ECG Authentication for Mobile Devices

by

Juan Sebastian Arteaga Falconi

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
In partial fulfillment of the requirements
For the M.A.Sc degree in
Electrical and Computer Engineering

Ottawa-Carleton Institute for Electrical and Computer Engineering
School of Electrical Engineering and Computer Science
Faculty of Engineering
University of Ottawa

Abstract

Mobile devices users are storing more and more private and often highly sensitive information on their mobiles. Protective measures to ensure that users of mobile devices are appropriately safeguarded are thus imperative to protect users. Traditional mobile login methods, like numerical or graphical passwords, are vulnerable to passive attacks. It is common for criminals to gain access to victims' personal information by watching victims enter their passwords into their cellphone screens from a short distance away. With this in mind, a Biometric authentication algorithm based on electrocardiogram or ECG is proposed. In this system the user will only need to touch the ECG electrodes of the mobile device to gain access. With this authentication mode no one will be able to see the biometric pattern that is used to unlock the devices. This will increase the protection for the users.

The algorithm was tested with ten subjects from MCRlab at the University of Ottawa at different days and conditions using a two electrode ECG phone case. Several tests were performed in order to reach the best setting for the algorithm to work properly. The final results show that the system has a 1.41% of chance to accept false users and 81.82% of accepting the right users. The algorithm was also tested with 73 subjects from Physionet database and the results were around the same, which confirms the consistency of the algorithm. This is the first approach on mobile authentication using ECG biometric signals and shows a promising future for this technology to be used in mobiles.

Acknowledgments

I would like to express my gratefully and sincere gratitude to my thesis supervisor Dr. Abdulmotaleb El Saddik for his trust, continuous support and guidance throughout my studies. With his help and supervision was possible to successfully achieve the present work and the current studies.

I would also like to express a special thanks to Ph.D candidate Hussein Al Osman for his invaluable guidance and continuous feedback throughout this research, his friendship and collaboration was very important to reach the objectives of the present work. I am also thankful to Dr. Jamal Saboune for his collaboration at the beginning of this study and also to all the people at the Discover Lab and MCRLab at the University of Ottawa for their contribution during the development of this work.

I would like to thanks my parents and all my family for their support. They have always been there for me during the hard and happy moments of my life, without their help it would have been really hard to accomplish this big step on my life.

And also like to thank my country Ecuador, that through the national government with the public institution SENESCYT they invested in my education. Without the financial support from my people, it would have been very hard to have been doing my graduate studies abroad. My gratitude and commitment to give them back the acquired knowledge.

Contents

List of Tables

List of Figures

Glossary of Terms

ECG	Electro cardiogram
TAR	True Acceptance Rate
FAR	False Acceptance Rate
Circumvention	To bypass, go around or spoof the systems
EER	Equal Error Rate
TRR	True Rejection Rate
FRR	False Rejection Rate
GAR	Genuine Acceptance Rate.
LDA	Linear Discriminant Analysis
PCA	Principal Component Analysis
K-NN	K-nearest neighbour
PCG	Phonocardiogram
DWT	Discrete Wavelet Transform
ADC	Analog Digital Converter
PRD	Percent Residual Difference
CCORR	Correlation Coefficient
WDIST	Wavelet Distance Measure
FCR	Fail to Capture Rate

Chapter 1.

Introduction

Authentication is the process of verifying an individual that is trying to access a system, in order to confirm that he is registered on that system, and to grant him access if he is authorized [1]. This marks the difference with the identification process, where the input is compared to a database of information stored in the system. This will determine who the user at the input is among the users stored in the database [1]. The extraction of information might be the same in both systems, but the process will differ.

There are several ways to authenticate; the most common is by means of a password, which can be a secret code or pattern. However, the latest authentication trends involve biometrics that is the process of authentication by using the unique physiological characteristics of the individuals such as the fingerprints, hands, face, iris, retina, hand signature, voice, ECG, and gait, among others. These systems tend to provide greater security than password or number based systems [2].

Biometrics have been implemented in different systems, but are rarely used on mobile devices because of current issues like time and the fragility of the physiological characteristic, which can easily be damaged if exposed [2]. Fingerprints can be easily damaged because of its constant interaction with objects, but ECG is an inherent vital signal that cannot be easily damage [3]. This damage can only be caused by affecting the cardiac function that will be related with health issues.

This work proposes a different approach, where ECG is used in mobile devices as a biometric method to authenticate users, therefore changing the way to login. The user could simply touch the device using fingers

from both their hands, in order to gain access. The position, the number of fingers, or which finger is used does not affect the process, making it easier for the user to login.

1.1 Problem Statement

Mobile smart devices have become indispensable gadgets for numerous functions. Users are becoming more comfortable with the idea of storing highly private information such as emails, photos, and other sensitive documents on such devices. The popular mobile login methods rely on numerical or graphical passwords. These techniques are vulnerable to passive attacks instigated by individuals watching from a short distance in order to see the phone screen or the movement of the fingers with the goal of stealing the password.

Biometric systems offer better security mechanism over traditional authentication methods [2], like password based, given the fact that the "password" in biometrics is a unique physiological characteristic that is always present and, depending on the method used, may not be visible to other people. However, one concern is that some biometrics techniques have certain requirements that make it not appropriate for mobile devices. Some requirements are related with hardware complexity, processing requirements and timing.

Fingerprints are one of the most popular biometric techniques and have been used for a long time in different applications, including authentication on mobile phones. Fingerprint authentication has some issues like the possibility of damaging the print, which will cause the system to fail [4], or the trail that is left on everything that has been touched by the fingers. With the use of some latex, the system can even be spoofed [5].

ECG has the advantage of low exposure, but complex hardware is required to acquire this signal, making it hard to implement in mobile devices. In spite of this, some companies already have ECG devices available on the market that works with mobile phones [6] as for medical monitoring purposes only. They have not been used for authentication and no research has been conducted using these devices for ECG authentication. ECG signals obtained from such devices are lower quality than other ECG ambulatory devices, and this makes the authentication process more challenging.

Current ECG authentication algorithms show great results on validating users but they are not designed to work in mobile environments given the fact that these algorithms require long periods of time to capture ECG signals or needs to be combined with another biometric method in order to achieve good results. This is not viable on mobile devices, where users cannot wait long periods of time to gain access or pay more to have complex systems.

1.2 Objectives

Given the advantage of ECG as a biometric system that is not easy to access or to alter, at least for most of the users, the main objective of this work will focus on developing an algorithm that will use ECG as an authentication technique for mobile devices. This should reduce the risk of passive attacks during the authentication process on mobiles by implementing a biometric technique where the physiological characteristic is not exposed to be altered or copied in the goal of spoofing the system to gain unauthorized access.

Not all biometric methods can fit in a mobile device, but ECG monitoring is already available in the market [6]. To take advantage of this situation, it is necessary to develop an algorithm that will make ECG authentication easy to implement in mobile devices. This algorithm will allow mobiles to authenticate with fair quality ECG signals that come from affordable hardware available in the market. This would make it easy for most smart mobile device users, which, these days, is a vast majority of people, and the number tends to keep increasing.

Another objective of this work is to offer an alternative protection for mobiles from being hacked during authentication. This can be accomplished using ECG since electrical signals from the heart are not easy to access or alter [5], preventing the system from easy hijack. Also, ECG does not leave a trail, except with the medical doctor, thus making it extremely difficult to steal the physiological characteristic in the goal of spoofing the system.

This work also aims to demonstrate that ECG authentication can be performed in a mobile device by using hardware with a fair quality signal, coming from two electrodes that are touched with fingers from both hands. There is currently hardware available in the market that is used for medical monitoring purposes, and it could be embedded in mobile devices as an input for authentication or other uses.

The proposed ECG authentication algorithm for mobiles is as reliable as the traditional ones. This can be prove by comparing TAR – True Acceptance Rate – and FAR – False Acceptance Rate –, and by studying the time requirements needed to acquire ECG signals to see if they can be reduced. The time requirements need to be low to make it viable to apply to mobiles, since mobile device users cannot wait long periods of time just to gain access to their device.

1.3 Contributions

The main contribution to the present work is the new authentication method for mobile devices using ECG. This is a biometric technology that gives the user the possibility of “touch and access”. With this

option, users do not have to worry about forgetting their access password since they always have the “key” with them. A consequent benefit is the reduction of system access fraud, since ECG does not show the signal to the naked eye, making it more difficult to steal the physiological characteristic that unlocks the system. The algorithm will authenticate a user in a short time, with good accuracy and using fair quality ECG signals from hardware designed for mobile devices that uses two electrodes.

An important aspect to be considered for the correct function of the algorithm is the detection of the R peaks. Some R peak detection algorithms are process consuming, which is worth it in other applications but not in authentication. For this reason, a different R peak detection algorithm is also presented in this research, but it has not been tested for purposes other than authentication, where it has shown a good performance in time and accuracy.

1.4 Scholarly Output

The idea of having ECG authentication on mobile devices, the work that has been accomplished, and the obtained results, have provided the motivation needed to start a patenting process. The paper work has been started and a successful outcome is expected.

A journal publication has been submitted to the IEEE Transactions on Instrumentation and Measurement, and an answer from the evaluation committee is expected.

Chapter 2.

Background and Related Work

2.1 Biometrics

2.1.1 Concept of Biometrics

To understand Biometric Authentication systems, it is first necessary to describe some of the concepts that are involved in it.

Biometrics is any human physiological or behavioural characteristic that is measurable and present in everybody and that has unique differences that will not change significantly over time [7]. In other words, biometrics is any characteristic that we have been using to identify individuals, and that can now be translated to be used by a computer. An example is the way we differentiate people by their face, their body and their talk. If we are more attentive, we can even determine who is approaching by the sound they make when they walk, or we can identify somebody by observing the fingerprints. The latter is more technical and has been used in different applications as a forensic technique. Some animals, like dogs for example, can track a person by their smell.

Some of the physiological characteristics that can be used to identify a person are: face, eyes, fingerprints, and the ECG of their heart, as shown in Figure 2-1. As for behavioural characteristics, there is: signature, voice, gait, or keystroke pattern [8]; most of these have been studied and applied in different systems.

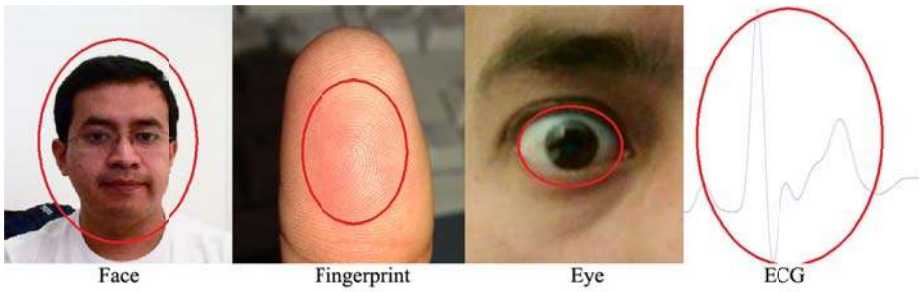

Figure 2-1: Physiological characteristics

2.1.2 Biometric Systems Accuracy

A biometric system, or just biometrics, is a pattern recognition method that uses any biometric characteristic to distinguish individuals among others by acquiring data and comparing it with previously saved data [9]. There is an important distinction that needs to be stated about biometrics; this term has been used before to refer to the collection of biological data [10], but in the present work the term will be used to refer to any biometric system.

A good biometric system needs to be accurate, fast, easy to use, applicable for most people, and able to work in the different environments in which the application might need it. This should not affect the vulnerability of the system, and will increase the user acceptability [9].

A biometric system has 4 general modules [9], as shown in Figure 2-2. These 4 elements are present in the two operation modes, identification and authentication, and are described later in this chapter. In order to work properly, both of the modes require an enrolment or training mode to be run at least once before using the system.

The training or enrolment mode works in a similar way as the identification and authentication modes. The difference is that this mode collects longer or several samples of data in order to get a more accurate template that will be the base for the identification or authentication modes [11].

- The *user interface* module is where the sensor is located and will extract the biometric features (fingerprints, eye, iris, gate, ECG, etc.). This is where the user will interact with the system.

- At the *feature extractor* module, the system will process the data obtained from the user interface, extracting only the discriminatory characteristics of the information to create a template and save it in a database if the system is in training mode, or to pass the information to the next stage if the system is in authentication or identification mode.

- In the *matcher* module, we find the algorithms to authenticate or identify. The information is obtained from the feature extractor as well as from the database and is compared. Based on the results, it will either give a positive or a negative response in the case of authentication, or an answer for the identification mode.

- The *system database* module is where the templates are stored; this can be just one template, for the verification mode, or several for the identification mode. The system database will be accessed by the feature extractor to save the information and by the matcher module to read the information.

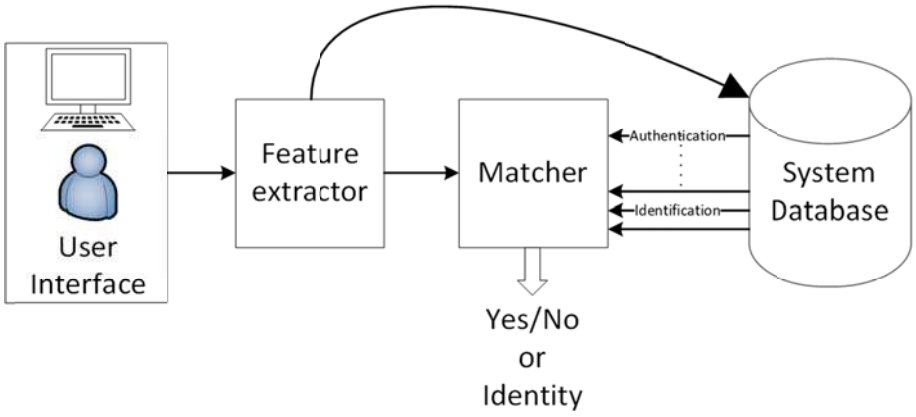

Figure 2-2: Modules of a biometric system

Another important aspect that needs to be considered in any biometric system is the errors. External and internal aspects like moisture, weather, sensors, physical conditions, etc., produce samples that are similar but never the same. This is why the implementation of a threshold is required in any biometric system [9]. The insertion of a threshold in the system will cause the system to make various errors. A very permissive threshold will result in a system that will not only validate the right users, but also the ones that are not allowed access. This is known as False Acceptance [12] and is evaluated in the system as FAR – False Acceptance Rate – where FAR is calculated using the equation (2-1):

$$FAR = \frac{\text{Total false acceptances}}{\text{Total impostor attempts}} \tag{2-1}$$

The opposite of the false acceptance is the false rejection and the false non-match, which refer to scenarios when the system has a very restrictive threshold, causing genuine users to be rejected. The system evaluation of this aspect is known as FRR [12] – False Rejection Rate – and is represented in equation (2-2):

$$FRR = \frac{\text{Total false rejection}}{\text{Total genuine attempts}} \tag{2-2}$$

FAR and FRR are terms that are dependent of the threshold. They are usually the only two values that are needed during the system testing, which is done in order to determine its reliability. Figure 2-3 shows how FRR and FAR are affected when moving the threshold over a probability density function of impostors and genuine users [12]. If the threshold is set to low FRR will be low as well, which means that genuine users will have a very low probability of being rejected when trying to access. However, this also means that the FAR will increase, making the system insecure because the probability that non authorized users will access it is also increased. On the other hand, if the threshold is too high, the opposite will happen; the probability of a false user accessing the system will be reduced as FAR is reduced, but the probability of rejecting genuine users will be increased. As a result, it will be very hard for impostors and genuine users to access the system.

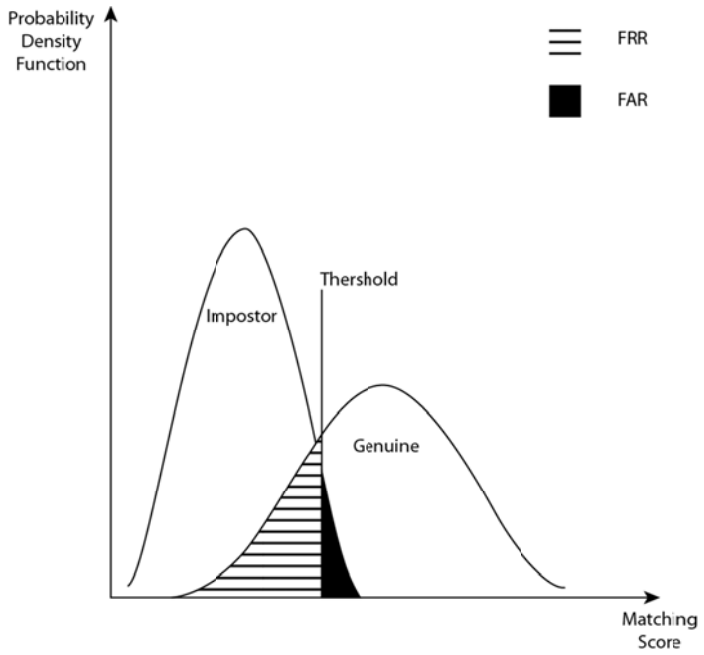

Figure 2-3: FRR and FAR as a function of the threshold [12]

When FRR and FAR are evaluated, it is desirable to have these two values as low as possible in order to ensure an accurate system. TRR is related with FAR given that TRR is the total number of true rejections against the total impostor attempts. TRR = 1-FAR, and TAR is the total true acceptances against the total genuine attempts, which is related with FRR, and TAR=1-FRR [1]. Given this analogy, a system can also be evaluated based on its FAR and TAR, where a very low FAR with a very high TAR is desirable for a reliable system. It is important to notice that in different publications the term TAR is also known as GAR, which means Genuine Acceptance Rate.

2.1.3 Operation Modes of a Biometric System

A general biometric system can work in two different modes: authentication and identification. There is an important difference between these two, and it is in how they handle the acquired information to match and grant or deny access.

Authentication or verification mode refers to a system that compares the input information against a template stored in the system. If the input matches the stored information, the system will validate a claim, otherwise it will not. This is known as one-to-one scheme [1] and is shown in Figure 2-4.

For a better understanding of the verification mode, the concept [9] is represented in expression (2-3):

$$\left(X_I, X_Q\right) \in \begin{cases} w_1, & \text{if } S\left(X_Q, X_I\right) \geq t \\ w_2, & \text{otherwise} \end{cases} \tag{2-3}$$

Where, X_Q is the biometric data at the input of the system and is generated when the user accesses the input sensor. X_I is the template or data previously stored in the system at the stage of training, and t is the threshold of the system. $S\left(X_Q, X_I\right)$ is a function that generates a score value after comparing the input data and the stored data, where the closer the values are, the higher the score. If the score reaches the set value, then the system will be in a valid stage w_1 or if not, then the system will be in a not valid stage w_2 .

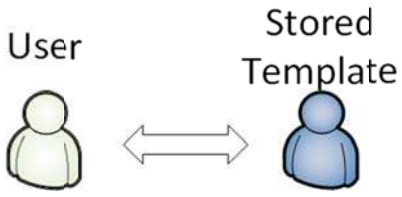

Figure 2-4: One-to-one scheme

In an identification mode, the system will determine whom the person at the input is by comparing their data against several templates stored in a database [1]. This is shown in Figure 2-5 and is known as a one-to-many scheme. Depending on the application, this can be used to give access to a system to several people or to determine which user, out of all the users in the database, is the one that is accessing the system. Similar to the authentication mode, this concept [9] is shown in expression (2-4):

$$X_Q \in \begin{cases} I_k, & \text{if } \max_k \left\{S\left(X_Q, X_{I_k}\right)\right\} \geq t, k = 1,2,\ldots,N \\ I_{N+1}, & \text{otherwise} \end{cases} \quad (2\text{-}4)$$

X_Q is the biometric data at the input of the system and is generated when the user accesses the input sensor. X_{I_k} is the database that has all the templates that correspond to all the N number of users stored in the system at the enrolling stage, and t is the threshold of the system. $\max_k \left\{S\left(X_Q, X_{I_k}\right)\right\}$ is the function that generates a score value after comparing the data at the input X_Q against all the N number of users stored in the database X_{I_k}, the k number at which the score function reaches the threshold is the user number I_k and therefore the system will tell that the input data X_Q belongs to user I_k. If the system goes through all the users without reaching the threshold, then X_Q belongs to I_{N+1}, which means that there is a non match, and the user will be rejected.

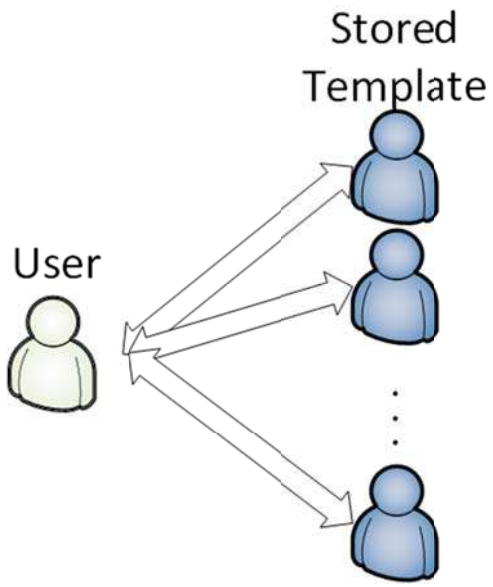

Figure 2-5: One-to-many scheme

2.2 ECG as Biometric Authentication Technique

Electrocardiogram, better known as ECG, is a method used to observe the activity of the heart by measuring and recording the electrical potential from one instant to the next. It is represented in a special graph as seen in Figure 2-6. The machine that does the work is called the electrocardiograph; it gets the information by means of conductive electrodes placed on the skin of the arms, legs, and chest wall [13].

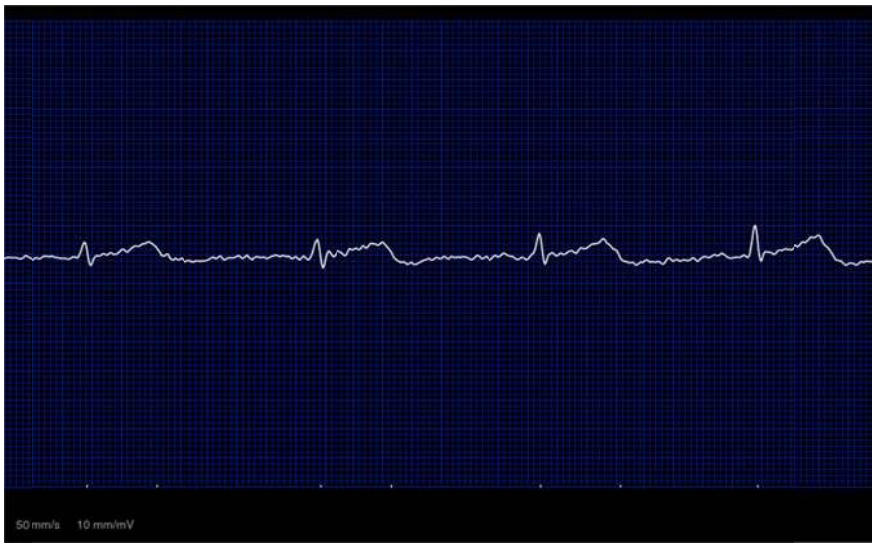

Figure 2-6: ECG graph

An ECG period has three complexes: P, QRS, and T, as it can be seen in Figure 2-7. The physical contraction of the heart muscle is known as heartbeat. This contraction is caused by the myocytes that generates chemical/potential differences. The myocytes have negatively charged interiors and a heartbeat begins with the P peak that results as a movement of ions of sodium (NA+) which causes the myocytes to depolarize and compress. From P to R it represents the depolarization that happens during atrio-ventricular (AV) conduction that slowly moves calcium (CA+) ions. The next step is the activation of QRS complex by activation of the two ventricles. The ventricles contract rapidly which produces the QRS complex. From S to T it represents the ventricular recovery [13] [14].

