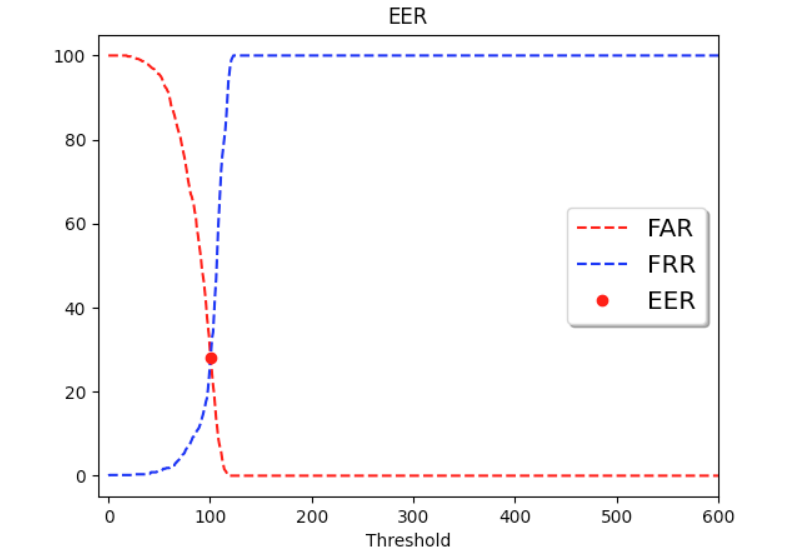
This EER value is still high above the state-of-art biometric authentication systems in Section 2.2. Several factors may have caused this, such as noise in the input signal and imprecision in the feature detection. Further discussion on these factors, as well as the next steps for improving the results can be found later in this chapter (Section 4.4).

4.3.2 Computational cost

The performance in means of computational cost concerns specifically the memory usage of the decision algorithm based on Euclidean distance. For this analysis, Valgrind's tool Massif was used to measure the total memory allocated by the application (both heap memory usage and the size of the program's stack).

A graph of memory usage per time was generated for better visualization of the results. The test consisted of a single authentication attempt from a legitimate user, shown in Figure 4.7, and a succession of ten authentication attempts also from a legitimate user, in Figure 4.8. The initial peak in memory consumption, reaching 7.2 KiB in both tests, represents the user's template matrix being loaded into memory. The following section of the graph shows the remaining Euclidean distance calculation between the test vector and

Figure 4.6 – Equal error rate of the proposed system



Source: The author

each of the 30 vectors in the user's template, as discussed in Section 3.3. The memory usage in this phase of the program does not exceed 2 KiB.

It is possible to conclude from the tests that the total cost of the program is suitable even for Class 0 devices. This is the most resource-constrained class defined in RFC7728 (BORMANN; ERSUE; KERANEN, 2014), with less than 10 KiB of memory available for data (i.e. RAM size). Even if more features are necessary for accuracy improvement, the system is still far behind in crossing the bounds of Class 2 devices and could easily increase the memory usage for doing so. With this result, it is safe to conclude that the proposed system would be suitable for HIoT devices in means of resource capabilities.

4.4 Discussion

Several points have had a substantial impact on the performance of the proposed system in means of accuracy. First, while trying to guarantee high intra-variability from the ECG-ID database, some of the records used had more noise than average. This led to the loss of relevant features of the signal in the filtered versions, such as happened in Figure 4.1, and resulted in poor performance of the feature detector that could be better if all the recordings were equally precise. The feature detector, while modified by the author to detect extra fiducial points in addition to the P, R, and T-peaks, was not always