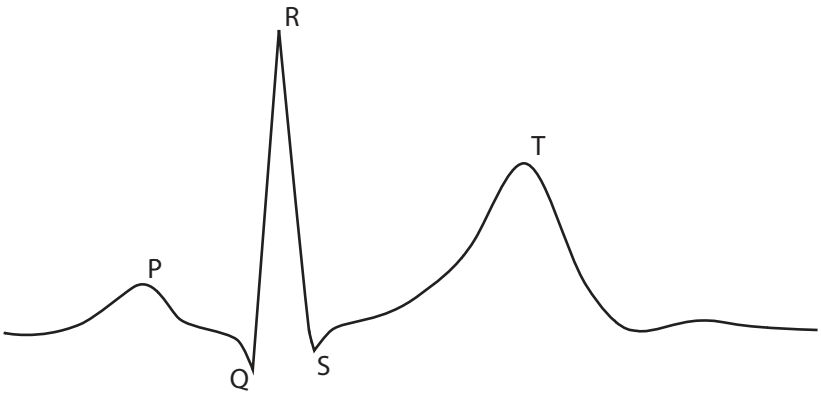

Figure 2-7: ECG complex

It is important to mention that there is a difference between leads and electrodes as these terms are often confused. Leads refer to the different placements of the electrodes that are positioned in the body and show

the variations of potentials in 12 directions. There are therefore 12 leads and they are classified as shown in Table 2-1 [15].

Lead	Position of Electrodes	Group
I	Right and left arm	Bipolar
II	Right arm and left foot	
III	Left arm and left foot	
aVL	Left arm	Unipolar (Right foot ground)
aVR	Right arm	
aVF	Left foot	
V1 to V6	6 chest electrodes	

Table 2-1: ECG leads

ECG's are different for every individual, and this is a result of age, sex, heart mass orientation, conductivity, and order of activation of cardiac muscles [16] [17] [18]. Traditional medicine has made efforts to universalize this signal in order to have a general diagnosis method that can be applied to most people [19], but this distinctiveness of ECG among individuals that might be a problem in medicine is an advantage when ECG is applied in biometrics [20].

Different studies have been performed in order to contribute to the robustness of ECG as biometric, therefore different research projects are analyzed in the following section in order to help improve some of the concepts in the present work, to reach the objectives presented.

2.3 Existing ECG Identification and Authentication Work

To prove that it is possible to identify people using ECG, Biel *et. al.* [15] used a method based on the appearance of the signal. They extract features for classification based on time, amplitudes and slopes, shown in Figure 2-8, and apply a multivariate method analysis on them. The results obtained show that it is possible, under resting conditions, to identify a person from a predetermined group of people using ECG. Also, it is not necessary to use a 12 lead configuration with 10 electrodes and extract many features that are redundant and can cause a misclassification problem. One lead – three electrodes – is enough to achieve good results, and the acquisition of data is less complicated in this configuration.

Based on the information obtained from various documents, it seems that this is the first attempt at using ECG for identification. They introduce the features that need to be extracted from ECG to proceed on identification; time requirements and the states of anxiety of the subjects are not considered.

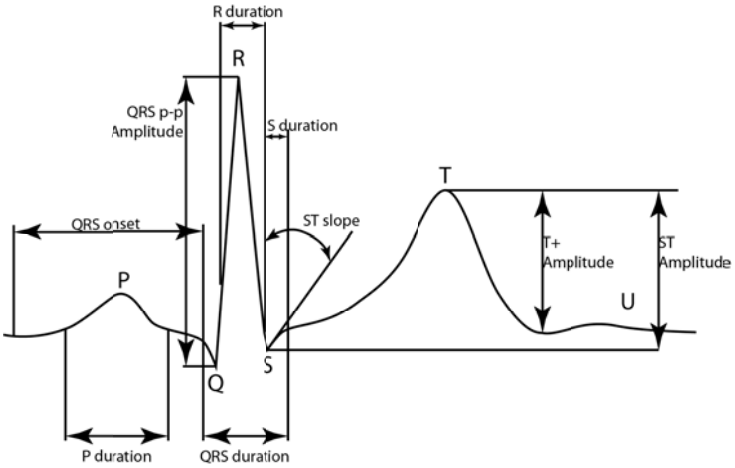

Figure 2-8: ECG extracted features

To corroborate the work of Biel *et. al.* [15], who state that only one lead is necessary, Shen *et. al.* [21] worked on human ECG identification again with one lead – three electrodes – by using two methods. First, a correlated template matching method that compares the stored signal and the signal at the input. Based on a score, they classify it as match or no match, getting an accuracy of 95%. For the second method, they use a decision-based neural network, obtaining an accuracy of 80%, where they extract only seven features to train the neural network. This is less than Biel *et. al.* [15]. Most of these features are extracted from the QRS part of the signal, and two features are from the T peak, as seen in Figure 2-9. One corresponds to QT distance, and they apply normalization to deal with heart rate changes that might affect this feature. They combined these two methods and obtained a 100% match. They applied their experiment using 20 people from the MIT/BIH PhysioNet database [22], with 20 samples for each individual. It is not clear how the results are obtained, as the measure of TAR and FAR are not mentioned, and the time required is based on the number of beats (average is 20 beats per 30 seconds). It is important to know that it is also possible to use less features for ECG identity verification.

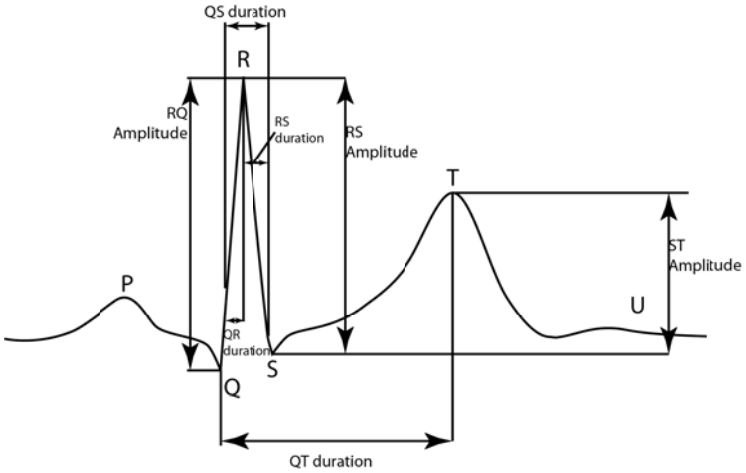

Figure 2-9: Seven features for ECG indentification

A physiological analysis of ECG and its relation to the features extracted to apply ECG identification is presented by Israel *et. al.* [14]. In this work they analyse how the heart rate changes and how each feature is affected by these changes, determining that QRS are not affected but that the secretion of neurotransmitters alters the conductivity and directly affects the length in P and T complex. The features extracted are based on time, and to solve the effects of heart rate changes in the algorithm they empirically determined that there is a linear relation in these changes, applying normalization to the features where P and T complex are involved. The normalization is done by dividing the length of each affected feature by the total length of the ECG signal, from L to T, as can be seen in the Figure 2-10. Similar features as in previous works are extracted, see Figure 2-10, but amplitudes are not considered since a change in the placement of the electrodes directly affects these values. Fifteen features are determined, but in the experiment only twelve features are used. It is performed with 29 people with samples of 20 seconds at different states of anxieties and with different electrode placement positions. The analytic classification is performed based on a linear discriminant analysis of the features, and the results obtained conclude that a correct classification can be performed even if the heart rate is affected by different states of anxiety and also independent of the placement of the electrodes.

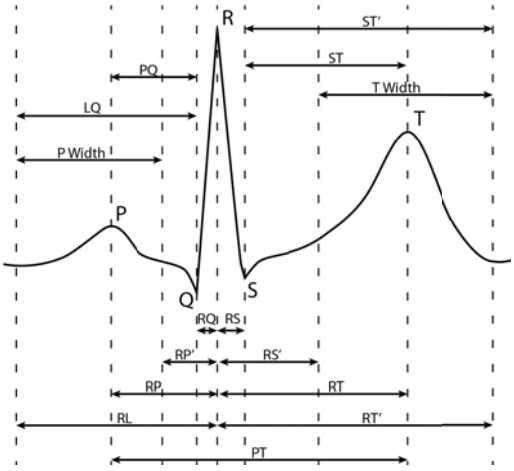

Figure 2-10: ECG features by Israel *et. al*. [14]

Different methods for classification have been applied separately to achieve ECG human identification, but Wang *et. al* [5] decided to combine two different classification methods, analytic features and appearance features, to improve the obtained results. They perform their experiments on 13 subjects, each with two records collected within a two year time lapse. The length of the records are not specified but based on the results presented it can be estimated as an average of 70 seconds per individual. At the first stage of the research they use the time domain features and apply the analytical method proposed by Israel *et. al*. [14] but they add the amplitude features of the signal and obtain an 84% identification rate. Separately, they apply an appearance based method, where they determined that a principal component analysis – PCA – with a K-Nearest Neighbour classifier – K-NN – gives the best results with a 95.55%

correct heartbeat classification. In the second stage of the research they combined these two methods, as shown in Figure 2-11, and obtained a 96.03% correct heartbeat classification.

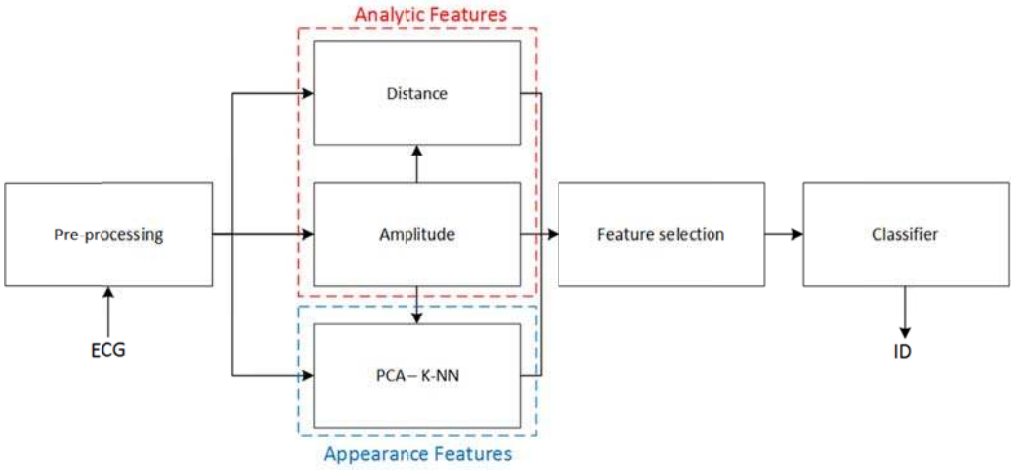

Figure 2-11: Analytic and appearance attributes fusion

When thinking about ECG authentication, one of the concerns that arises is the length of time that an ECG record can remain valid. To test that concern, Wüebbeler *et. al.* [23] perform ECG verification based on a database of 74 subjects, where their data were collected with a time difference ranging from months to years. Using recordings of 10 seconds, they compare the QRS complex part of the signal at the input, with the QRS complex part of the signal stored in the template. Applying a Euclidean distance measure, and based on a tolerance, they establish authenticity, getting up to 98.1% of correct validation. They therefore state that ECG can still be used several years after the generation of a template, even with a shorter record time.

An alternative approach to ECG authentication is done by Sufi *et. al.* [24] where they use a polynomial method and calculate the coefficients with only normal beats taken for process. These coefficients are compared and based on a tolerance error it either gives a match or not. The polynomial method is applied in a remote telecardiology application [25], where they use a mobile phone only to transmit data from a device that connects the electrodes to the body and then transmits via Bluetooth to the mobile, which sends the signal to a remote server. The server is the one that processes the information to validate the authentication. This method will access the remote server and allow the acquisition time to be reduced to 2.49 seconds because of the processing power of the server. The validation rate obtained is of 95%.

With the purpose of increasing the validation rate, Fatemian *et. al* [3] applies a multimodal biometric system that fusions two biometric techniques, ECG and PCG, applying a Quadratic Spline method that is a DWT technique for feature extraction of ECG. The experiment was performed with 21 subjects with 3 minutes sessions for each. The results obtained with just ECG show a rate of 95.12% correct recognition,

and based on the graph presented FAR and FRR can be estimated at 2%. For a PCG biometric, the rate of correct matches was 72.3%, but once they combine ECG and PCG, the rate goes up to 97%. This result shows that a higher accuracy can be obtained by using two methods and merging their results.

Another approach in multimodal biometrics is done by Singh *et. al* [26], where they analyze ECG as unimodal and multimodal separately. For the unimodal analysis, they extract 20 features from the ECG signal, including those based on time, amplitude and angles. Each feature that belongs to a subject form a matrix, see Figure 2-12, with a number of columns equal to the quantity of features "*d*", in this case 20 features, and the number of rows that corresponds to the number of ECG beats "*m*" that were extracted. This number is related to the acquisition time, therefore $f_{j,k}$ is the the *k*th feature that corresponds to the *j*th ECG beat. For each ECG beat they calculate the Euclidean distance among the 20 features extracted. After this, they will have a number of Euclidean distances that correspond to the number of ECG beats that has been acquired. Then, the mean of all these Euclidean distances is calculated which gives a score value. The lower the value, the better the match. The experiment was done with 73 subjects using the MIT/BIH Physionet database [22], with sample durations of at least 3 minutes. This time is based on records stored in the database, and some are longer. The results obtained with this unimodal biometric technique are 82% of TAR with a 7% of FAR. Their results are improved when they combined it with fingerprint and face recognition. This multimodal system gave them a TAR of 99%.

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

Figure 2-12: Individual matrix with ECG feature vectors

ECG identification can also be performed by reducing its dimension. Singh *et. al.* [27] classify ECG features by using Eigen vectors. They extract more features from the signal, five features based on time length that goes from P to T interval in a heartbeat, ten features that are measured based on the distance between two heartbeats, and sixty-one features from the amplitude of the signal. To process all these features they apply a linear projection to reduce the dimensional space using PCA. This reduction will give as a result a separation between subjects based on Eigen vectors, as each dimension of Eigen vectors corresponds to the feature vectors; the authors calls it Eigen beat features and the identification process is done by using the K-NN method. For their experiment they used two databases, 44 subjects with records of

30 minutes from the first database, and 29 subjects with records of 100 beats, which gives an average of 1 minute and 40 seconds, from the second database. The obtained results were an accuracy of 95.5% and 91.42% for each data base. The difference is that the first database has healthy subjects under resting conditions and the second one is a mix of healthy and non-healthy subjects.

To test the feasibility of using ECG for biometrics by gathering the signal with the fingers, Chan *et. al.* [20] ran an experiment with 50 subjects. To get the best results, they used three methods of classification and comparison: percent residual difference (PRD), correlation coefficient (CCORR), and they introduce a new technique for classification based on wavelet transform (WDIST). They obtain the signal from the finger tips and they use extra hardware as amplifiers and 1Khz ADC. For the training and testing, three data sessions of 90 seconds were taken from each subject, at different states of anxiety, showing different results. For PRD, where they basically measure the difference between signals, the results were up to 75% of correct matches. For the CCORR method, which quantifies a linear least squares, the results were of 82%. For the WDIST method, which calculates the wavelet coefficients and measures the distance, the results obtained were 95% accuracy. This work shows that wavelets transform can also be used for authentication at different states of anxiety.

The most common approach in mobile biometrics is the use of fingerprint, some companies already have their products in the market. There are some other approaches that have been studied in biometrics authentication for mobiles.

In a first approach Dal-ho *et. al* [28] uses a mobile to extract the Pupil and Iris for further recognition. As a result they showed that is possible to process the image and extract the features, but the authentication is not performed. They just detect these two features in different lightening conditions by using a mobile. The contribution here is the extraction process proposed that can be handled by a mobile. Behavioural characteristics have been proposed to be used as biometric authentication in a mobile.

Saevanee *et. al.* [29] evaluate keystroke dynamics and the finger pressure. The test was performed with 10 subjects by using a notebook touchpad acting like a touchscreen. Each user had to type a 10 digit phone number for 30 times. The results shows that finger pressure with 99% TAR, performed better than keystroke. The study shows that this can be implemented in mobiles as long they come with a pressure sensor touch screen. The time required to type 10 digit will vary from user to user but even for users with faster typing skills this will represent a couple seconds.

Palmprint and knuckle are also proposed to be used in a mobile as biometric authentication technique. Choras et. al. [30] run an experiment where they process images taken by mobile phones. The process of authentication is not performed in the mobile and the results obtained are very good with 1.02% of FAR.

2.4 Active Authentication

The traditional methods to authenticate are well known, like passwords or biometrics that grant access to a system as soon as the authentication process succeeds, but there is a problem when they change users. The system will keep giving them access, therefore a new authentication technique has been discussed and is called active authentication or continuous authentication, which will keep getting information from the user to see if it is still the same user working on the system. If it is not, then the system is blocked [31]. Not all the authentication methods can be used for active authentication. There are restrictions attached to biometric methods, and in this group not all the biometric techniques can be implemented for active authentication. Fingerprints or iris scans, for example, cannot be measured all the time without discomforting the user. However, face recognition or keystrokes can be used [31], as well as ECG. The latter has the advantage of being a continuous vitality signal.

A basic model for active authentication is based on time slots that are continuously checking the biometric sensor, acquiring data, and processing it to see if the information corresponds to the authorized user. The length of the time slots will vary depending on how secure the system is. If the time slots are very short, then the system is under high security and will therefore also use more resources. If the time slots are longer, the system is probably designed to work in safe environments [32].

The architecture of an active system can be summarized in three steps: scheduling where the time slots to continuously check the system are established; observation step, where the system checks the information at the biometric sensor according to the schedule and processing it to verify if the authorized user is still in the system; and deciding step that keep the system open or close it if it is or not an authorized user [32].

2.5 Conclusions

Based on all the different works that have been studied, it can be concluded that ECG can be used as a biometric technique. Some methods have better results than others based only on accuracy, but there are other ways to compare and decide which method is better, and this will vary depending on the application. Some methods might be suitable for certain systems where computation resources are high, but might not be suitable for other systems where the process power is limited. But all these methods, no matter which one is better, conclude that ECG authentication is viable to apply as biometrics. The technology needs to keep improving in aspects such as comfort, acquisition time, efficient processing, and reliability, and the present work will contribute in the progress of this technology.

One of the concerns for ECG as biometrics is in how much heart rate changes and the passing of time will affect the system. However, different studies show that heart rate changes can be well managed by the

normalization of the signal or by applying domain transformation techniques. Other tests show that the ECG pattern is invariant with time, where different samples were analyzed with a gap of months or even years to test the effect of this issue on the system. Tests performed in the different studies show that ECG authentication is not affected by these aspects if the signal is treated properly.

The placement of the ECG sensors every time a sample is required can be a problem, as this will affect features related to the amplitude of the ECG signal. If the system works with features strictly related with amplitudes it will be a problem, but most of the systems use a mix of amplitude and time features of the signal. In these cases, amplitudes will be used as an extra feature, and instead of being a problem they become helpful, especially when time features are very close between different subjects.

One way of improving ECG recognition results is the fusion of different biometric techniques, better known as multimodal biometric systems. Different studies show a very high improvement of the systems under this scheme, but when a multimodal system is used the systems stops being an exclusive ECG biometric system, therefore the ECG biometric method is not improved by the fusion, but the multimodal biometric system is. If just the unimodal ECG biometric technology can be improved, by simple analysis we can say that the multimodal system will get better as well. This, however, only works in the case where the system can afford multimodal biometrics, as some systems might be limited to the use of only unimodal biometrics. This will depend on the application and hardware resources. As an example, we can mention ECG authentication for mobiles, where a mobile device cannot hold many biometric sensors. For mobile use, ECG can be fused with face recognition, taking the advantage that most of the smart phones have a camera now, but the processing power will increase and battery life will decrease, causing discomfort in the users.

Most of the tests done by the different studies use databases to test their algorithms, but these samples might have been taken with very sophisticated hardware that some systems in real applications would not have, as with ECG authentication in mobiles for example, giving good results that might not be the same in other applications with different quality of hardware or different conditions of the subjects. Therefore, to test the system it is necessary to perform the experiments in real conditions in order to see the performance, and with the databases of other studies as a way to compare the efficacy of the systems.

An important aspect in ECG authentication is the time required to get the signal to perform the recognition. Some studies have reduced this time by changing the domain of the signal, which requires less space on the template, affecting the time needed for the samples, but they have a computer dedicated just to the processing of all the information that is sent from the system interface. The transmission link can be interrupted causing the system to block, therefore in order to prevent this problem an ECG authentication method that requires a short acquisition time without high processing techniques is required. In this mode it

can be performed locally by the system and does not require access to external components. As an example, in ECG authentication for biometrics, the whole process has to be done in the device and cannot be sent over to an external device, since there is no guarantee that the link will be available all the time.

Some people evaluate biometric systems by using EER (Equal Error Rate), where the FAR and FRR are the same, and the lower this value is, the better the system. However, other people evaluate the system by using TAR and FAR, where TAR should be very high, with the lowest FAR possible, in order for it to be considered a good system. After analysing the previous work, it is decided that this work will be analyzed by using TAR and FAR, because the main concern of authentication is the protection of the system, therefore false rejections are not as dangerous as false acceptances. If it is intended for the system to reach the same rate for FAR as for FRR, a good system with a very good FAR but with a less than great FRR could be overlooked. The FRR is directly related to the TAR, therefore an increase in FRR will decrease the TAR, but the system will still be secure and comfortable for the users.

The purpose of this work is to use ECG authentication in mobiles, therefore the ECG signal will be gathered from the fingers. As was shown in previous work, the placement of the sensors will affect the amplitude features of the system, but for the purpose of this work, the fingers will always be used. Chan et. al. [20] work corroborate the feasibility of identifying people using ECG signals coming from the fingers, but that work used a sophisticated hardware and very long ECG samples that is not likely to be applied in mobile devices, therefore a different approach is needed to use the signal that comes from hardware that is suitable to fit in a mobile device and that can perform very well with short samples that can be handled by common users.

One of the works studied used a very interesting technique which featured a vector matrix [26] that can be applied in ECG authentication for mobiles, although after some modifications, as this method does not require domain transformations that can be process consuming. Some concerns do need to be researched though, such as the improvement of the acquisition time, as it needs to be drastically decreased while maintaining or even improving the quality of the results. The signal obtained from the hardware that will be used in the real application might not work with this algorithm given the lower quality that the hardware will give. For this reason, it will be impossible to extract all the features. The number of features also needs to be decreased without affecting the reliability of the system. From this work, the main concept of the featured vector matrix can be used, but the algorithm needs to be changed to make it suitable to work in mobile devices. With the goal of achieving this objective, different contributions will come forth from this research.

Some of the approaches in biometrics mobile authentication analyzed here are not performed in the device. This can be because of processing requirements of the algorithms, but they use the mobile as a

biometric input for processing in an external computer. Comfort plays an important role at the time of using these algorithms. Therefore this aspect should be evaluated given that some methods will require taking a picture or typing a pattern that users might find not necessary or too long for authentication. Fingerprint authentication is the most used technology nowadays and some companies have already launch mobiles with this technology. Fingerprint technology has been in development for many years. This has helped to make a lot of progress in speed and accuracy if we compare with other technologies. ECG authentication is a new approach. Therefore needs to keep improving in aspects like time and accuracy. But definitely has a big advantage over fingerprint and this is the difficulty to spoof the system. The main security leak about fingerprint authentication has already been discussed in different publications and lately by different online articles. All the discussions conclude that fingerprint authentication is easy to spoof by just using some latex [33].

After analysing several works and researching various resources, it can be said that in the best of the knowledge of the people involved in this research, ECG authentication for mobile devices has not yet been studied, and that will be the main contribution of this work. Therefore, our mobile ECG authentication algorithm has to be customized for the type and quality of the signal collected using cheap ECG devices connected to the fingers. This work will also help contribute to the development of ECG as biometrics, making it useful in other applications as a form of active authentication. This is possible since ECG is a vitality signal, and the placement of electrodes in the phone will make continuous authentication possible while the user is holding the phone.

Chapter 3.

Design of an ECG Authentication System for Mobiles

3.1 Hardware Architecture

The system has two main hardware components that contain all the components that a basic biometric authentication system should have, as shown in Figure 3-1. The ECG case contains the sensor, which is where the user interface is, and transmits the data to the mobile device, which contains the feature extractor, the matcher module, and the system database, and will make the decision for authentication. In this case, since it is authentication and not identification, the database only stores one template.

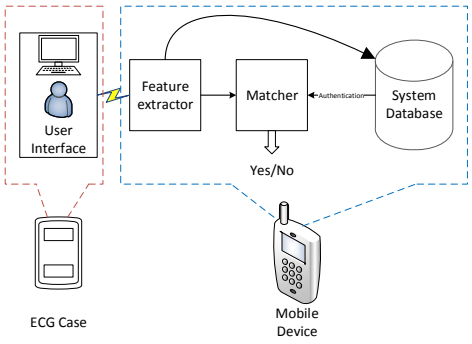

Figure 3-1: Hardware Components

3.2 Signal Acquisition

Figure 3-2: ECG phone case from AliveCor.

The signal is acquired by two electrodes that are touched by any part of the body that can cause a potential difference and allow the measurement the ECG signal. For this study, fingers from both hands are used. When the electrodes are touched, it activates a signal that the system uses as the indication to start working. In order to test the system and the algorithms, a phone case with two electrodes from Alivecor [6] has been used, as shown in Figure 3-2. Figure 3-3 shows the general acquisition scheme where the phone case transmits ECG information in a FM modulation through the audible spectrum, from 18 Khz to 20 Khz. Data is acquired in the mobile device by its microphone at a 44.1 Khz sampling frequency. It is then filtered using a bandpass filter (18 Khz to 20 khz), and a down sampling is applied with a factor of two. This will produce the aliasing of the FM signals that invert and shift the frequency spectrum to a range of 2 Khz to 4 Khz. The signal is ready to proceed with the FM demodulation, which is done by using the Zero Detector technique. This method works better with modulated signals under 6 Khz, explaining the need to down sample the signal. Once the demodulation is done, a lowpass filter is applied with a cut-off frequency of 35 Hz, in order to eliminate the 60 Hz power source noise. It is then down sampled again to 315 samples per second [6]; this is to comply with the minimum frequency required to work with ECG signals [34]. It is also a good sampling rate for current mobile devices to process the signal.

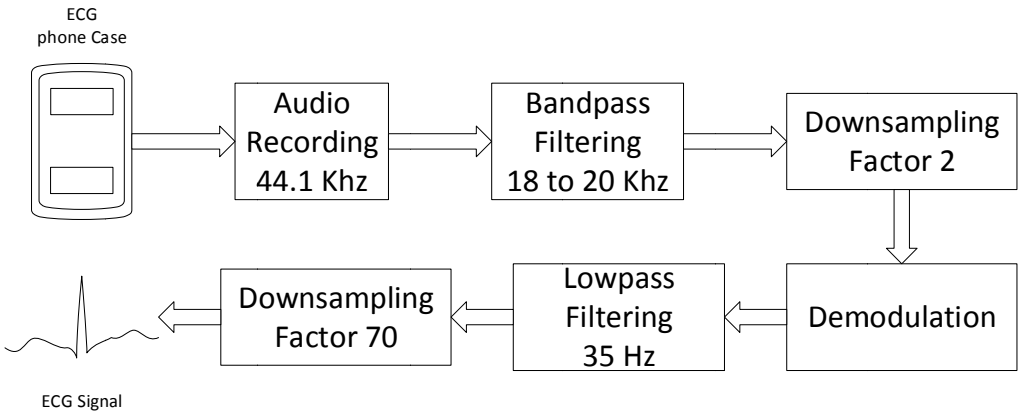

Figure 3-3: ECG Signal Acquisition from AliveCor Phone Case

The system is not restricted to the design presented here; it can work with any other ECG device with two electrodes and other sampling frequencies, as long as the signal can be sent to the phone. This can be with the same audio transmission scheme, or with bluetooth, wifi, or any other form of transmission, as long as the ECG signal is available in the device for further process.

3.2.1 Signal Filtering

As mentioned before, Bandpass and Lowpass filters are used during the signal acquisition of ECG. The characteristics for each filter are shown in Table 3-1.

	Lowpass Filter	**Bandpass Filter**
Type	Butterworth	Butterworth
Cut-off Frequency	35 Hz	18 KHz to 20 KHz
Sampling Frequency	22.05 KHz	44.1 KHz
Order	5	2

Table 3-1: Filter characteristics

With these characteristics for each filter, the coefficients to apply the filter can be calculated or obtained from computer software. For this study the coefficients were obtained from the Interactive Digital Filter Design web page [35].

Once the coefficients are available, the next step is to apply the filter. To ensure that the mobile device is not saturated by the use of too much processing power, a differentiate filter is applied in computer code [36] using the following linear difference equation (3-1).

$$y[n] = -\sum_{k=1}^{N} a_k\, y[n-k] + \sum_{k=0}^{M} b_k\, x[n-k] \qquad (3\text{-}1)$$

The result is two functions, one for the Lowpass filter and the other for the Bandpass filter, which will be called by the program according to the diagram shown in Figure 3-3.

The Bandpass filter is to eliminate all the environment noise in the transmission from the case to the mobile device, while the Lowpass filter has two purposes, one is to eliminate the noise introduced during the ECG capture, like the 60 Hz in the power line, and the second one is to apply the filter missing in the demodulation to recover the original signal information.

3.2.2 Downsampling

In order to acquire the ECG signal, two downsampling stages are required, each one with a different rate and a different purpose. The first downsampling has a factor of two, which means that the resulting frequency will be half of the original, in this case 22.05 KHz. This is done after the Bandpass filter eliminates all the frequency components in the signal except those located in the band from 18 KHz to 20 KHz, where the ECG information is located.

The purpose of this downsampling is to prepare the signal for the zero cross FM demodulation as it only works in the spectrum of less than 6 KHz. When downsampling is applied, an inversion and an aliasing of the information occurs in the frequency from 2 KHz to 4 KHz, which can be used at the demodulation stage.

The second downsampling stage has a factor of 70, which will reduce the signal to 315 Hz. This will reduce the size of the signal, staying over the minimum 300 Hz sampling frequency recommended [34] for ECG and making it easier for a mobile device to handle and process it.

The downsample method is simple, and depends on the factors, which in this case are 2 and 70. The system will eliminate every 2^{nd} sample of the signal for the first case, and every 70^{th} sample for the second case. This method makes it easier for the mobile device to handle all the processing required. For this reason, some corrections are not made, like in the second case, where the factor is 70 and the resulting sampling frequency is 315 hz and not 300 hz. However, this does not affect the system and it reduces the processing requirements, which is very important for a mobile device.

3.2.3 Demodulation

The signal sent by the AliveCor ECG phone case transmits the ECG signal using a FM modulation technique [6]. Therefore, to obtain the signal it is necessary to apply an FM demodulation technique, and in order to not use a lot of resources in the mobile device, a zero cross FM demodulation technique is used. However, as mentioned previously, this works only with frequencies under 6 KHz, which is why a decimation or downsampling process is necessary and was explained in the previous section.

The demodulation process starts with the detection of zeros in the received signal. This is done by detecting a change of signals between samples. When the values from the samples change from negative to positive, a zero is detected and an amplitude of one is placed on that sample. This will generate a pulse train, where each pulse amplitude $f\Delta$ will be calculated using equation (3-2) based on the sampling frequency *fs*, carrier frequency *fc*, next sample number *tn,* and previous sample number *tp* [37].

$$f\Delta \approx \frac{f_s}{t_n - t_p} - f_c \tag{3-2}$$

With all the amplitudes calculated in the pulse train vector, there are still points with zero values. To establish the amplitude $f\Delta_{\text{int}}$ at the missing samples, a linear interpolation (3-3) is calculated with an amplitude correction of A_c = 8e-6.

$$f\Delta_{\text{int}} = A_c\left(\frac{f\Delta_n - f\Delta_p}{t_n - t_p}\left(t - t_p\right) + f\Delta_p\right) \tag{3-3}$$

The demodulation process finishes with a Lowpass filter that recovers the signal, but is not included in this stage, since the next Lowpass filter will eliminate the 60 Hz power line noise and will recover the original signal; two tasks reduced to one helps reduce processing time, which is important in mobile devices.

3.3 Proposed Algorithm for ECG Authentication System for Mobiles

This is an authentication, and not identification, method (login) for mobile devices using the ECG signal obtained from only two electrodes. ECG signals are unique in every human being and can be used as biometrics [15] instead of using the fingerprint, eye iris, or a lot of electrodes as current ECG authentication methods require. This method only requires the user to touch the electrodes for a short period of time in order to gain access, making the login process easier, faster, and secure, all the while using less hardware than other systems. The result is a system that is very suitable for use on mobile devices.

This is an application that needs to be installed in the mobile device. The user will run the program and if a first time running is detected, the system will start a training process. Once it is done, the system will be running in the background, and when the phone locks, the authentication process will be waiting for an ECG signal to come in. As soon as the user touches the electrodes, the authentication process will start and will give or deny access to the user.

The system will have an option to change users or to re-run the training process for the same user, in case of a high rate of authentication failures.

A backup feature is also available in case of several authentication failures, where the system will have the option to access the device with a traditional authentication method. In the case where the mobile device

is a phone, the system will allow emergency calls without the need for authentication, just as the traditional systems allow.

As it is shown in Figure 3-5, the system has two main sections: a training process and an authentication process.

The training process obtains the unique ECG pattern of a person and stores it; this process has to be done just once by the user and will take 30 seconds. The authentication process acquires the features of the person that is touching the electrodes, and this data is later compared with the pattern stored by the training process. If it matches, then access to the system is granted.

If a match is not possible, there is a counter that allows the user to try again. However, if the counter reaches a maximum of 3 tries, the system will temporary block for 1 minute before trying again.

The time required for the acquisition of the ECG for the authentication is less than the training process and is set to 4 seconds. The sampling rate is 315 samples per second, which is slightly above the minimum recommended, which is 300 samples per second [34].

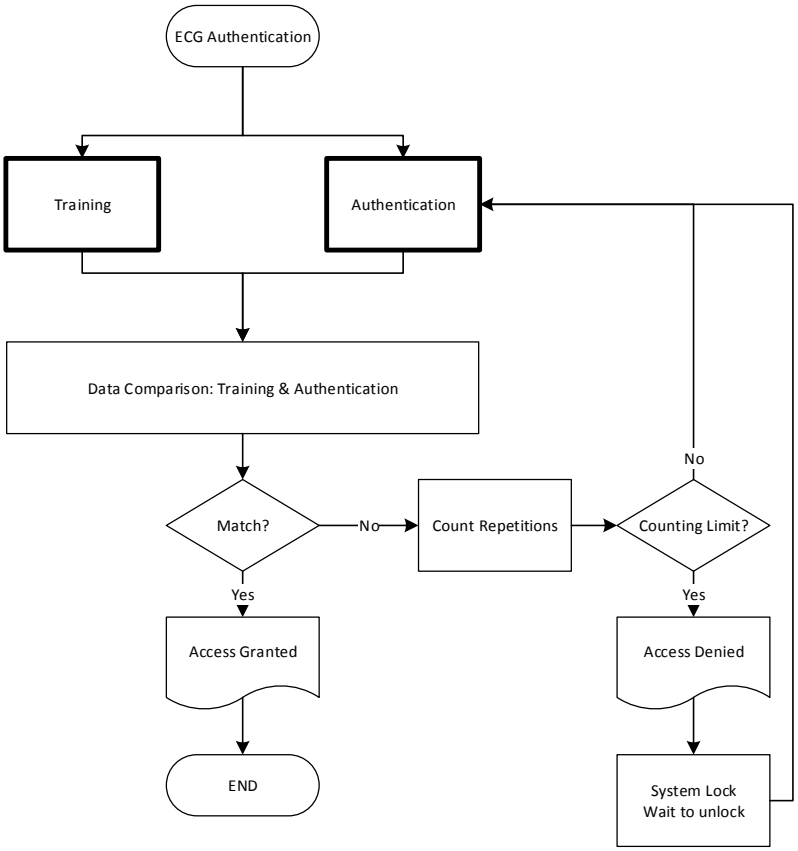

Figure 3-5: Proposed ECG authentication system for mobiles

3.4 Training

The goal of the training process is to obtain a template that has the unique parameters of the ECG pattern of a person and store it in memory for further comparison with data obtained from the authentication process. The training process can be described as shown in Figure 3-6.

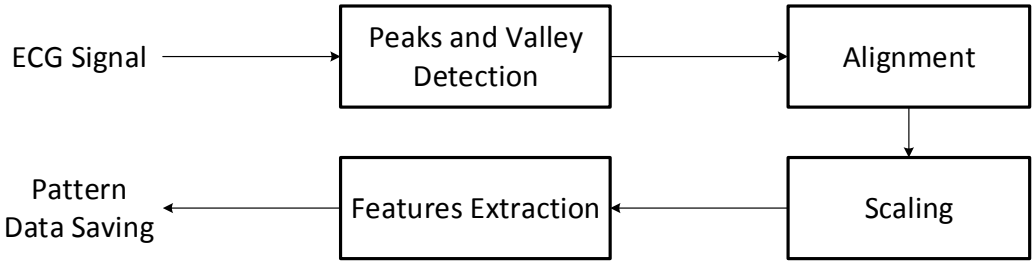

Figure 3-6: ECG training process

3.4.1 Fiducial Points Detection

In the training process there is an ECG signal with a long duration, where the fiducial peaks, valleys and amplitudes need to be detected. The information extracted are the sample numbers where P, Q, R, S, T, LP and TP exist, as well as the amplitude corresponding to R, S and T. LP and TP valleys are the ones that mark the start and the end of a beat process, these points are shown in Figure 3-7. Amplitudes are considered in this work because the signal will always be obtained from the same place, fingers in this case, and amplitude variations are reflected only when changes are made to the placement of the electrodes [14].

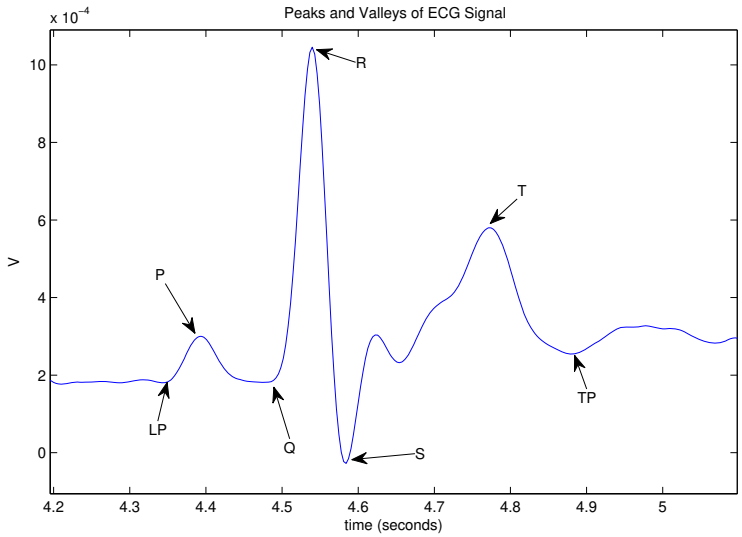

Figure 3-7: ECG peaks and valleys

The R peak is the main point to be detected as it is the base to extract an ECG period and the rest of the ECG features.

3.4.1.1 R Peak Detection

Detection of the R peak is based on the application of the second derivative to the signal [38]. This is because this method works better for signals obtained from the fingers, since most of the detection methods use an amplitude threshold [39]. However, sometimes when the signal is obtained from the fingers the threshold does not work because the R peak can go below the T peak for some people, as can be seen in Figure 3-8. Methods that apply the rate of change (second derivative) also use thresholds [38] [39], but with the hardware that only has two electrodes designed for use in a mobile device, a threshold is not viable. Therefore, in this work for the R peak detection we use the second derivative without thresholding as we will discuss later.

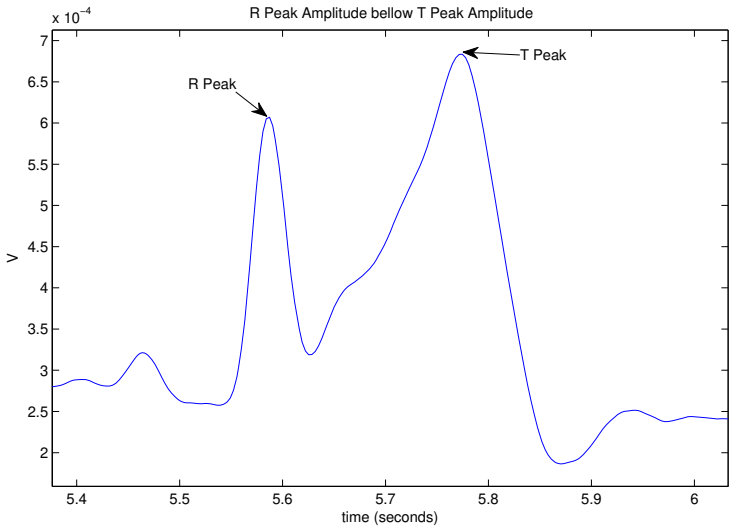

Figure 3-8: Case where R peak is below T peak

To detect the R peak, first the negative of the second derivative is applied to the ECG signal. As we can see in Figure 3-9, the second derivative gives us the high peaks very clearly, no matter how high the amplitude of the R peak. Since the ECG signals are unique for each person, we cannot set a threshold to detect the R peaks because for some people, sometimes even for the same person, the amplitude of the second derivative is higher or lower.

For this reason, another procedure is used. This procedure consists in acquiring a limited number of the maximum values of the second derivative of the signal; this will give us several points that are enclosed by red circles, as shown in Figure 3-9.

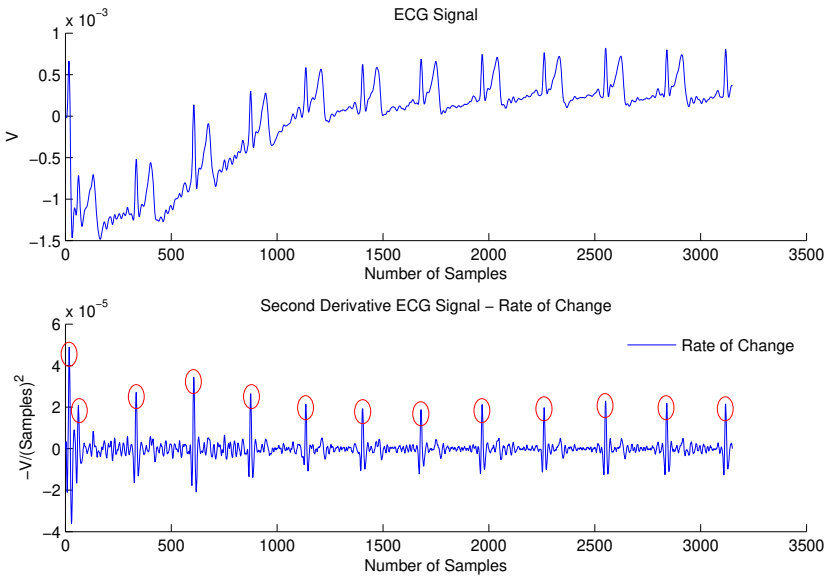

Figure 3-9: Detection of R peaks

It is hard to determine only the points that correspond to the R peaks. Therefore is necessary to capture the samples with the higher amplitudes that are enclosed by a red circles. Between all the samples captured it will be the one that correspond to the R peak. To determine the R peak, all the samples with higher amplitudes that are the samples with maximum values are sorted to form a group. From the groups formed, the median value is the one that correspond to the R peak. The formula to determine how many of maximum values are needed in order to detect the R peaks of ECG has been determined in this work and is given equation (3-4):

$$NP = F_p \frac{S}{f_s} \tag{3-4}$$

NP is the number of maximum values needed in order to proceed with the detection of R peaks, and S is the number of samples to be analyzed (this will change according to the length of the signal). As an example for the case of Figure 3-9, there is 3150 samples that were taken in 10 seconds; f_s is the Frequency sample, 315 Hz in this case, and F_p is a constant referred to in this work as the R peak factor, which, after different analyses and tests, has been determined at the value of *7.7*. This formula is directly related to the length of the signal S that is measured by number of samples. If the value of NP is too high, it will give more peaks than required, resulting in false R peak detections. If the value of NP is too low, then it will not detect all the R peaks.

The samples corresponding to the maximum values are not given in order, and a peak grouping is necessary to order them, as shown in Figure 3-10

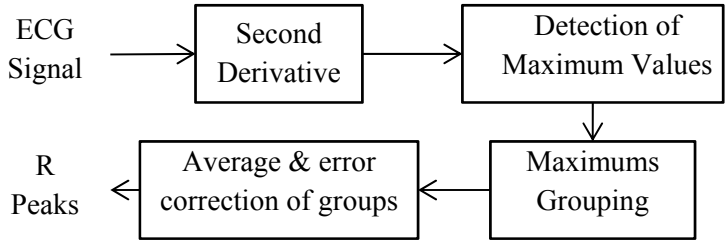

Figure 3-10: R peaks detection process

As an example, in the Maximums grouping process, the data will be received from the maximum detection process as is shown in Table 3-2, where data is sorted by the amplitude of the second derivative.

Sample Number	**2nd Derivative Amplitude Value (–mV/Sample^2)**
8	500
21	450
16	425
10	425
22	420
17	420
9	415
20	414
15	410

Table 3-2: Order of maximum values detected

Once data is received it is sorted by sample number, which gives 3 groups formed by consecutive sample numbers, as shown in Table 3-3.

Sample Number	**2nd Derivative Amplitude Value (–mV/Sample^2)**
8	500
9	415
10	425
15	410
16	425
17	420
20	414
21	450
22	420

Table 3-3: Data sorted by sample number

These data are sent to the “Average & error correction of groups” process, where from each group one point is determined and this is done by averaging the sample number of each group, getting as a result the data shown in Table 3-4.