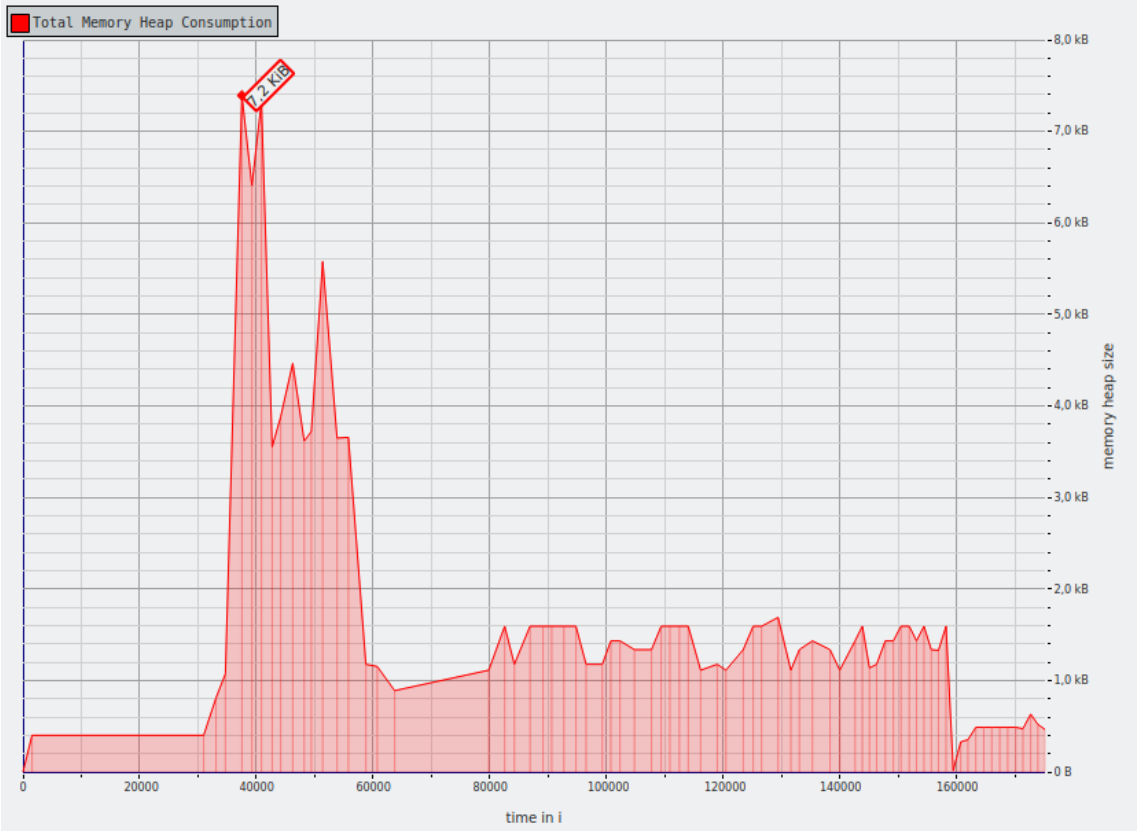
reliable in its accuracy. This led to erroneous identification of structures such as the T wave. Figure 4.4 in the previous chapter has an example of this behaviour. This caused an impact in the computation of important features such as the $PQRST^D$, T^A, and ST^A, and caused the similarity between two feature vectors, from signals that would otherwise be identical, to decrease.

The performance of the feature detector combined with the noisy records resulted ultimately in the overall threshold of the system to increase greatly. The consequence of a high threshold is the high percentage of the EER value, shown in Figure 4.6 to be 28%, which means that the number of false positives and false negatives will be high no matter the threshold.

The performance in means of computational cost, in turn, was highly satisfactory. As shown in Figures 4.7 and 4.8 the total memory consumption of the program as no higher than 10 KiB, which is suitable for Class 0 devices and have even room for increase without crossing the resource boundaries of these devices.

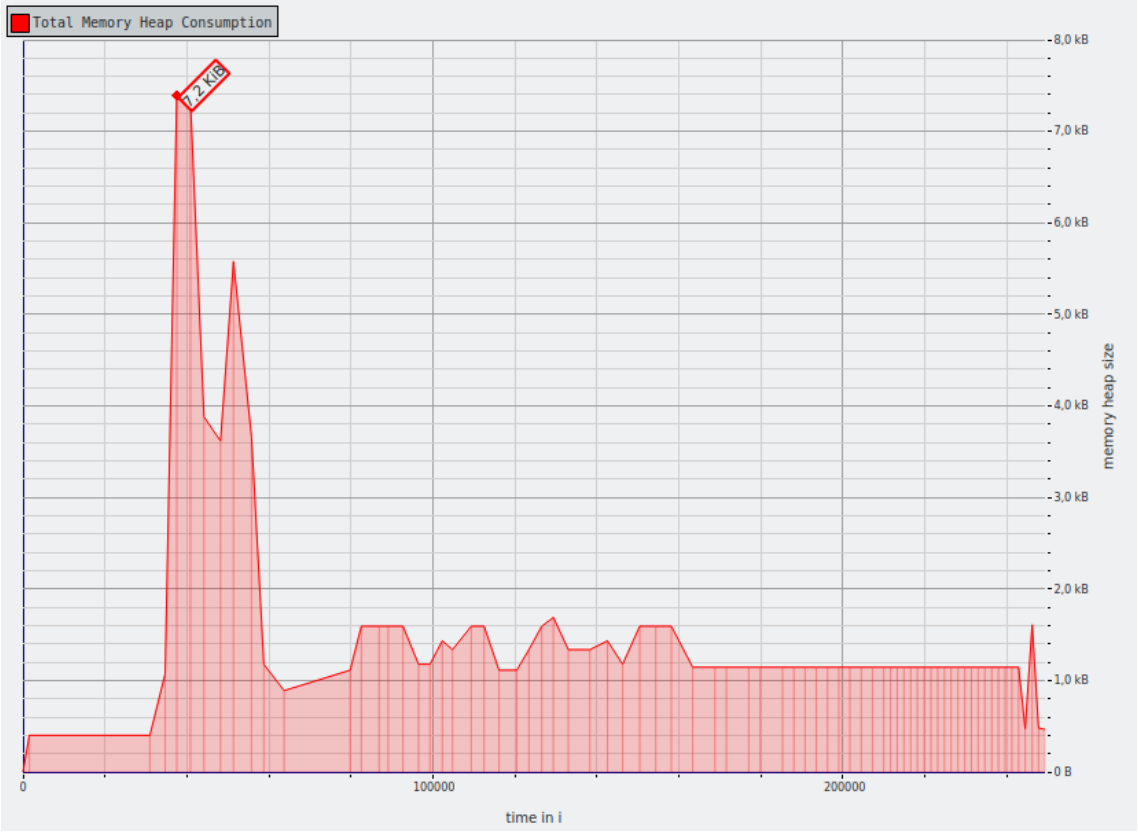
A necessary next step must evaluate if the accuracy can be improved only by the refinement of the input signal and feature vectors, or if there is the need to reevaluate the Euclidean distance algorithm in exchange of greater memory usage. This issue, as well as the future work inside this project, will be discussed in detail in Chapter 5.