Sample Number
9
16
21

Table 3-4: Samples where R peaks are located

When groups are very close together it means there is an error and that information is rejected. This is because very close groups of data mean a very high heart rate, which is out of the boundaries of what is considered to be the limits of the human heart rate.

ECG authentication algorithms are based on time and not on sample numbers, and the information given by this R peak detection algorithm are the sample numbers where the R peaks are located. However, sample numbers are directly related to time by the sampling frequency, therefore a straight conversion can be applied if needed.

3.4.1.2 Q and S Valley Detection

The detection of Q and S valleys is done by analyzing the periods of the total signal length, one at a time, where each period is determined by the R peaks. The analysis is done starting at the end of the signal and moving toward the beginning of the signal, because after different tests it was found that the signal is more stable at the end, which gives us more accurate data to work with.

To proceed with the detection, the ECG signal is divided into beat periods that go from R peak to R peak, according to the information obtained in the R peaks detection stage. The limits of each period are shown in the expression (3-5)

$$R_{i-2}\ to\ R_i \qquad \begin{cases} i-2 \geq 1 \\ i \leq m \end{cases} \tag{3-5}$$

Where R is a vector that contains the location of all the R peaks of the signal, i is the period number, m is the number of R peaks detected or the length of the R vector, R_{i-2} is the R peak that marks the beginning of the period, R_i is the R peak that marks the end of the period, and R_{i-1} – not presented in the expression – would be the R peak that corresponds to the period selected.

The detection of Q and S valleys requires a similar process and is shown in Figure 3-11. The only difference is that for Q the processed data is the one to the left of the R_{i-1} peak, and for S it is the one to the right.

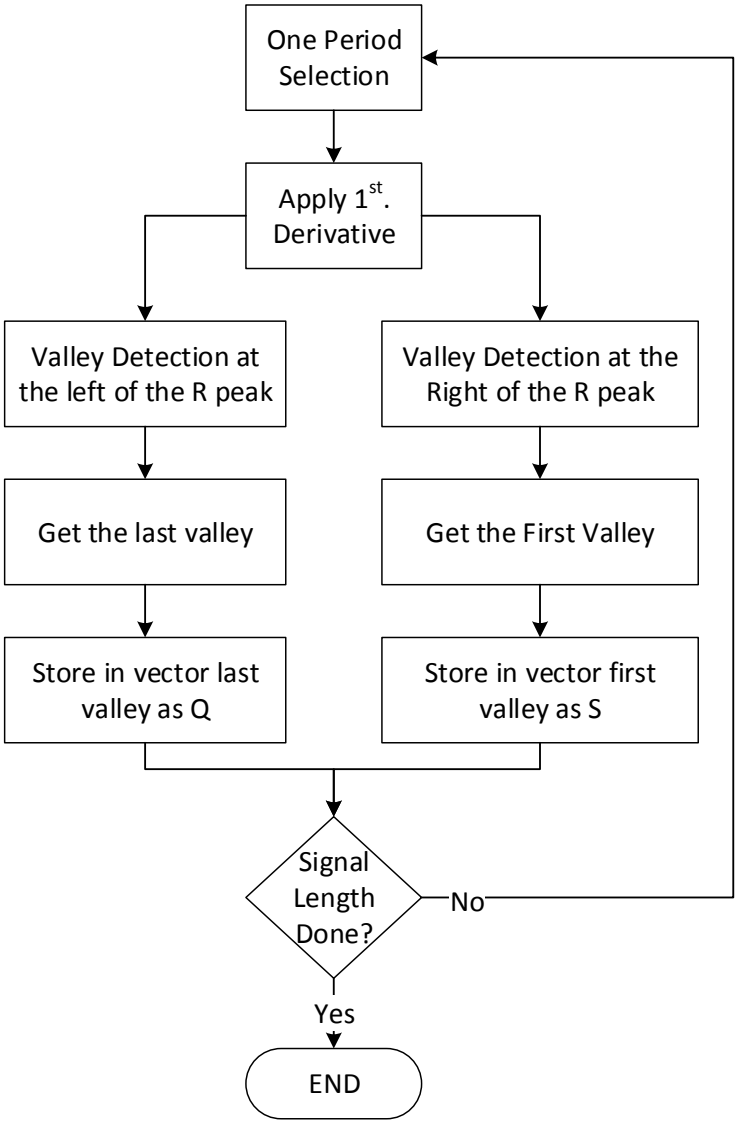

Figure 3-11: Detection of Q and S valleys

To detect the sample location of the valleys it is necessary to use a zero detection method from negative to positive on the first derivative of the signal.

Basic mathematical concepts show that the first derivative of a signal indicates the slope value of the signal, and a value of zero in the first derivative indicates a valley. Therefore, all the zeros are detected and the last zero detected in the portion of the signal that is located to the left of the R_{i-1} is the one determined to be the Q valley.

In a similar manner, the first zero to the right of the R_{i-1} peak is where the S valley is located, as is shown in Figure 3-12. The system takes advantage of the fact that Q and S are the closest valleys to the R peak.

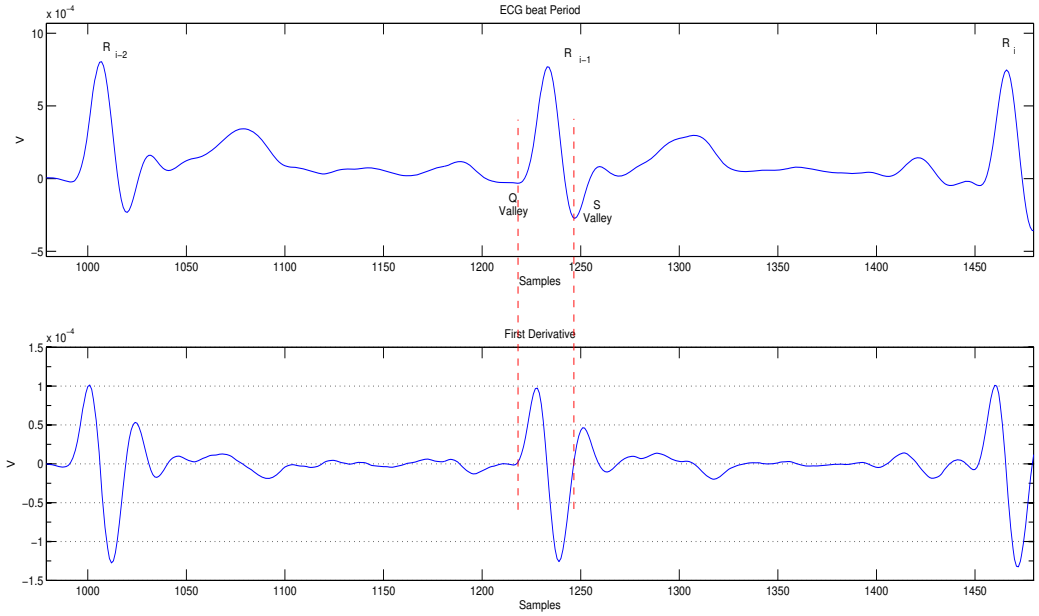

Figure 3-12: Zero detection of Q and S valleys in the first derivative

The detection is done period by period and each sample number corresponding to Q and S valleys are stored in a vector. The process is repeated until the whole signal has been processed.

The logic of working with data from the right and the left of the R peak separately is going to be used to detect the rest of the peaks and valleys necessary to apply the authentication algorithm.

3.4.1.3 T Peak Detection

As in the S valley detection, the T peak detection is also done period by period, using only the samples to the right of the R peak.

However, this time the half period is divided in two, where only the first half is used, as we can see in Figure 3-13.

The T peak is obtained after applying a first derivative and a zero detector from positive to negative, which indicates a peak. The peak with the greatest amplitude is the T peak.

The sample number where the T peak is located is stored in a vector and this is repeated until the whole signal is analyzed.

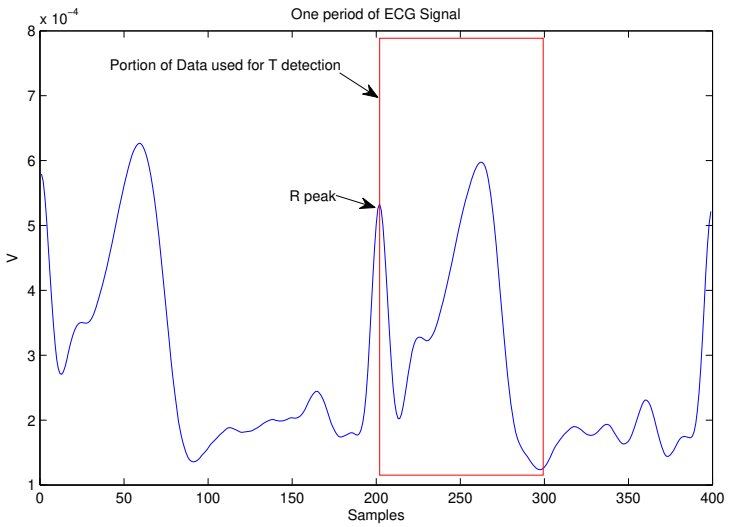

Figure 3-13: Detection of T peak

3.4.1.4 TP Valley Detection

The TP valley detection is similar to the S valley detection, as can be seen in Figure 3-14. It is done by using only the data to the right of the R peak, but in this case it is the first valley after the T peak that was previously detected, and is obtained with a zero detector that goes from negative to positive. The value corresponding to the sample number where the TP valley is located is stored.

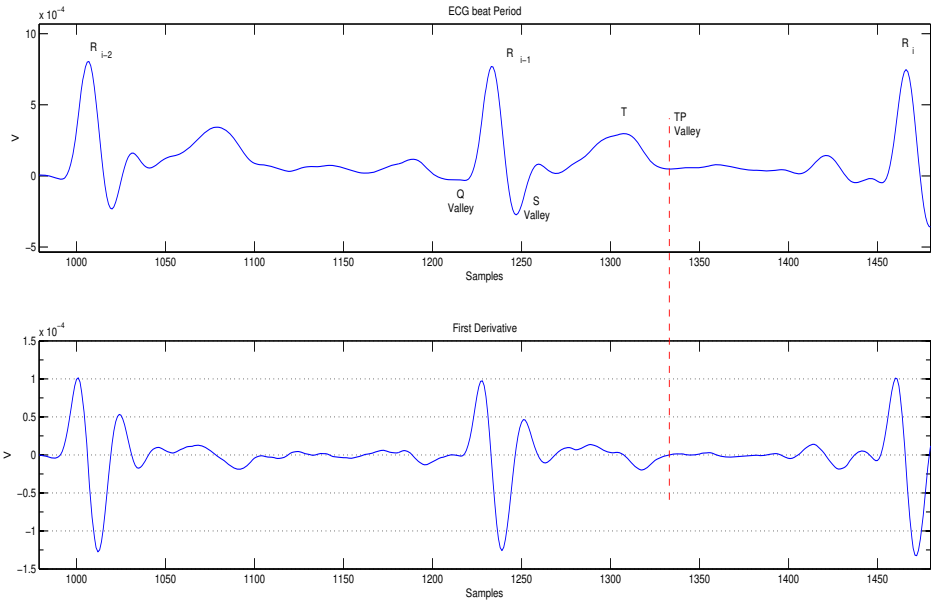

Figure 3-14: Detection of TP valley

3.4.1.5 P Peak Detection

The P Peak detection is similar to the T peak detection but this time using the data to the left side of the R peak and determining the maximum on an area of data that is half of the half of the period. The maximum amplitude is the P peak, and the sample number corresponding to the P peak is stored. This is shown in Figure 3-15.

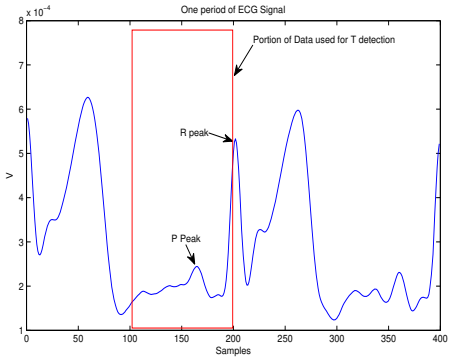

Figure 3-15: P peak detection

3.4.1.6 LP Valley Detection

As shown in Figure 3-16, The LP valley is detected like the Q valley, with data to the left of the R peak. The first derivative is applied as well as the zero detectors from positive to negative, in order to obtain all the valleys. The LP valley is the first valley, going from right to left, after the previously detected P peak. The value stored is the sample number where the LP valley is located.

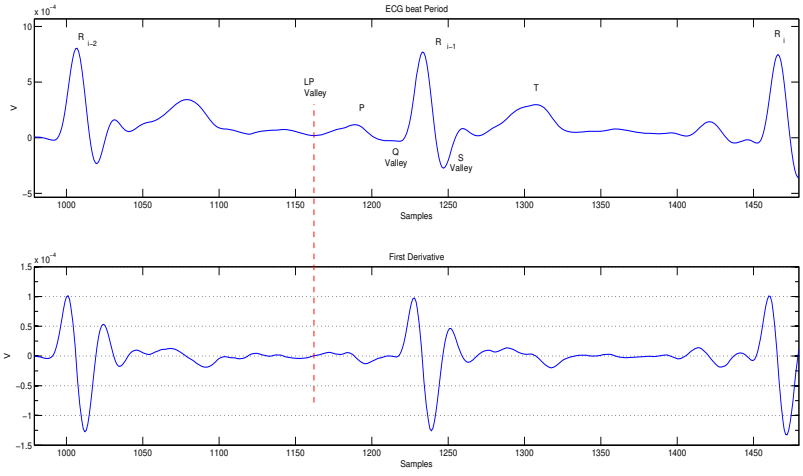

Figure 3-16: LP valley detection

3.4.1.7 Amplitudes Detection

Amplitudes play an important role in ECG authentication in determining if a user is valid or not [27]. The amplitudes needed for this work are the ones corresponding to the Q valley, R peak and S valley.

The process used to obtain these values is straightforward since all the previous peaks and valleys detected were given the time location or the sample number associated to their location.

The amplitude can be found by looking at the value located at the sample number in the signal vector. The amplitudes needed for this algorithm are shown in Figure 3-17.

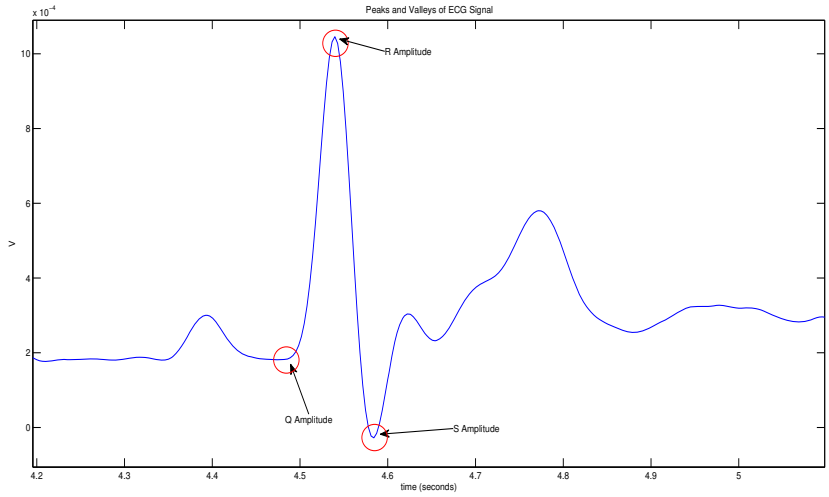

Figure 3-17: Amplitudes detection

3.4.2 Alignment

This process consists in aligning all the extracted periods from the ECG signal to a reference, which is the median sample value obtained from all R peak values detected. This is done by using the R peak data extracted from the previous process.

The upper part of Figure 3-18 shows the raw periods obtained after the peak detection, and the lower part shows the ECG periods aligned to the median value of all R peaks.

For the rest of the peaks, some of them match the same number of samples and others do not; that is explained by changes in the heart beat rate, which is corrected in the next process.

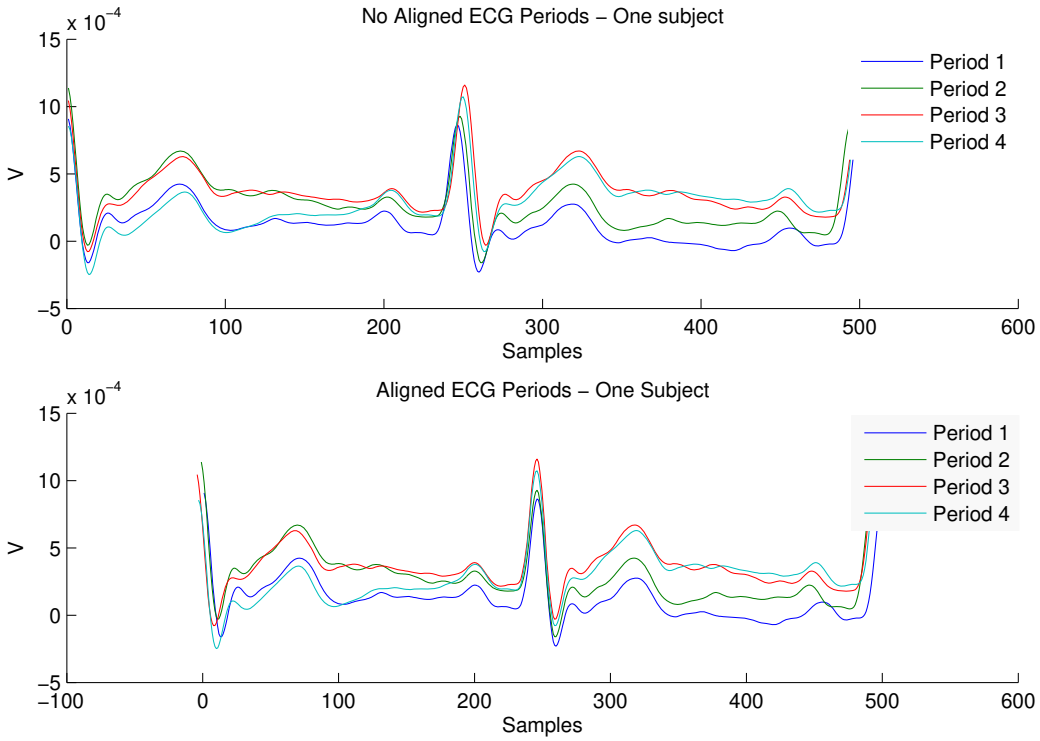

Figure 3-18: Alignment of ECG periods to the median of R peaks

3.4.3 Normalization

Different heuristic studies show that changes in the heart rate are linear [15] [14]. Based on that information, a scaling process of the signal is applied to match the ECG of a subject despite any changes in the rate of their heart beat caused by different situations. The classic normalization is based on a unitary system [14] where the duration of each feature is divided by the total length of a heartbeat.

Based on the idea that heart rate changes are linear, for this work a different normalization process was applied by scaling the signal. This is done period by period and two points are taken as references, R peak and TP valley, where the R peak is the same for all periods because of the alignment process, but the TP valley is different for each period. The median of all TP valleys is calculated and is taken as a reference to scale all the fiducial points of all the periods of the ECG signal based on these two points.

The normalization algorithm requires the location of the R peak and the TP valley. With the information of these two points as a reference, the location of the remaining fiducial points is calculated according to the following scaling formula (3-6):

$$NS_{peak} = \frac{(D_{cur} - Rp_{ref}) \times (TP_{ref} - Rp_{ref})}{TP_{cur} - Rp_{ref}} + Rp_{ref} \quad (3\text{-}6)$$

Where, D_{cur} is the position (sample number) of the fiducial point that needs to be scaled and can be any peak or valley of the signal, Rp_{ref} is the R peak used as a reference for scaling, TP_{ref} is the median value of all TP valleys of the signal that is considered as a reference for scaling, TP_{cur} is the position (sample number) of the TP valley of the current period of the signal that needs to be scaled, NS_{peak} is the position (sample number) of D_{cur} that has been scaled based on Rp_{ref} and TP_{ref} as a reference.

The result of scaling can be seen in Figure 3-19, where it can be observed that peak and valley positions match on data enclosed by the red box.

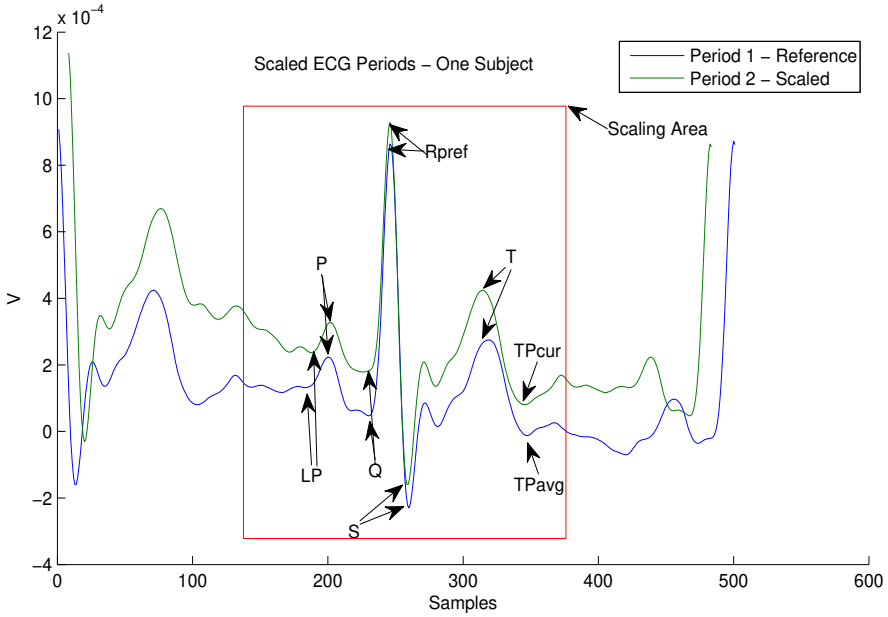

Figure 3-19: Normalization of ECG periods by scaling

As mentioned before, the amplitudes position in respect to zero changes constantly, but the amplitude relative to the R peak depends on the placement of the electrodes. Since for this study all ECG records will be taken from the fingers, there is no need to normalize the amplitudes, as we can see in Figure 3-20; the relative amplitudes remain the same.

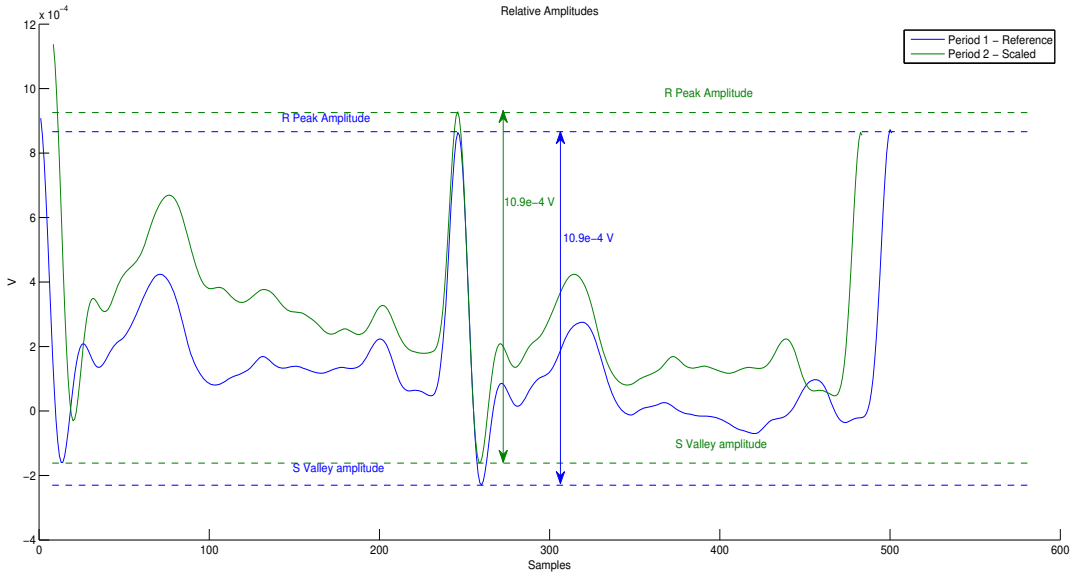

Figure 3-20: ECG relative amplitudes

3.4.4 Features Extraction

With all the periods of the ECG signal aligned and scaled, the next step is to extract the unique features of the ECG by which a person can be identified. In Figure 3-21, the eight features extracted are shown. After preliminary evaluation, these features were chosen because they tend to be the most clear to be extracted from the signal obtained from the ECG hardware designed for mobiles.

Since all data has been saved in vectors, the process of extracting the features is straightforward. It simply requires a subtraction of the R peak vector by the Q and S valley vectors, in order to find the amplitude difference of the Q and S valley amplitudes with respect to the R peak amplitude. The features of each period will be stored in eight vectors: RLP, RP, RQ, RS, RT, RTP, RQA, and RSA. The length of the vectors will correspond to the number of ECG periods extracted.

As mentioned previously, amplitudes are considered in this work because they will not be affected in mobile devices given the fact that the signal will always be obtained from the fingers; there is no change in the placement of the electrodes [27]. These amplitudes are not affected when they are measured between each other, using another peak as a reference. However, if they are measured using the ground 0V as a reference, there is constant change and this will represent a problem; that is why in this work the amplitudes considered are relative to the R peak and not to the ground.

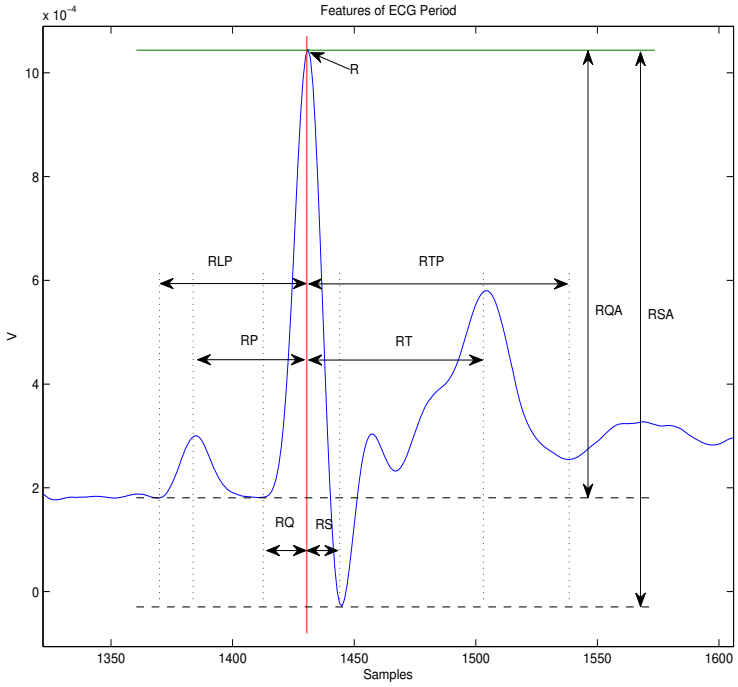

Figure 3-21: Extracted features from an ECG period

3.4.5 Pattern Data Saving

The features in every period vary slightly, even for the same person. This is a common phenomenon for biological signal. Nonetheless, in order to obtain the best results, a median of each feature set for the whole signal is calculated. The more periods there are, the more accurate the results will be. For this reason, the training time is longer, established at 30 seconds for this study. It is only required to do this task once per authorized user, to create the template for the system.

The features are stored in vectors and from them the median value is calculated. Eight results will be obtained and will be stored in the permanent memory of the mobile device as eight variables: RLP, RP, RQ, RS, RT, RTP, RQA and RSA; the median values corresponding to the R peak Rp_{ref} and the TP valley TP_{ref} that were used as references for the alignment and scaling are also stored in memory with the other features.

All this data will be further accessed by the authentication process, which will compare the features extracted with the features obtained from the training process.

3.5 Authentication

The authentication process is similar to the training process, with the difference that the acquisition time is shorter, lasting only 4 seconds, which gives a faster access to the device. This process does not store data but instead has an extra process called Validation, which indicates if the user trying to access the system matches a template registered in the system; this whole process is shown in Figure 3-22.

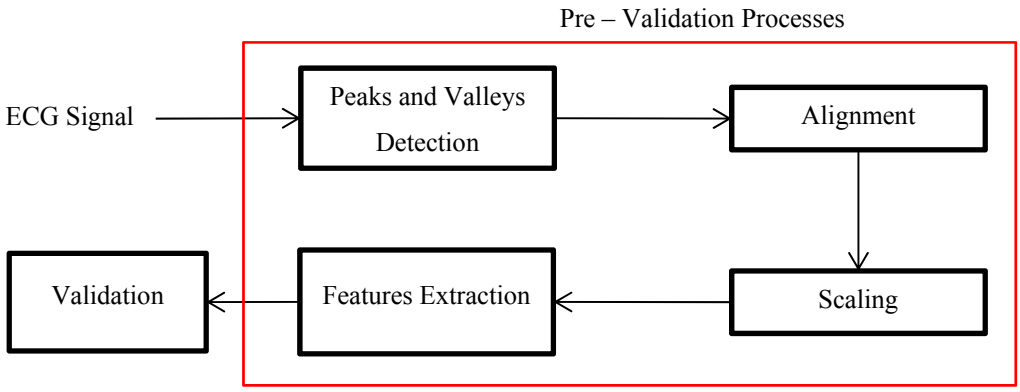

Figure 3-22: Authentication process

3.5.1 Pre – Validation Processes

All the sub processes that involve the Pre - validation algorithm are the same as the training process. However, here the system will start the process by sending data as soon as the user touches the electrodes, keeping in mind that this data is four seconds long, which is shorter than the 30 seconds required during the training.

The ECG signal, with a short duration that contains two or more periods, will go through the following processes: Peaks and Valleys detection, Alignment, Scaling, and Features Extraction. These processes will take less time since the ECG signal for authentication is short as well.

When the system is in authentication mode, the median values that are needed as reference points for the alignment and scaling processes are not calculated again. Instead, the system reads the values obtained during the training process and uses these values to proceed with the alignment and scaling of

the new signal obtained at the input. Once these data have been processed by the pre-validation process they are ready for the validation process.

3.5.2 Validation Process

At this point the system accesses the features saved by the training process and compares them with the features that are extracted at the end of the Pre – validation sub process.

The system will reach a match when the information at the input of the validation process is “very close” to the information from the training process.

The term “very close” is used because there is an error tolerance in the system that has been calculated for every feature, and if the information falls in this range then it is considered a match.

The validation algorithm that has been designed in this work is shown in Figure 3-23 and differs from previous ECG authentication algorithms in two aspects: each ECG feature has a percentage of tolerance and uses a hierarchy validation scheme.

All the features based on time, except RTP, are evaluated individually and if they fall in the accepted range of tolerance, they are given one point; if not, they are given a value of zero. Once this step is complete, all the features are added up and if the total reaches a minimum established value for this summation, the features based on time are considered valid.

With the features based on time, it was found that the FAR was still high when using the two electrode devices for mobile phones. Therefore, the features based on amplitudes are considered in a hierarchical order, meaning that the features based on time are the most important, and if this criteria is met the system will proceed to check the RS amplitude.

If the RS amplitude falls into the accepted range, the RQ amplitude will then be verified. If any check of these features does not fall in the permitted range, then the system will consider a non-match.

In this scheme, amplitude features are more prominence than the other features. If all the other features match and if the amplitudes do not, then it is considered as a non-match.

This is because the amplitude features differs significantly from one person to another. But this is not the case for the features based on time. The evaluation that confirms this concept is presented in sections 4.1.5 and 4.2

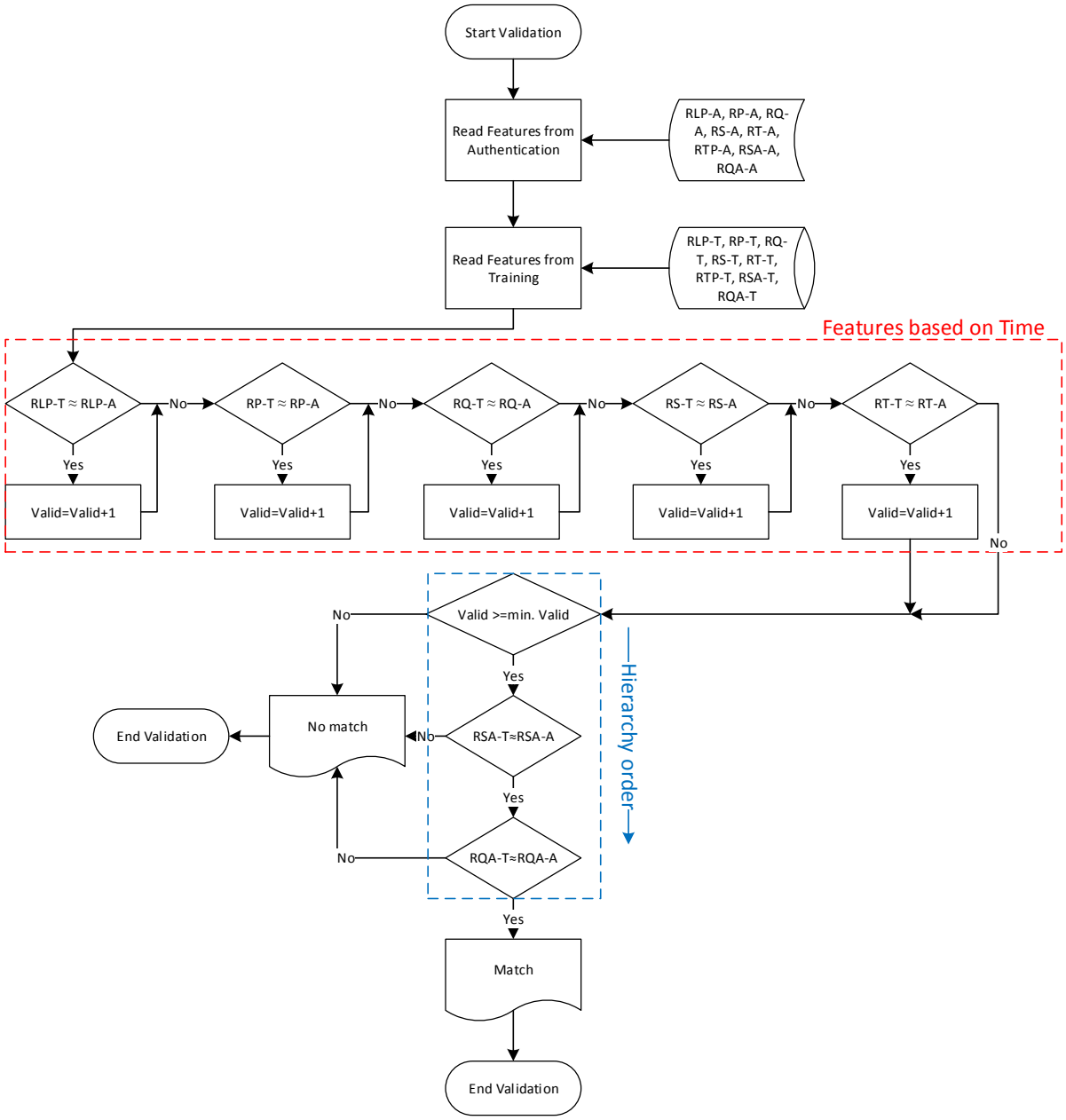

Figure 3-23: ECG validation algorithm

3.6 Execution of the Algorithm

The system was executed using the ECG phone case from AliveCor [6] with two electrodes, and a Windows based computer with Matlab was used to perform the calculations and to test the algorithm. The signal obtained from this mobile device is not as reliable as a signal from other advanced equipment.

Therefore, a different approach on the ECG authentication algorithm is performed and tested with this device that could easily be used by any mobile device that has a microphone input.

The general system was described in the previous section and the values to make the system work under the conditions presented were obtained after different tests and are shown in Table 3-5. A different range of tolerance was used for each feature because it was found that for some features the deviation was greater than for others, therefore with some features the system needed to be stricter than for others. For the RTP feature that is based on time, it was found that the deviation was too high, causing the system to malfunction. For this reason, this feature is not considered in the algorithm.

Feature	Threshold
RLP	± 10.00 %
RP	± 18.80 %
RQ	± 17.09 %
RS	± 12.90 %
RT	± 11.30 %
RQA	± 22.00 %
RSA	± 17.00 %
Min. Valid	4

Table 3-5: Threshold values

In Figure 3-21, all the extracted features are observed and the percentages presented in Table 3-5 correspond to thresholds over and below the value stored in the template. In Table 3-6, the values corresponding to the ones stored in the template are shown, as well as the corresponding threshold percentages and the lower and upper threshold values.

Feature	Template Value	Threshold Percentage	Lower Threshold	Upper Threshold
RLP	71.07	± 10.00 %	63.96	78.18
RP	48.21	± 18.80 %	39.15	57.27
RQ	21.00	± 17.09 %	17.41	24.59
RS	12.94	± 12.90 %	11.27	14.61
RT	87.75	± 11.30 %	77.84	97.67
RQA	194.98	± 22.00 %	152.08	237.87
RSA	193.02	± 17.00 %	160.20	225.83

Table 3-6: Features with threshold values

For a better system performance when validating the features based on time, there needs to be four out of five features that are valid in order to proceed with the next stages and achieve a low FAR and a high TAR; consequently, four is the value that corresponds to “Min. Valid” in Figure 3-23 and Table 3-5.

With the proposed algorithm, the best performance of the system was found with four seconds of acquisition time during the authentication stage and 30 seconds during the training stage. The extra time in training stage is needed to generate the template. If these values are incremented, the performance of the system would not improve significantly. However, if these values are reduced, the performance will also be reduced. The acquisition time during the authentication process is more sensitive than the acquisition time during the training, and that is because the time for the training can be longer, since the user is required to do this step only once. It was found that 30 seconds for the training was the breaking point in order for the system to perform well with this algorithm.

In Figure 3-5, the general ECG authentication system for mobiles is presented, and there is a counter with a limit. This limit has been set to a value of three, where the system will try at least three times before rejecting a user. The counter is internally known by the system and the user would not be aware of this. The number of trials allowed was determined based on other authentication methods like passwords or graphical patterns, where after three unsuccessful tries the system locks for a determined period of time before allowing a user to try again.

3.7 Conclusions

In this work, the phone case from AliveCor [6] was used, but this work is not limited to this device. Other mobile devices that can transmit data in different ways can also be used. Here the data is obtained through the microphone and a FM demodulator is used to obtain the information; but that is not the algorithm, it is just the information that is going to be processed. Therefore, any other means of transmission, such as Bluetooth, wifi, and others can also be used. As long as the ECG signal information is provided with this information, the algorithm can be applied. These days the signal from these mobile devices is not very accurate but as technology progresses these devices will provide us with a higher quality signal, and the algorithm has been tested to work with better quality signal as well.

The difference between identification and authentication has been explained, where identification requires the storage of more information, usually databases. This is something that mobile devices cannot do independent of external sources, while authentication is a method that can be entirely performed in the mobile device. This work is done in authentication mode since that process can be entirely performed in the mobile device. In identification mode, however, the mobile device would only be an interface to transmit and present results, and would not do much work, as it would require access to a remote database. If external access were possible, it would be better to do all the processing work at the remote location as well. Small identification tasks with just a few templates can be performed in a mobile device, but if it is just for few users, then identification task will be very limited.

Amplitudes change based on the placement of the sensors, but for this application the sensors will always be placed on the fingers, therefore the amplitudes will remain unchanged in an acceptable range. Consequently, the system can use features based on amplitudes, and the thresholds are not referenced to zero volts but to the amplitude difference of two peaks. In order to save processing time, a baseline wander is not performed. Despite this, the process is still valid since a baseline wander is only necessary in special cases like medical monitoring, but not for this ECG authentication algorithm.

Normalization is necessary to deal with heart rate changes, and various techniques have been used in the past. In this work, a linear normalization method is used based on heuristic tests performed in other works, which found that heart rate changes are linear. The same concept is used, but instead of using a unitary system, two reference points are used to scale each heart beat. As a result, all heart beats have a constant rate. This approach has shown to perform better in ECG authentication for mobile devices than other normalizations. This is because for this application the separation of heart beats is based on T peaks, while other normalization techniques mark the beginning and the end of a heart beat at the LP and TP valleys respectively. The latter technique cannot be performed in this work case because at time the quality of the signal does not allow the identification of these valleys.

In this work a different approach for the detection of the R peak has been performed because traditional methods of R peak detection are based on amplitude thresholds, and as mentioned previously the amplitude thresholds in ECG for mobile authentication changes constantly since no baseline wander is performed. The approach presented here works very accurately, especially with the short term duration of the ECG signals that are needed for this application. As future work, different tests can be performed with this R peak detection technique in order to assess its reliability for longer signals and for use in the medical field; this is an open gate for further research.

The detection of the R peak is very important in this algorithm; the ECG periods are counted based on the R peaks, and the rest of the peaks and valleys are detected to the right and to the left of the R peak. For this reason, special caution needs to be taken when detecting this peak, and other R peak detection techniques could not be applied given the fact that the available signal is not as reliable as the signal given by the hardware used in the works of other people.

According to the research knowledge applied to this work, the hierarchy used in this validation process, together with the combination of time based and amplitude based features, makes this algorithm unique; it has not been used in any other ECG biometrics studies. The main contribution of this work is that it is applied in ECG authentication for mobile devices, but it could also be applied in any other application that requires ECG biometrics. In this work only seven features are used, with a training time of 30 seconds, and an authentication time of four seconds. Good results were also achieved in regards to TAR and FAR, which

makes the system comfortable and secure for the users and, given that this approach is new, leaves room for further research in order to keep improving performance and times on ECG as biometrics for mobile devices and other applications.

Chapter 4.

Evaluation

4.1 Determination of Default System Values

In order to determine the values and methods to be used in this work, different sets of experiments were performed in order to observe which options achieved the best results.

Three different samples were taken from 10 consenting volunteers at the MCRLab in the University of Ottawa, 7 males and 3 females with an average age of 28 years old; the samples were taken on different days and at different times.

Given the various times of sample acquisition, it is assumed that each sample was taken when the subject was in a different state of anxiety. The sample acquisitions lasted two minutes and were followed by the different experiments, which ranged in time from 4 seconds to 30 seconds, depending on the test being performed.

4.1.1 First Tolerance Estimation

The first step in estimating the right value of a threshold was measuring the Euclidean distance of the time based features using a percentage of tolerance. This is not the final method used, but this test helps determine a tolerance value that will be used to determine other fixed values and methods used in this work.

Figure 4-1 shows the results of the first attempt, where the system was evaluated with 10 people using a training time of 20 seconds and an authentication time of 10 seconds. The data of only one user was taken as reference during the training, and with that information the evaluation of the system was performed by changing the threshold percentage value.

In Figure 4-1, the behaviour of TAR and FAR when the tolerance value moves can be observed. As the threshold value is reduced the TAR and the FAR decrease as well. These values show that with a more restrictive threshold, the system becomes more secure as false users do not have access. However, it also shows that the access of the authorized users is reduced, which means a system failure.

Observing these results, a threshold value of 8% is chosen for the following experiments, where TAR is 33.3% and FAR is 10%. These values are still not ideal for a system to work properly, but they will help find the correct values as they will help modify other parameters.

As mentioned before, TAR is inversely related to FRR, and FAR is inversely related to TRR; some of these values don't reach 100% because there are errors during the acquisition when the algorithm doesn't process the signal. This data is known as fail to capture and is not presented here as it does not depend on the threshold values.

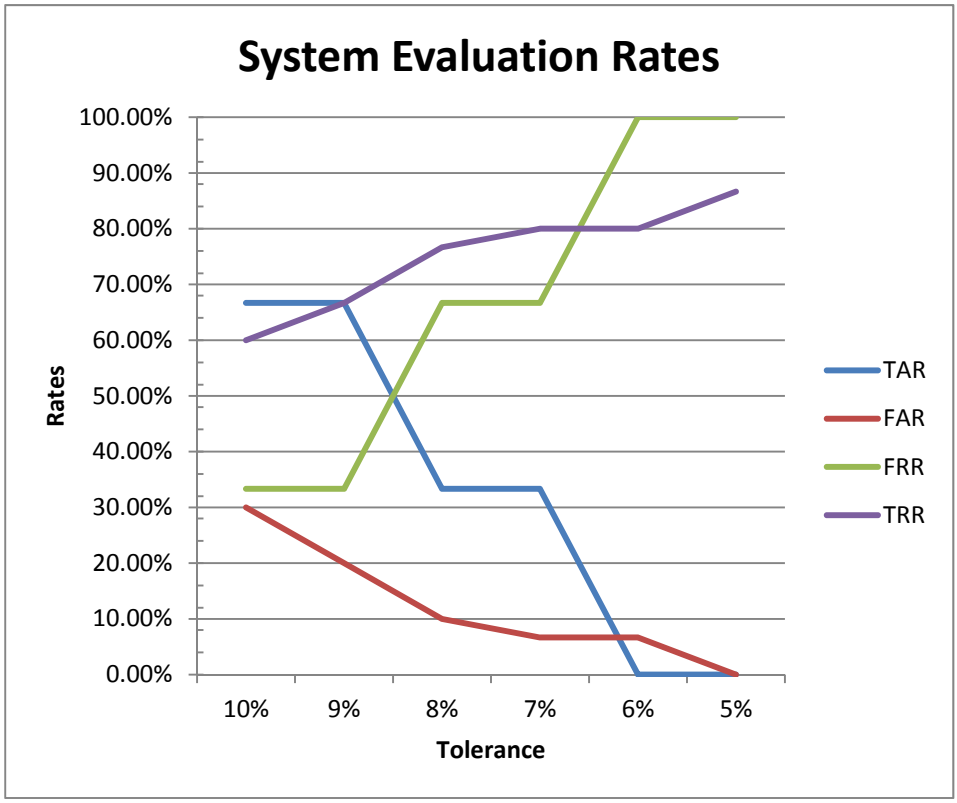

Figure 4-1: Behaviour of system rates based on Euclidean Tolerance

4.1.2 Evaluation of System Alternatives

In order to obtain a better performing system, different alternatives were thought of and have been presented here in various cases.

To evaluate all these cases, the tests were performed with the same data obtained from section 4.1.1, but this time the duration of the training was 20 seconds, the authentication time was decreased to 6 seconds, and the Tolerance with Euclidean distance was set to 8 %. The evaluation of TAR and FAR was performed for each user, which means that the data of every user was employed, one at a time, to train the system and run the algorithm against every other user. This process will deliver more information and results, leading to a better evaluation of the system.