Figure 4.7 – Memory usage for one authentication attempt



Source: The author

Figure 4.8 – Memory usage for ten successive authentication attempts



Source: The author

5 FINAL CONSIDERATIONS

In the present work, an ECG-based biometric authentication system employing resource-friendly techniques and algorithms had its performance analyzed in means of accuracy and computational cost. Besides, the implementation decisions were based on a review of related works in the existing literature proposing similar systems but with different sets of requirements.

The results, while highly satisfactory in the computational cost analysis, have room to improve in their accuracy. The total memory consumption of the template-matching program based on Euclidean distance was under 7.2 KiB, but the EER metric, widely used in the evaluation of the accuracy of this kind of system, was not yet acceptable for use in a real-life scenario, with a 28% equal error rate.

The next steps for corrections, after this initial assessment of fiducial feature extraction and performance in authentication analysis, will be focused on improving the quality of the feature extractor and better quality input signals. A feature extractor will be developed from scratch in a resource-friendly language like C, following the method described by Pan and Tompkins (1985) and improved using shifting windows such as described by Tan and Perkowski (2017). Both the refactoring of the feature extraction and the improvement of the input signals aim to reduce incorrect measurement in the feature vectors to a minimum.

After these corrections, the focus will be on the refinement of the features and the feature vectors. As suggested by Singh and Singh (2012) in their work, the impact of normalization of the features related to time intervals will be tested, with the goal of reducing the impact of changes in the heart rate of a subject. Computing the feature vectors using the mean of three or more beats instead of a single beat may lead to more consistent results as well. The new feature extractor will also be complemented to include angle-related features, such as the ST slope, that may be more stable and consistent across different measurements. New decision algorithms will only be investigated after this optimization of the feature set, in case the Euclidean distance fails to deliver sufficient accuracy. In this case, metric-based algorithms will be preferred, due to the HIoT resource requirements. Only after an adequate accuracy has been attained in the previous steps, the system will go through a hardening process to work properly in situations where the subject's ECG signal is slightly altered, such as fatigue and heart conditions.

The number of works making use of ECG biometrics has raised considerably in

recent years (PINTO; CARDOSO; LOURENÇO, 2018), but most of this research has not yet translated directly into real-life applications in healthcare facilities. A few exceptions are proprietary equipment and protocols that can not be acquired by every public-funded medical institution. While wearable sensors and HIoT technologies are becoming more affordable every day and could be used to improve patient well-being in these circumstances, many of them are not employed in their full capacity out of concern for the user's privacy.

This work is the first step of a broader project, focused on the development of an ECG-based biometric authentication system to be applied in resource-constrained devices in a healthcare environment, namely in HIoT sensors. After the authentication step achieves satisfactory performance, the research will move on to investigate how these ECG-based biometric signatures can be translated into credentials applied in a broader scope inside a healthcare facility. Further work on this subject will be the main research topic for the author's master's degree.