For case A, the system was executed with the TPAVG, showed in Figure 3-19, calculated as an average of all the signals during the training stage and rounded to the closest value. All the scaling was performed with these values. In section 4.1.1, the TPAVG was obtained from the TP value of the first ECG beat during the training process, and that value was also calculated during the authentication process. The results for case A, shown in Figure 4-2, are better than the ones in previous sections because this time the TPAVG was calculated with the average of all the ECG beat periods during the training stage, which led to a FAR of 7.44% and a TAR of 61.54%.

Case B is the same as case A, but instead of rounding the TPAVG value, it was used with the decimal value obtained. Since these values are used to scale the signal, there is no change in the results; the FAR of 7.44% and the TAR of 61.54% are still the same, which proves that the approach of this work to scale the signal works as a normalization technique, based on the heuristic concept of Israel *et. Al*, which states that heart rate changes are linear [14].

In case C, instead of calculating TPAVG as an average to apply the normalization, the median is extracted during the training stage; the results obtained show a decrease of the TAR to 40%, and the FAR is reduced by about six percentage points, to 2.22%.

This large of a reduction is very hard to achieve in FAR, but this approach shows a good reduction even if the TAR is also reduced. Other aspects will later be considered to improve TAR, therefore this approach will be used for further experimentation with the goal of obtaining a proper algorithm.

At some point the thought occurred of seeing how the system would be affected if the normalization was skipped. This meant the use of raw TP values in the algorithm, which is what was done for case D. In the end the results showed similar values to those of cases A and B, with slightly lower TAR of

58.97% and a FAR of 8.46% for case D. This latter value is higher than in the other cases, which means that normalization is also necessary in ECG authentication for mobiles, and then case D is not considered.

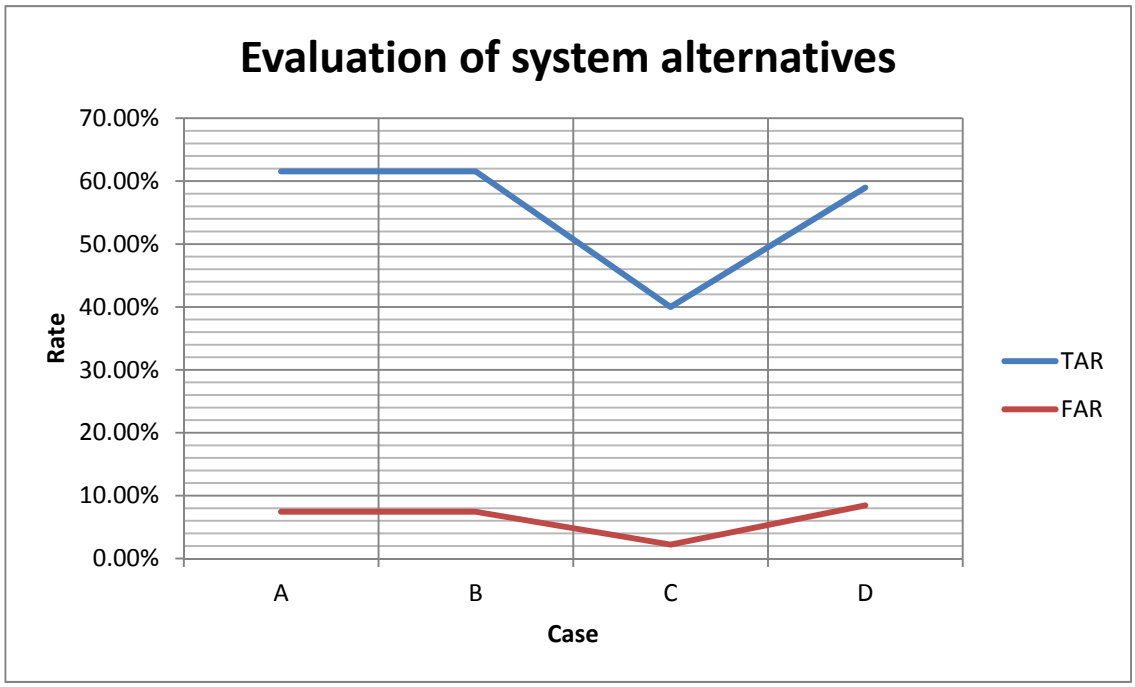

Figure 4-2: System evaluation for different cases

4.1.3 Determination of the "Min. Valid" Value of the System

To determine the minimum number of valid "time based features" required to achieve a match in the ECG authentication algorithm presented in this work, another test was performed with similar conditions to those of case C in section 4.1.2. Here the training time was increased to 30 seconds and the authentication time was reduced to 4 seconds.

To determine the "min. valid" shown in Figure 3-23, the test was performed using the median value as a reference point, with the same 10 users and the time previously indicated. The results obtained are shown in Figure 4-3, where five features are required to be valid corresponds to case C of the previous section. The values are different because training and authentication times are also different, which gives, for this case, a FAR of 1.41% and a TAR of 26.85%. As the number of features required are reduced, the FAR and the TAR change, when the system has a major distance between FAR and TAR, with 10.85% and 51.36% respectively, it is determined that four features are needed in order to achieve a better performance. The results obtained are still not optimal, but will be helpful to keep working on different aspects of the system until the results are improved.

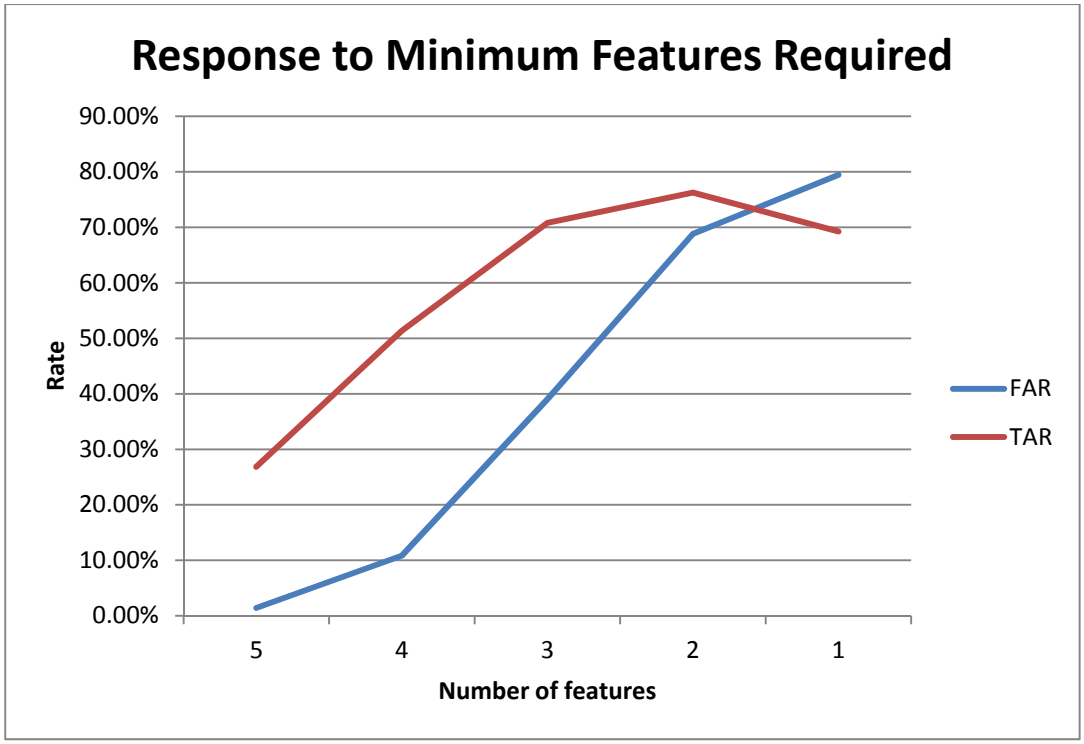

Figure 4-3: Determination of number of features required

4.1.4 Individual Threshold Values for Features

To improve the results obtained in section 4.1.3, a different experiment was performed using the same conditions: 30 seconds for training and 4 seconds for authentication.

Using the median values as a reference for the normalization, a requirement of 4 valid time features was set to accept as a match, and the same 10 subjects from the MCRLab at the University of Ottawa were used.

The goal of this experiment is to set individual threshold values for each feature based on the deviance observed for each one during previous experiments.

Therefore, the experiment started by setting a threshold of 101% for all features; this value was then decreased by 10%, feature by feature, until it reached 1% for all features.

For a better explanation, the sequence is as shown in Table 4-1. Each feature is reduced by 10% and this results in 7776 combinations, where FAR and TAR were calculated for each of these combinations and is shown in Figure 4-4.

Sequence	RLP	RP	RQ	RS	RT
1	101	101	101	101	101
2	101	101	101	101	91
…	101	101	101	101	…
…	101	101	101	101	1
…	101	101	101	91	101
…	101	101	101	…	…
…	101	101	101	1	…
…	101	101	91	101	101
…	101	101	…	…	…
…	101	101	1	…	…
…	101	91	101	101	101
…	101	…	…	…	…
…	101	1	…	…	…
…	91	101	101	101	101
…	…	…	…	…	…
7776	1	1	1	1	1

Table 4-1: Combination sequence

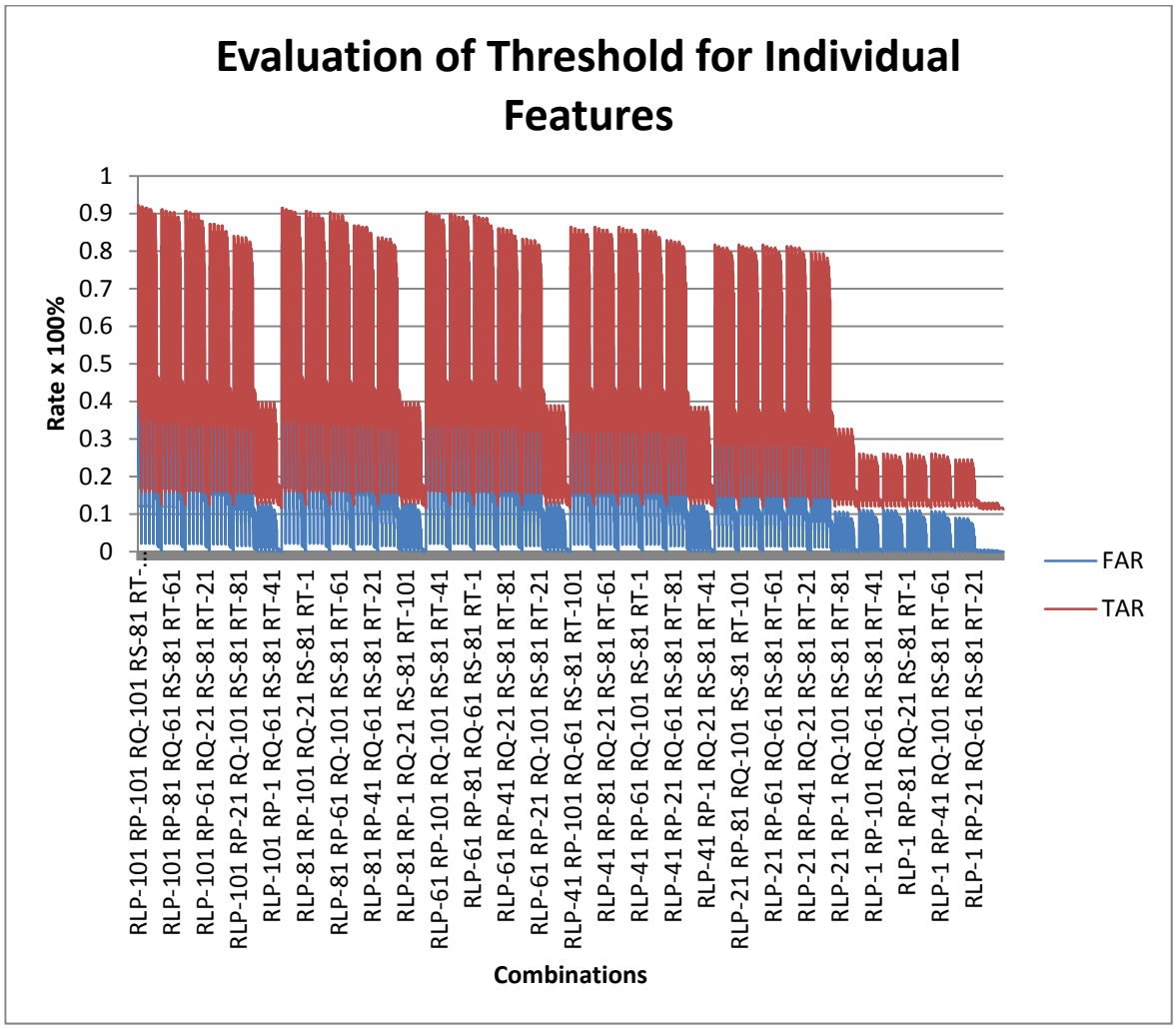

Figure 4-4: Threshold combination for each feature

For a better appreciation of the information displayed in Figure 4-4, note that the data is sorted in a descending order by TAR, and this is shown in Figure 4-5, where it can be observed that a big gap occurs in combinations between RLP-21 RP-41 RQ-41 RS-21 RT-21 and RLP-81 RP-61 RQ-81 RS-21 RT-1.

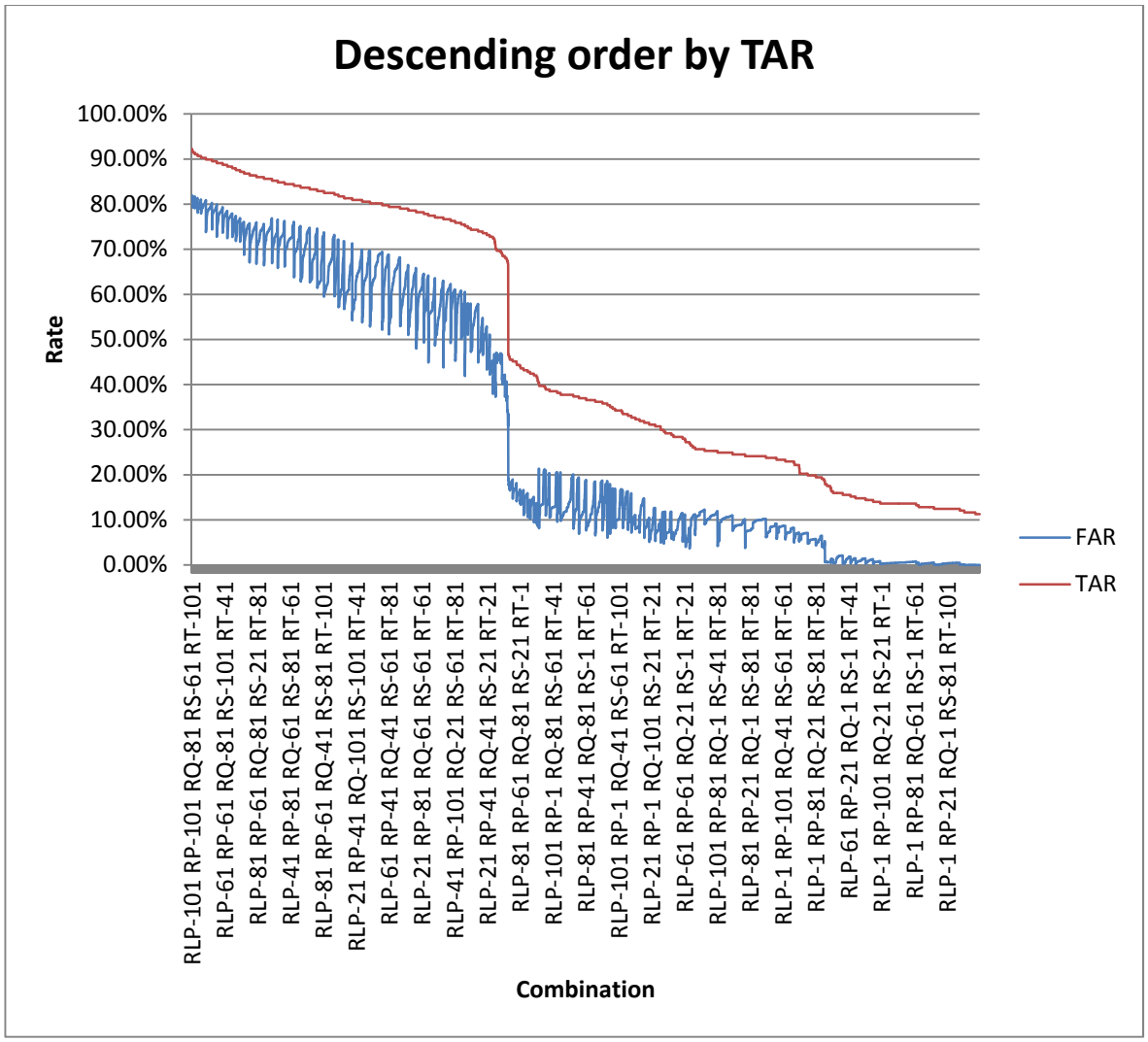

Figure 4-5: Combination features in descending order by TAR

For a better estimation of the values, a zoom on the information data is performed by reducing all the plotted data into a smaller window, as shown in Figure 4-6. It can be observed that the biggest gap between FAR and TAR is at the combination RLP-21 RP-21 RQ-21 RS-21 RT-21.

This combination representing the values for each feature is considered as a starting point to determine the best threshold for each feature. The computation time required to perform this test was

very high, therefore it was done only by leaps of 10%, but with this reference, smaller hops can be made around these values in order to determine the best thresholds.

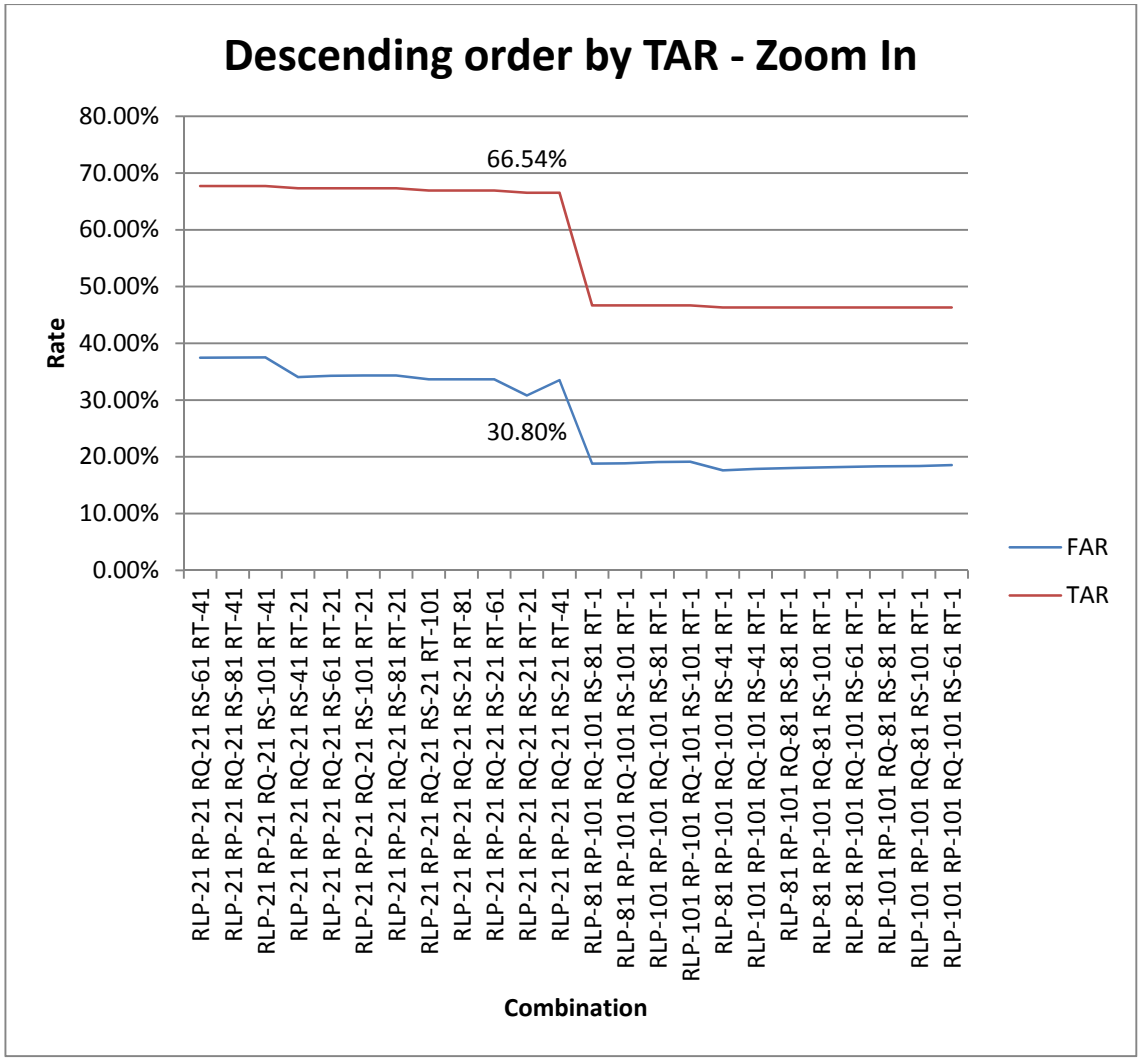

Figure 4-6: Zoom in of combination features in descending order by TAR

With the starting point of combination RLP-21 RP-21 RQ-21 RS-21 RT-21, a similar test is run, but this time the percentage is decreased by 1% at a time, from 20% (rounded from 21%) to 10%, or until a bigger gap in the TAR is observed.

For the feature RLP, it can be observed in Figure 4-7 that while the threshold is reduced, the TAR of the system remains constant at 80% while the FAR is gradually decreased until the threshold reaches 12%.In the transition from 12% to 11%, the TAR changes from 80.00% to 78.18%; given this change, it is decided to take 12% as a starting point for a later evaluation.

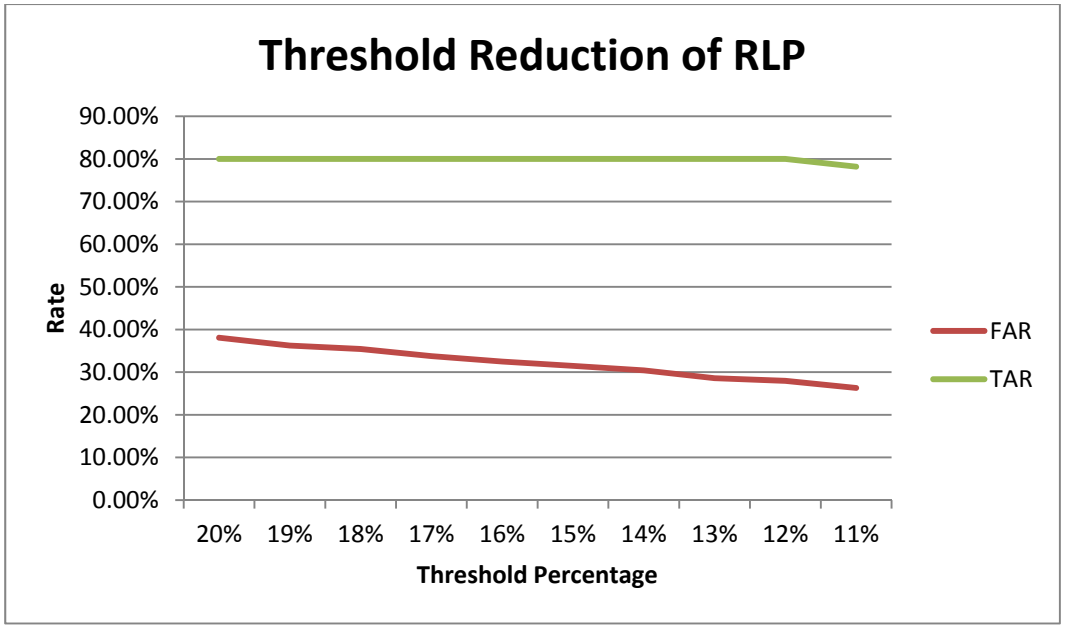

Figure 4-7: Estimation of RLP threshold

In Figure 4-8 the RP feature shows a change on the transition from 19% to 18%; TAR goes from 80.00% to 76.36%, and the 18% threshold is therefore considered as starting point for a later evaluation.