Other works inside the same project include the study of secure data transport techniques and cryptography, so the privacy of the users can be preserved, as well as a storage system based on blockchain. The final results of each module will be integrated at last, in hopes of providing a valuable contribution to the well-being and security of patients in the healthcare field.

REFERENCES

BARROS, A. et al. Data improvement model based on ecg biometric for user authentication and identification. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 20, n. 10, p. 2920, 2020.

BIEL, L. et al. Ecg analysis: a new approach in human identification. **IEEE Transactions on Instrumentation and Measurement**, IEEE, v. 50, n. 3, p. 808–812, 2001.

BORMANN, C.; ERSUE, M.; KERANEN, A. Terminology for constrained-node networks. **Internet Engineering Task Force (IETF): Fremont, CA, USA**, p. 2070–1721, 2014.

CAMARA, C. et al. Ecg-rng: A random number generator based on ecg signals and suitable for securing wireless sensor networks. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 18, n. 9, p. 2747, 2018.

CHANDRA, S.; SHARMA, A.; SINGH, G. K. Feature extraction of ecg signal. **Journal of medical engineering & technology**, Taylor & Francis, v. 42, n. 4, p. 306–316, 2018.

CHOI, H.-S.; LEE, B.; YOON, S. Biometric authentication using noisy electrocardiograms acquired by mobile sensors. **IEEE Access**, IEEE, v. 4, p. 1266–1273, 2016.

GOLDBERGER, A. L. et al. Physiobank, physiotoolkit, and physionet: components of a new research resource for complex physiologic signals. **circulation**, Am Heart Assoc, v. 101, n. 23, p. e215–e220, 2000.

GOPE, P.; HWANG, T. Bsn-care: A secure iot-based modern healthcare system using body sensor network. **IEEE sensors journal**, IEEE, v. 16, n. 5, p. 1368–1376, 2015.

HE, D.; ZEADALLY, S. An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. **IEEE internet of things journal**, IEEE, v. 2, n. 1, p. 72–83, 2014.

HOEKEMA, R.; UIJEN, G. J.; OOSTEROM, A. V. Geometrical aspects of the interindividual variability of multilead ecg recordings. **IEEE Transactions on Biomedical Engineering**, IEEE, v. 48, n. 5, p. 551–559, 2001.

HUANG, P. et al. Practical privacy-preserving ecg-based authentication for iot-based healthcare. **IEEE Internet of Things Journal**, IEEE, v. 6, n. 5, p. 9200–9210, 2019.

JAIN, A. K.; ROSS, A. A.; NANDAKUMAR, K. **Introduction to biometrics**. [S.l.]: Springer Science & Business Media, 2011.

KO, H. et al. Ecg-based advanced personal identification study with adjusted (q i* s i). **IEEE Access**, IEEE, v. 7, p. 40078–40084, 2019.

LUGOVAYA, T. S. **Biometric human identification based on ECG**. Dissertation (Master) — Faculty of Computing Technologies and Informatics, Electrotechnical University "LETI", Saint-Petersburg, Russian Federation, 2005.

PAN, J.; TOMPKINS, W. J. A real-time qrs detection algorithm. **IEEE transactions on biomedical engineering**, IEEE, n. 3, p. 230–236, 1985.

PETER, S. et al. Design of secure ecg-based biometric authentication in body area sensor networks. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 16, n. 4, p. 570, 2016.

PINTO, J. R.; CARDOSO, J. S.; LOURENÇO, A. Evolution, current challenges, and future possibilities in ecg biometrics. **IEEE Access**, IEEE, v. 6, p. 34746–34776, 2018.

SEEPERS, R. M. et al. Enhancing heart-beat-based security for mhealth applications. **IEEE journal of biomedical and health informatics**, IEEE, v. 21, n. 1, p. 254–262, 2015.

SILVA, H. P. D. et al. Check your biosignals here: A new dataset for off-the-person ecg biometrics. **Computer methods and programs in biomedicine**, Elsevier, v. 113, n. 2, p. 503–514, 2014.

SINGH, Y. N.; SINGH, S. K. Evaluation of electrocardiogram for biometric authentication. **Journal of Information Security**, Scientific Research Publishing, v. 3, n. 1, p. 39–48, 2012.

TAN, R.; PERKOWSKI, M. Toward improving electrocardiogram (ecg) biometric verification using mobile sensors: A two-stage classifier approach. **Sensors**, Multidisciplinary Digital Publishing Institute, v. 17, n. 2, p. 410, 2017.

WANG, Z. A privacy-preserving and accountable authentication protocol for iot end-devices with weaker identity. **Future Generation Computer Systems**, Elsevier, v. 82, p. 342–348, 2018.