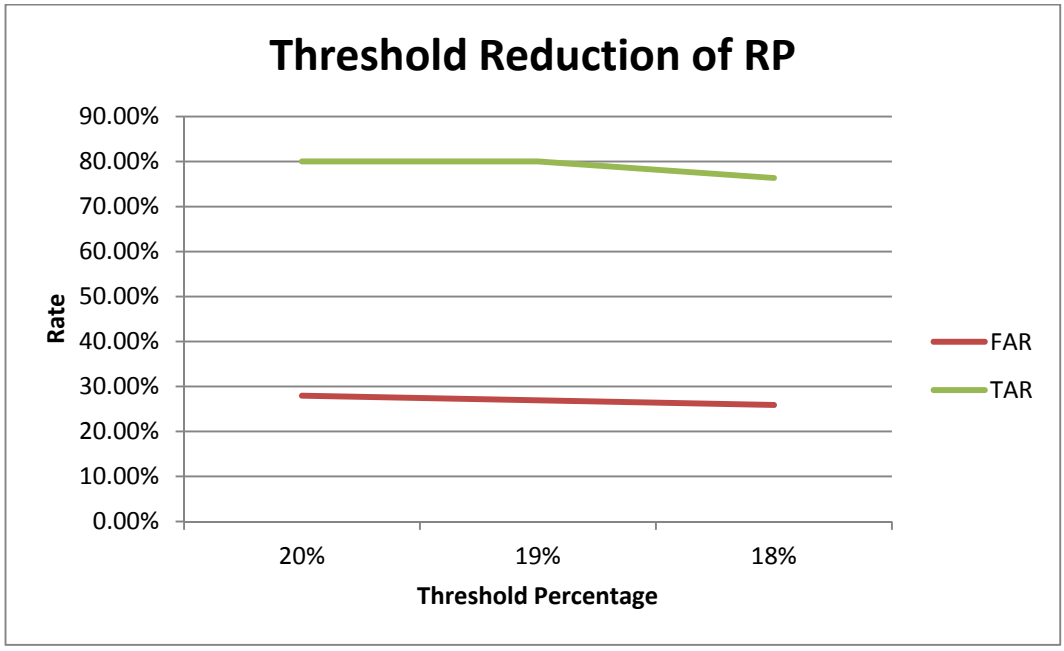

Figure 4-8: Estimation of RP threshold

The threshold for RQ shows a change in TAR from 76.36% to 74.55% when threshold goes from 18% to 17%, this can be observed in Figure 4-9, where FAR is 24.43%.

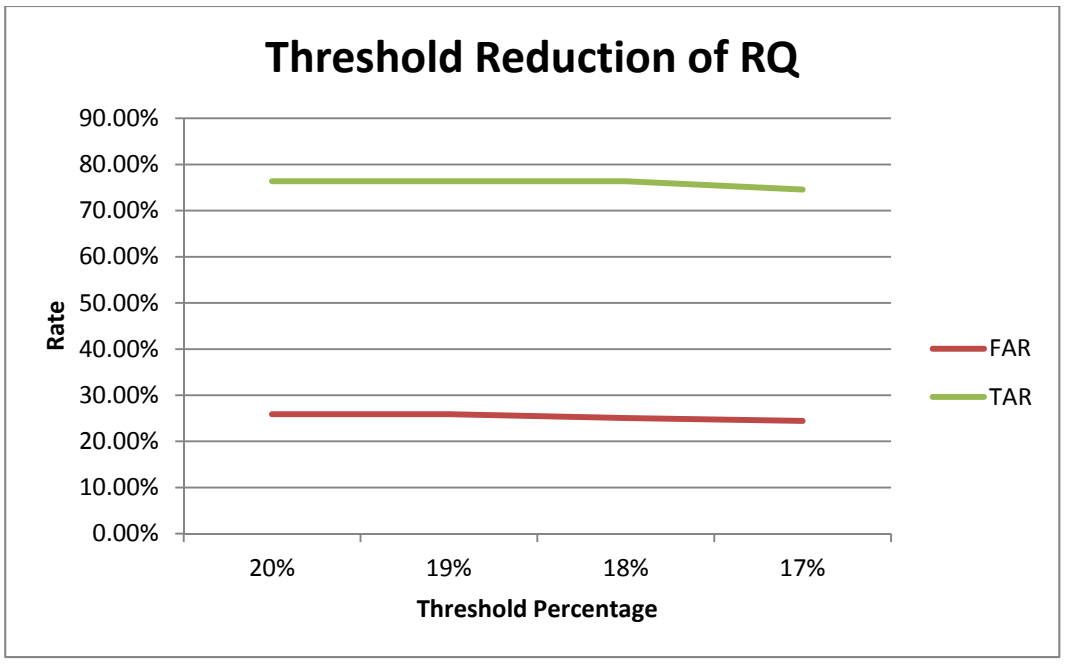

Figure 4-9: Estimation of RQ threshold

For RS, shown in Figure 4-10, the change is observed when the threshold changes from 13% to 12%, with a change of TAR from 74.55% to 72.73%. FAR is 20.7 % when the threshold is set to 12%.

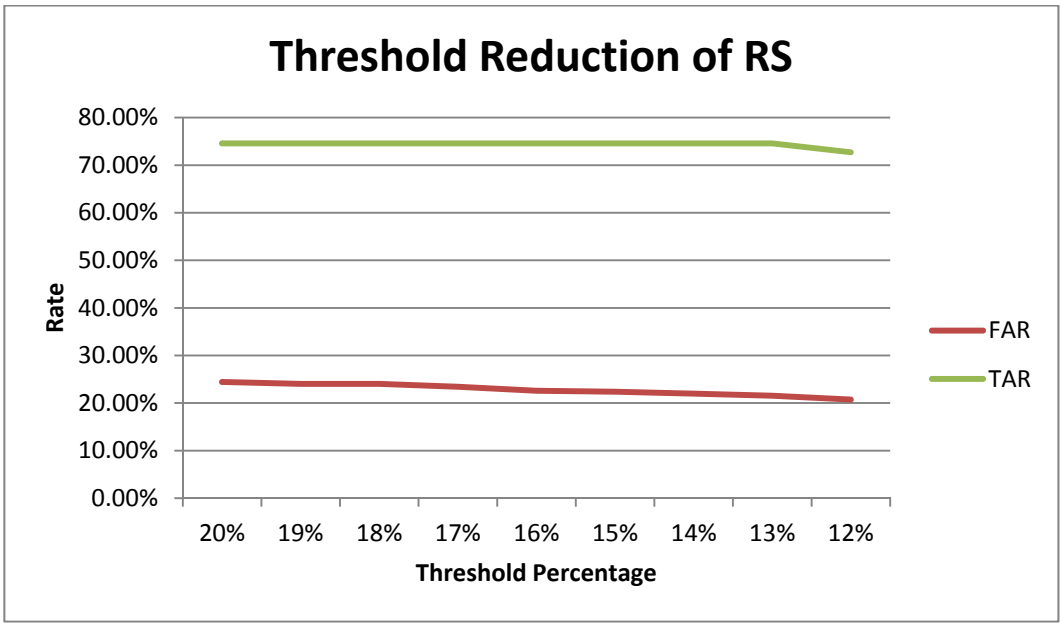

Figure 4-10: Estimation of RS threshold

In Figure 4-11 changes are observed for RT, the last feature, when the threshold goes from 12% to 11%. At a threshold of 11% the TAR is 70.91% with a FAR of 16.36%.

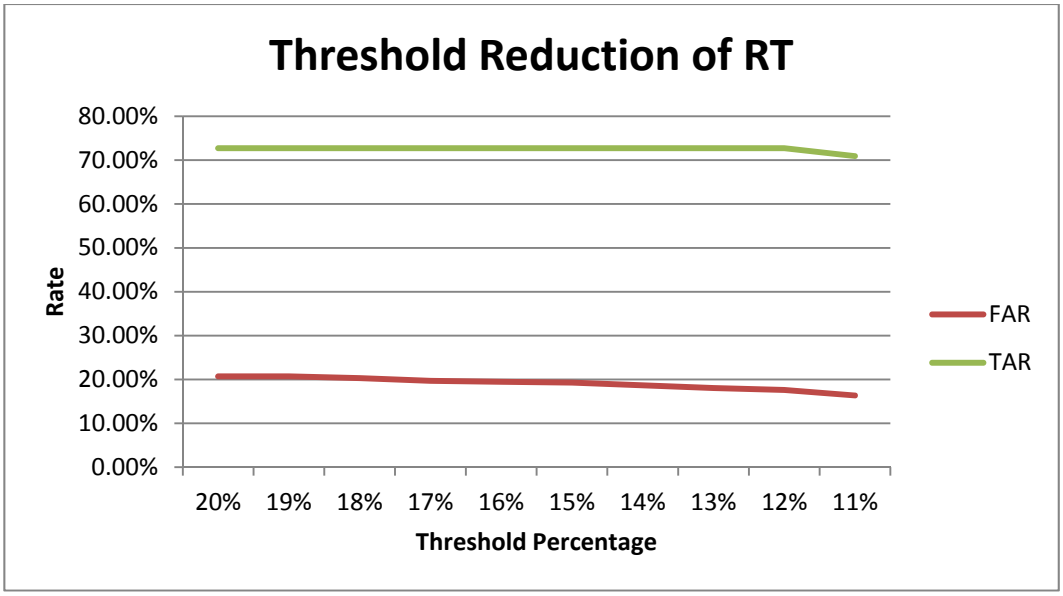

Figure 4-11: Estimation of RT threshold

With all these tests the new threshold combination value is set to RLP-12 RP-18 RQ-17 RS-12 RT-11, which gives a TAR of 70.91% and a FAR of 16.36%. This is a starting point for a heuristic experiment in order to achieve better results by moving values across features based on the deviance of each feature.

From these points FAR and TAR are very stable, which means that the separation distance between them does not vary that much; if the TAR increases the FAR will also increase and vice versa. After modifying the threshold values for each feature, the final results are shown in Table 4-2.

	RLP	RP	**RQ**	**RS**	**RT**	**FAR**	**TAR**
Percentage	13.20 %	18.80 %	17.09%	12.60 %	11.30 %	**19.04 %**	**80.00 %**

Table 4-2: Final threshold values for time based features

The results of Table 4-2 show that the system has a high FAR with an acceptable TAR, which is why the features were adjusted to comply with a minimum TAR of 80%.

However to adjust the FAR another modification to the algorithm is needed and is discussed in the following section.

4.1.5 Implementation of Amplitude Based Features

The results obtained in the previous section show a high rate of FAR; a new approach is therefore needed. The use of two extra features based on amplitudes has been considered for this system, these being RQA and RSA, as shown in Figure 3-21. These amplitudes are relative measures between the R peak and the Q and S peaks, thus are not affected by constant changes of potential. These changes affect the peaks in relation to ground or zero volts; the potential differences are still the same.

RQS peaks have been considered as these features are very clear in the signal obtained from the two electrodes ECG case that will be used for authentication in mobile devices.

The insertion of the amplitudes in the system also requires individual thresholds for these features. The first attempt to obtain the best values to use in the system produced a threshold starting at 45 % for RTA and at 26 % for RSA and the same values for the time based features of the previous section.

Another aspect that is reconsidered is the number of minimum valid features required for a match, the “Min. Valid” value, and this is because there are now seven features instead of five. Based on the response of the system when the threshold values are changed, a final approximation is approached by evaluating different threshold combinations of the features, as in Table 4-3.

FEATURE	Comb. 1	Comb. 2	Comb. 3	Comb. 4
RS	12.60 %	12.60 %	12.90 %	12.90 %
RT	11.30 %	11.3 %	11.30 %	11.30 %
RQ	17.09 %	17.09 %	17.09 %	17.09 %
RP	18.80 %	18.80 %	18.80 %	18.80 %
RLP	13.20 %	13.20 %	13.20 %	10.00 %
RQA	45.00 %	30.00 %	26.00 %	25.90 %
RSA	26.00 %	26.00 %	16.50 %	11.00 %
Min. Valid	6	4	4	4

Table 4-3: Feature combinations for amplitude and time based features

Combination four is the one that achieves the best results, as can be seen in Figure 4-12. FAR reaches 2.22 % and TAR 81.82%.

At this point the system seems to have improved significantly over the previous approaches, using the same strategy but just adding the amplitude features; the acquisition time is still 30 seconds and the authentication time 4 seconds.

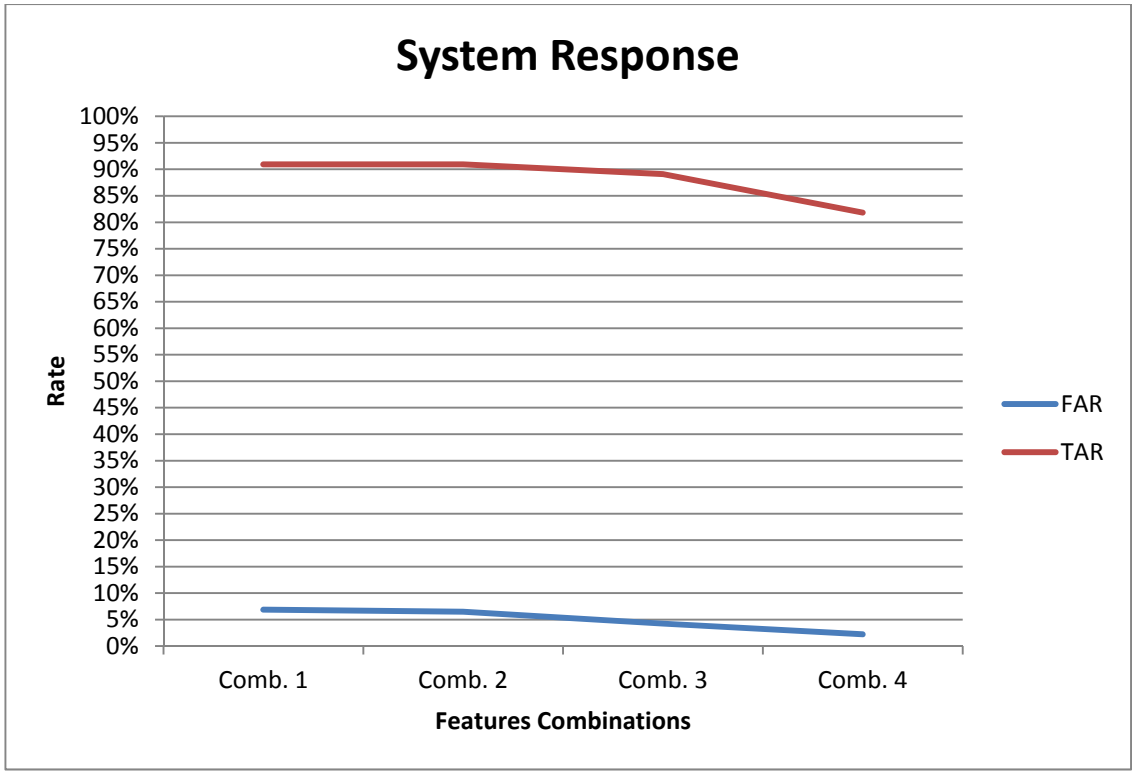

Figure 4-12: System response with seven feature combinations

4.2 Final Testing Procedure and Environment

At this stage, reducing FAR without affecting TAR becomes more challenging. In order to improve the ECG authentication algorithm for mobile devices, a final test is performed, where the validation algorithm changes the way to process the amplitude features together with the time features. This is one of the main contributions of this work and it can be seen in Figure 3-23.

The validation process uses a hierarchy order and separates the five ECG features based on time in one group, the RSA ECG amplitude feature as a single element of another group, and a third group that contains the RQA ECG amplitude feature. If the authentication performed by the first group obtains a valid result, then it evaluates the authentication of the second group; if the evaluation of the second group is valid, then it does a final check of the third group, and if this last validation succeeds, then the system will consider it a match. If at any of these stages the validation fails, the system will consider it a non-match.

The test was performed using the same data available, with a training time of 30 seconds and an authentication time of 4 seconds; the threshold value for the features based on time are the same as in previous sections, and the combination of thresholds is done with a modification of RQA and RSA features. The adjustment is done according to the response of the system to FAR and TAR. If a non-convenient value

is approached, then the threshold for that feature is stopped and the modification of the next feature starts until it reaches an acceptable value. The combinations with the FAR and TAR results can be observed in Table 4-4.

Combination	RLP	RP	RQ	RS	RT	RQA	RSA	FAR	TAR
1	10.00%	18.80%	17.09%	12.90%	11.30%	25.90%	11.00%	**1.41%**	**65.45%**
2	10.00%	18.80%	17.09%	12.90%	11.30%	24.00%	11.00%	**1.21%**	**65.45%**
3	10.00%	18.80%	17.09%	12.90%	11.30%	23.00%	11.00%	**1.01%**	**65.45%**
4	10.00%	18.80%	17.09%	12.90%	11.30%	22.00%	11.00%	**1.01%**	**65.45%**
5	10.00%	18.80%	17.09%	12.90%	11.30%	21.00%	11.00%	**1.01%**	**63.64%**
6	10.00%	18.80%	17.09%	12.90%	11.30%	22.00%	12.00%	**1.21%**	**70.91%**
7	10.00%	18.80%	17.09%	12.90%	11.30%	22.00%	13.00%	**1.21%**	**78.18%**
8	10.00%	18.80%	17.09%	12.90%	11.30%	22.00%	14.00%	**1.21%**	**76.36%**
9	10.00%	18.80%	17.09%	12.90%	11.30%	22.00%	15.00%	**1.21%**	**78.18%**
10	10.00%	18.80%	17.09%	12.90%	11.30%	22.00%	16.00%	**1.41%**	**78.18%**
11	10.00%	18.80%	17.09%	12.90%	11.30%	22.00%	17.00%	**1.41%**	**81.82%**
12	10.00%	18.80%	17.09%	12.90%	11.30%	22.00%	18.00%	**1.41%**	**81.82%**
13	10.00%	18.80%	17.09%	12.90%	11.30%	22.00%	19.00%	**1.62%**	**81.82%**

Table 4-4: Test results to hierarchy order algorithm

It can be observed in Figure 4-13 that the initial combination 1 has a very low TAR of 65.45% with an acceptable FAR of 1.41%.

As the RQA threshold is decreased, FAR also decreases, maintaining a constant TAR until it reaches combination 5. Therefore, the values of combination 4 are used again and start the modification of the RSA threshold.

When the RSA threshold is increased, the TAR is also increased, maintaining a constant FAR; this can be observed from combinations 6 to 9. From combinations 10 to 12, the TAR keeps improving and the FAR also increases slightly.

There is nothing that will strongly affect the system until combination 13, where FAR is over 1.5% and is considered over the limit set in this work. The final result is combination 12, where FAR is 1.41% and TAR is 81.82%. Here FAR is the same as in the initial combination 1, but TAR has been increased over 16 percent points, which makes the system more reliable.

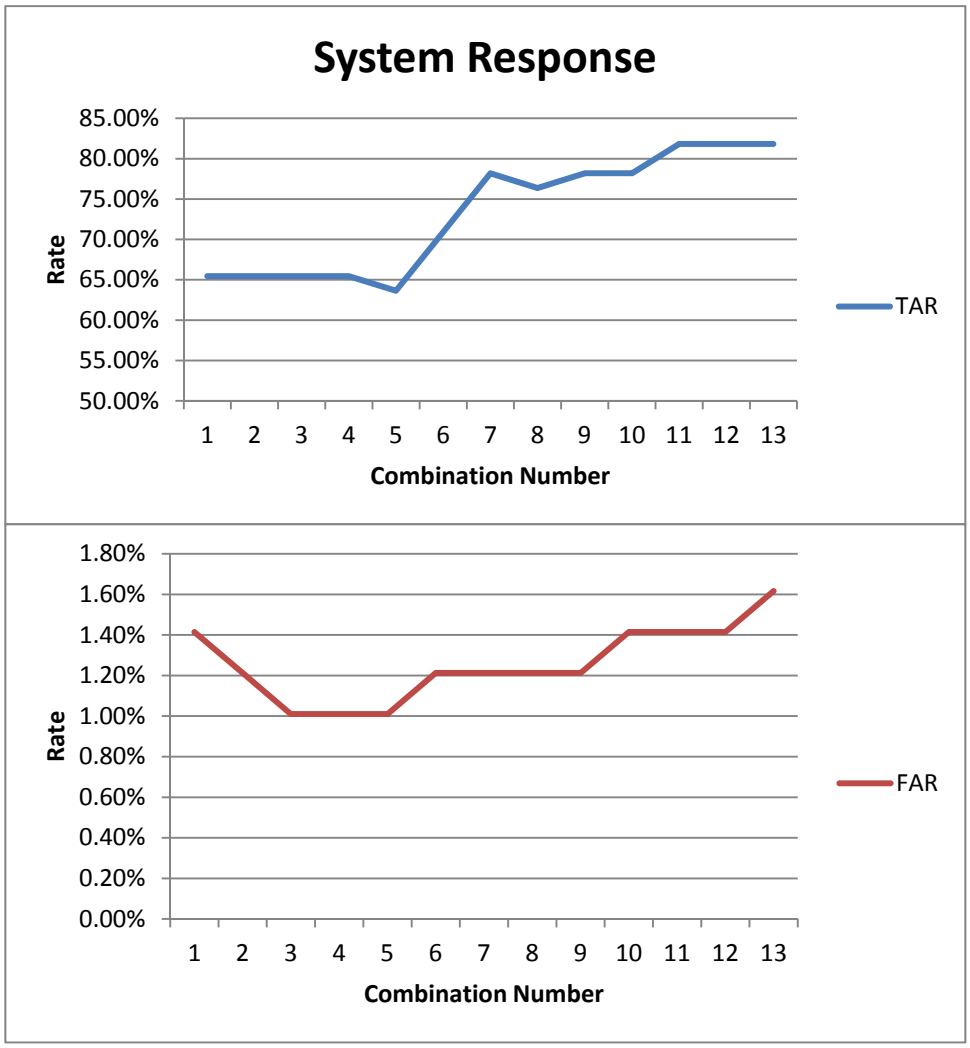

Figure 4-13: System response to hierarchy order algorithm

4.3 Signal Acquisition

4.3.1 Subjects from MCRLab

The signal acquisition was performed with 10 subjects from the MCRLab at the University of Ottawa during three different sessions. Each session was performed on different days or after a change in the activity of the subject. Each session lasted two minutes, during which different tests were performed and the data was acquired with the use of the AliveCor ECG phone case [6] in a laptop computer through MatLab ©.

The environment of acquisition was at one of the desks at the MCRLab, with the subject sitting while holding the phone case close to the computer, as can be seen in Figure 4-14.

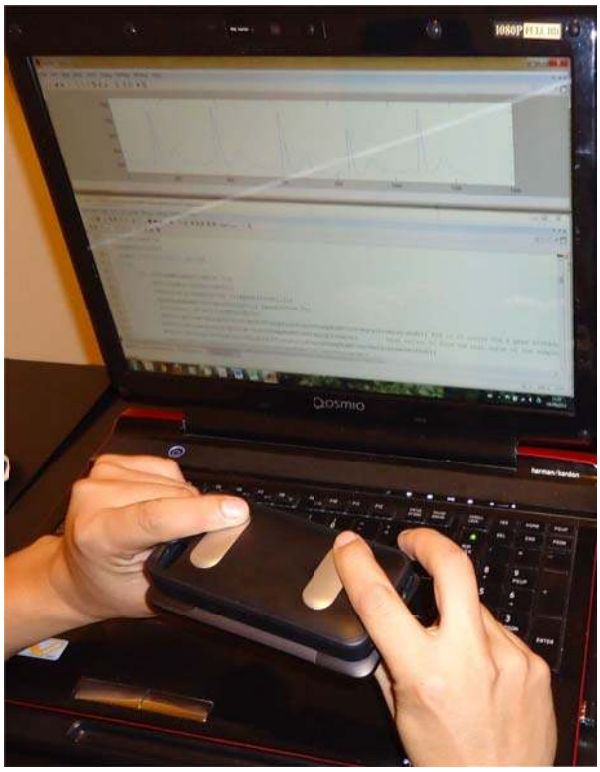

Figure 4-14: Signal acquisition for ECG mobile authentication.

The length of the signal was long but for the experimentation just the amount needed was extracted. In the last experiment of this work, a fragment of 30 seconds was extracted from one of the sessions and three fragments of four seconds from different parts of the same session. Six fragments of four seconds were extracted from the two remaining sessions, 3 fragments from each. This procedure was done for each of the 10 users. With all this information available, the experiment was performed by training the system with one of the 30 second fragment that belongs to one of the users. It then performed the authentication with every fragment of four seconds from all the sessions from all the users. Once completed, the system is trained again with the next 30 second fragment that belongs to another user and again performs the authentication with every fragment of four seconds from all the sessions from all the users. This is repeated until the system completes the training with all 10 users.

4.3.2 Subjects from PhysioNet

For comparison testing purposes, the ECG information from 73 different subjects was extracted from the PhysioNet Database [22] in order to realize a test with similar subjects used by other ECG authentications, and compare the results with the algorithm for ECG mobile authentication. Four databases from Physionet were extracted: European ST-T Database [40], MIT-BIH Normal Sinus

Rhythm Database, MIT-BIH Arrhythmia Database [41] and QT Database [42]. To be more specific, the files corresponding to each subject that was used are shown in Table 4-5.

Subject	File	Subject	File	Subject	File
1	edb/e0105	**26**	edb/e0417	**51**	nsrdb/19093
2	edb/e0106	**27**	edb/e0601	**52**	mitdb/116
3	edb/e0107	**28**	edb/e0603	**53**	mitdb/117
4	edb/e0111	**29**	edb/e0604	**54**	mitdb/121
5	edb/e0113	**30**	edb/e0606	**55**	mitdb/122
6	edb/e0114	**31**	edb/e0607	**56**	mitdb/123
7	edb/e0116	**32**	edb/e0610	**57**	mitdb/124
8	edb/e0118	**33**	edb/e0611	**58**	mitdb/202
9	edb/e0148	**34**	edb/e0613	**59**	mitdb/205
10	edb/e0123	**35**	edb/e0615	**60**	mitdb/212
11	edb/e0133	**36**	edb/e0704	**61**	mitdb/220
12	edb/e0136	**37**	edb/e0801	**62**	qtdb/sel45
13	edb/e0151	**38**	edb/e1301	**63**	qtdb/sel48
14	edb/e0154	**39**	edb/e1304	**64**	qtdb/sel49
15	edb/e0159	**40**	nsrdb/16272	**65**	qtdb/sel811
16	edb/e0161	**41**	nsrdb/16420	**66**	qtdb/sel840
17	edb/e0163	**42**	nsrdb/16483	**67**	qtdb/sel873
18	edb/e0170	**43**	nsrdb/16539	**68**	qtdb/sele0509
19	edb/e0207	**44**	nsrdb/16786	**69**	qtdb/sel100
20	edb/e0404	**45**	nsrdb/16795	**70**	qtdb/sel103
21	edb/e0405	**46**	nsrdb/17453	**71**	qtdb/sel123
22	edb/e0406	**47**	nsrdb/18177	**72**	qtdb/sel116
23	edb/e0408	**48**	nsrdb/18184	**73**	qtdb/sel117
24	edb/e0410	**49**	nsrdb/19088		
25	edb/e0413	**50**	nsrdb/19090		

Table 4-5: Files for subjects extracted from PhysioNet database

The conditions from each subject are not specified in most of the cases, and to adjust the signals to the present work, the signal of each subject was divided into four fragments of data, one of 30 seconds for training, and three of 20 seconds for authentication; each fragment was taken from different times of the subject's signal.

4.4 Data Comparison

In this work, an algorithm for ECG mobile authentication was developed, but the question is still whether this algorithm can work for other purposes too, as the traditional ECG authentication that has already been developed.

In order to test if the algorithm works as the other ECG authentication system, one work is picked as a reference for data comparison, and this is the Evaluation of Electrocardiogram for Biometric Authentication by Singh *et. al.* [26], where they use the Physionet database to evaluate an unimodal ECG authentication system.

The database used by Singh *et. al.* [26] is the same as the one specified in section 4.3.2, but in respect to the users, some could be the same and others not, since in this work the users from the databases were picked randomly and the reference work does not specify which users they are using. Nevertheless, some databases are small, therefore some of the users might be the same.

The test was extracted using Matlab, from the files specified in section 4.3.2, and the system was trained for the 73 subjects, one at a time. Each time the system was trained with one of the users, the authentication was performed with the same user and the 72 users left; each user had three tries. Given this condition, it can be said that while testing the system with the information from the PhysioNet database, the algorithm was trained 73 times and the authentication process ran 15987 times.

The results obtained from running the algorithm presented in this work with the PhysioNet database of 73 subjects gives a FAR of 1.2938 % and a TAR of 84.9315 %, which is a little better than the previous results obtained using the 10 users at the MCRLab.

In Table 4-6 it can be observed that the algorithm presented in this work improved the results obtained by Singh *et. al.* by reducing FAR by a little over 5% and increasing TAR by almost 3%. This is under the same conditions presented in the work by Singh. Also, the results from the 10 subjects at the MCRLab are almost the same as the results obtained by using the Physionet database, hence it can be said that the algorithm for the ECG mobile authentication can be used as a traditional ECG authentication system with a slight improvement on the performance.

	ECG Mobile Authentication		**Singh *et. al.***
	MCRLab	**Physionet**	
FAR	1.41 %	1.29 %	7.00 %
TAR	81.82 %	84.93 %	82.00 %

Table 4-6: Data comparison

4.5 Conclusions

In a first approach of this work, an algorithm founded on the Euclidean distance was used and tested based on previous works that yielded good results. Given the limitations of an ECG authentication applied in mobile devices, a lot of features were missed, which caused poor results for our purpose. Therefore, it can

be said that the Euclidean distance might work in other applications, but it does not perform well for ECG authentication for mobiles because of the hardware limitations necessary to make the system available in a portable system.

The normalization method proposed in this work is different from in previous works in the way that it is performed, but not in concept. This is because the quality of the ECG signal in mobiles can be very low, and a lot of features are missing, one of them is the feature used in previous works to calculate the normalization. In this work, normalization is done with two reference points and these points are the important ones. In a first approach, the results obtained based on an average calculation for the reference points were lower than the results obtained with reference points that were calculated by using the median value. With these results it can be said that the normalization method proposed works better with median values as the means of calculations for reference points.

Normalization is an important aspect that makes the system work despite changes in the heart rate caused by the different states of anxiety of the person. Consequently, normalization is also required in ECG authentication for mobile devices. This concept was clearly stated by previous works, but a short experiment was nonetheless performed to confirm the idea that the same concept applies to this work; the results obtained were as expected and confirmed that normalization is necessary.

Authentication time is very important in ECG authentication for mobile devices as a system with a long authentication time will cause discomfort in the user. Existing algorithms for ECG authentication requires long capture times for an ECG signal to processed. In this work, the time was reduced to 4 seconds for authentication and 30 seconds for training, which makes the system viable to be comfortably used in mobile devices.

The threshold is another important aspect in biometrics, and the approach taken in this work, of different values of thresholds for each feature, produced improved results. These results show that some features are more important than others to distinguish the uniqueness of an ECG feature, therefore the tolerance will be more restrictive for some features and more permissive for others, in order to ensure a correct authentication.

Features based on amplitude are very important for ECG mobile authentication. Using only features based on time is not enough for a reliable system, but by introducing just two amplitude based features, the performance is increased as shown by the evaluation tests presented in this work. Again, the same concept of individual threshold is also applied here, meaning that one amplitude feature needs to be more restrictive than the other in regards to thresholds.

Combining all the features for authentication is not ideal for the purpose of this work, and the approach of using a hierarchy scheme during validation showed an important increase on the performance of the system, maintaining FAR at almost the same value but increasing TAR. The hierarchy scheme presented is a new approach in ECG authentication and the results obtained show that it works better for ECG authentication for mobiles.

The comparison test performed by using the PhysioNet database shows that this algorithm can also be used in different applications. This means that the concepts used in this work are also applied in previous works data conditions, given the fact that the information used to test the algorithm presented here is the same as the one used in the works of other people. The obtained results show that there is an improvement; this progress might not be large, but it is important to consider that this algorithm uses less characteristics from the ECG signal, which makes it less complex and more viable to be applied in simpler systems like mobile devices.

Chapter 5.

Conclusions and Future Work

5.1 Conclusions

The simplicity of the algorithm developed in this work, and its design to work for mobile hardware results in an authentication system using ECG that can be used in mobile devices. To the best of the author's knowledge, this is the first approach in this field which reduces the risk of passive attacks from people watching for password inputs as a letter combination or a graphical pattern. Only the user will know that he/she is being authenticated by touching the electrodes; other people might try to touch and gain access, but the probability of gaining access is of 1.41%.

The use of ECG to protect access to mobile devices is a new approach to mobile authentication, and because of that the risk of the system being hijacked is low. Because the data input method is different from traditional methods, and the ECG data is not a signal that can be easily observed with our eyes, it requires extra hardware to appreciate. Hijacking can therefore be more challenging, but as with any other system, is not impossible. As this technology improves, the odds of the system being hijacked are reduced.

The reduction of time is also a possibility in ECG mobile authentication, which requires only four seconds of signal capture time in order to achieve a good performance. This is also applied in other systems and was tested here with the same input information, getting better results even with a shorter time.

The algorithm presented here demonstrates that fair quality ECG signals from simple hardware can also be used for ECG authentication. A very reliable signal will improve the algorithm's performance, but it is not a requirement for the system to work. The advantage of being able to use fair quality ECG signals is that it makes it possible for ECG to be employed as a mean of authentication in mobile devices.

The normalization technique used in this work allows the algorithm to authenticate users despite how the heart rate changes. This answers the question that many people raise when they hear about ECG authentication; they wonder if it is still valid in different conditions. Normalization was tested in previous works but in this one it was tested using the same concept, that heart rate changes are linear [15] [14], but with a different approach.

The algorithm designed here for ECG authentication on mobiles also works in other applications and with better quality ECG signals. The results are also slightly improved, but it is important to mention that the working environment is more challenging. Since using an ECG on a mobile device does not guarantee a reliable signal, there are less signal characteristics available. In general, the performance is a little better than other systems that use more characteristics, which can be obtained from good quality ECG signals.

More electrodes can be used to improve the results of the algorithm but this approach is not viable in mobiles. This is due the comfort of the user. Depending of the environment that requires the access protection the electrodes can be incremented. But for mobiles a better way to improve the results could be to use different signal processing techniques to extract more features. But we need to be careful about the processing power of the mobile device. A commercial mobile ECG circuitry uses 2.2mW of power; the signal processing stage will probably consume more energy. This aspect needs to be taking in consideration at the time of using different signal processing techniques. A better approach in threshold combination can also be used to improve the results as well a deeply mathematic study in the R peak detection algorithm can help to increase the obtained results.

Previous works around ECG authentication cannot be applied for mobile authentication because the characteristics used are not clearly defined in mobile hardware. Consequently, the good results obtained in previous works would be different when applied in mobile authentication. This work presented an algorithm that can be used here and in other systems since the features used are simple and can be obtained by many different simple or complex hardware.

The hierarchy scheme used in the validation algorithm is a new approach to ECG authentication, not just for mobiles but also for other systems. It was tested to work with PhysioNet data, showing an improvement on the results. The scheme was designed to work for mobile devices, but is not limited to this environment; this can be deduced by the results obtained from different tests.

5.2 Future Work

Since this work is the first approach to ECG mobile authentication, it is thought that there is a lot of room for future work, for example improving the performance by searching for more appropriated thresholds for the individual features of the ECG signal.

Reduction of time required for authentication is another aspect that can be considered for future work. The time used in this work is low, just four seconds, but it can be reduced by trying to extract more features from the fair quality signal or by redesigning the authentication algorithm. This will create even more comfort for users since these days users want everything to be faster.

ECG mobile authentication can also been applied in active authentication; this is a field that can be widely explored given the fact that ECG is a vitality signal and active authentication systems require constant input. Traditional systems use techniques based on a keystroke input or similar and the study of how ECG authentication can perform in active authentication is open to research.

The hierarchy scheme for validation is an algorithm that can also be further tested in other applications, with more signal features and maybe a different hierarchy order to obtain a system with an improved performance, not just for ECG mobile authentication but also for others.

The R peak detection algorithm uses a different approach that works for the purpose of this work, but this could also be tested for medical purposes and the results could be verified to see its feasibility or to improve the methodology to make it work in the medical field. A deeper mathematical study can be performed in order to understand the behavior of the authentication algorithm and increment the performance of the system.

A study of different signal processing techniques can be performed in order to determine if more features can be extracted from the signal in mobile conditions. This will help to increment the accuracy of the system and keep it available for the mobile environment. A study of possible weakness of the system can be performed in order to know better the system and keep improving it.

References

[1] S. K. Sahoo, T. Choubisa and S. R. M. Prasanna, "Multimodal Biometric Person Authentication: A Review," *IETE Technical Review,* vol. 29, no. 1, pp. 54,75, 2012.

[2] R. W. Frischholz and U. Dieckmann, "BioID: A Multimodal Biometric Identification System," *Computer,* vol. 33, no. 2, pp. 64,68, Feb. 2000.

[3] S. Z. Fatemian, F. Agrafioti and D. Hatzinakos, "HeartID: Cardiac biometric recognition," in *Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on*, Washington, 2010.

[4] P. J. Phillips, A. Martin, C. I. Wilson and M. Przybocki, "An Introduction to Evaluating Biometrics Systems," *Computer,* vol. 33, no. 2, pp. 56-63, Feb 2000.

[5] Y. Wang, K. N. Plataniotis and D. Hatzinakos, "Integrating Analytic and Appearance Attributes for Human Identification from ECG Signals," *Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the,* pp. 1,6, Sept. - Aug. 2006.

[6] D. E. Albert, B. R. Satchwell and K. N. Barnet, "Wireless, ultrasonic personal health monitoring system". USA Patent US 8301232 B2, 30 Oct 2012.

[7] F. Agrafioti, F. M. Bui and D. Hatzinakos, "Medical biometrics: The perils of ignoring time dependency," in *IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems, 2009. BTAS '09.*, Washington D.C., 2009.

[8] S. Liu and M. Silverman, "A practical guide to biometric security technology," *IT Professional,* vol. 3, no. 1, pp. 27,32, Jan/Feb 2001.

[9] A. K. Jain and S. Prabhakar, "An introduction to biometric recognition," *Trans. Circuits Syst. Video Technol.,* vol. 14, no. 1, pp. 4,20, Jan. 2004.

[10] . A. K. Jain, A. A. Ross and . K. Nandakumar, Introduction to Biometrics, XVI ed., New York: Spinger, 2001.

[11] S. Pankanti, R. M. Bolle and A. Jain, "Biometrics: The future of identification [Guest Eeditors' Introduction]," *Computer,* vol. 33, no. 2, pp. 46-49, Feb. 2000.

[12] S. K. Dahel and Q. Xiao, "Accuracy performance analysis of multimodal biometrics," in *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society*, 2003.

[13] A. L. Goldberger, Z. D. Goldberger and A. Shvilkin, Clinical Electrocardiography: A Simplified Approach, 8th ed., Philadelphia: Elsevier, 2012.

[14] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold and B. K. Wiederhold, "ECG to identify individuals," *Pattern Recognition,* vol. 38, no. 1, pp. 133-142, January 2005.

[15] L. Biel, O. Pettersson, L. Philipson and P. Wide, "ECG Analysis: A New Approach in Human

Identification," *IEEE Trans. Instrum. Meas.,* vol. 50, no. 3, pp. 808-812, June 2001.

[16] R. Hoekema, G. Uijen and . A. van Oosterom, "Geometrical aspect of the interindividual variaility of multilead ECG recordings," *IEEE Trans. Biomed. Eng.,* vol. 48, p. 551–559, 2001.

[17] G. Kozmann, R. L. Lux and L. S. Green, "Geometrical factors affecting the interindividual variability of the ECG and the VCG," *J. Electrocardiology,* vol. 33, p. 219–227, 2000.

[18] B. P. Simon and C. Eswaran, "An ECG Classifier Designed Using Modified Decision Based Neural Networks," *Computers and Biomedical Research,* vol. 30, no. 4, pp. 257-272, Aug. 1997.

[19] H. Draper, C. Peffer, F. Stallmann, D. Littmann and H. Pipberger, "The corrected orthogonal electrocardiogram and vectorcardiogram in 510 normal men (frank lead system)," *Circulation,* vol. 30, p. 853–864, 1964.

[20] A. D. C. Chan, M. M. Hamdy, A. Badre and V. Badee, "Wavelet Distance Measure for Person Identification," *IEEE Trans. Instrum. Meas.,* vol. 57, no. 2, pp. 248-253, February 2008.

[21] T. W. Shen, W. J. Tompkins and Y. H. Hu, "One-Lead ECG for Identify Verification," in *Proceedings of the Second Joint EMBS/BMES Conference*, Houston, TX, USA, 2002.

[22] A. L. Goldberger, L. A. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C.-K. Peng and H. E. Stanley, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a New Research Resource for Complex Physiologic Signals," *Circulation,* vol. 101, no. 23, pp. e215-e220, June 2000.

[23] G. Wübbeler, M. Stavridis, D. Kreiseler, R.-D. Bousseljot and C. Elster, "Verification of humans using the electrocardiogram," *Pattern Recognition Letters,* vol. 28, no. 10, pp. 1172,1175, July 2007.

[24] F. Sufi, I. Khalil and I. Habib, "Polynomial distance measurement for ECG based biometric authentication," *Security and Communication Networks,* vol. 3, no. 4, pp. 303,319, 2010.

[25] F. Sufi and I. Khalil, "An Automated Patient Authentication System for Remote Telecardiology," in *International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, Sidney, 2008.

[26] Y. N. Singh and S. K. Singh, "Evaluation of Electrocardiogram for Biometric Authentication," *Journal of Information Security,* vol. 3, no. 1, pp. 39,48, Jan 2012.

[27] Y. N. Singh and S. K. Singh, "Identifying Individuals Using Eigenbeat Features of Electrocardiogram," *Journal of Engineering,* vol. 2013, pp. 1-8, February 2013.

[28] D.-h. Cho, K. R. Park, D. W. Rhee, Y. Kim and J. Yang, "Pupil and Iris Localization for Iris Recognition in Mobile Phones," in *Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. SNPD 2006.*, Las Vegas, NV, 2006.

[29] H. Saevanee and P. Bhatarakosol, "User Authentication Using Combination of Behavioral Biometrics over the Touchpad Acting Like Touch Screen of Mobile Device," in *International Conference on Computer and Electrical Engineering, 2008. ICCEE 2008*, Phuket, 2008.

[30] M. Choraś and R. Kozik, "Contactless palmprint and knuckle biometrics for mobile devices," *Pattern Analysis and Applications,* vol. 15, no. 1, pp. 73-85, Feb. 2012.

[31] P. Bours and H. Barghouthi, "Continuous Authentication using Biometric using Keystroke Dynamics," in *The Norwegian Information Security Conference (NISK) 2009*, 2009.

[32] J. Liu and F. R. Yu, "Optimal Combined Intrusion Detection and Biometric-Based Continuous Authentication in High Security Mobile Ad Hoc Networks," *Optimal Combined Intrusion Detection and Biometric-Based Continuous Authentication in High Security Mobile Ad Hoc Networks,* vol. 8, no. 2, pp. 806,815, February 2009.

[33] September 2013. [Online]. Available: http://rt.com/usa/hackers-bounty-iphone5s-fingerprint-157/.

[34] J. A. Van Alste and T. S. Schilder, "Removal of Base-Line Wander and Power-Line Interference from the ECG by an Efficient FIR Filter with a Reduced Number of Taps," *IEEE Transactions on Biomedical Engineering,* vol. 32, no. 2, pp. 1052,1060, Dec 1985.

[35] T. Fisher, February 2013. [Online]. Available: http://www-users.cs.york.ac.uk/~fisher/mkfilter/.

[36] Baum, February 2013. [Online]. Available: http://baumdevblog.blogspot.ca/2010/11/butterworth-lowpass-filter-coefficients.html.

[37] A. T. Boye, C. Steffensen, G. Høgh, J. T. Kristensen, N. C. Holm and P. K. Jensen, March 2013. [Online]. Available: http://kom.aau.dk/group/05gr506/report/node27.html.

[38] B. -U. Kohler, C. Hennig and R. Orglmeister, "The principles of software QRS detection," *IEEE Engineering in Medicine and Biology Magazine,* vol. 21, no. 1, pp. 42,57, Jan-Feb 2002.

[39] F. Sufi, Q. Fang and I. Cosic, "ECG R-R Peak Detection on Mobile Phones," in *29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2007. EMBS 2007.*, Lyon, 2007.

[40] A. Taddei, G. Distante, M. Emdin, P. Pisani, G. Moody, C. Zeelenberg and C. Marchesi, "The European ST-T Database: standard for evaluating systems for the analysis of ST-T changes in ambulatory electrocardiography," *European Heart Journal 13,* pp. 1164, 1172, 1992.

[41] G. Moody and R. Mark, "The impact of the MIT-BIH Arrhythmia Database," *IEEE Eng. in Med. and Biol.,* vol. 20, no. 3, pp. 45,50, May-June 2001.

[42] P. Laguna, R. Mark, A. Goldberger and G. Moody, "A Database for Evaluation of Algorithms for Measurement of QT and Other Waveform Intervals in the ECG," *Computers in Cardiology,* vol. 24, pp. 673,676, 1997.