ECG Based Biometrics Verification System Using LabVIEW

A thesis
Submitted towards the partial fulfillment of
the requirements of the degree of

Master of Engineering
In
Electronic Instrumentation and Control Engineering

Submitted By

Ankit Sharma
Roll No-80751005

Under the esteemed guidance of

Sunil Kumar Singla
Sr.Lecturer,EIED

DEPARTMENT OF ELECTRICAL AND INSTRUMENTATION ENGINEERING
THAPAR UNIVERSITY
PATIALA –147004.

July - 2009

DEDICATED

TO

MY PARENTS

CERTIFICATE

*This is to certify that my work presented in this thesis entitled **"ECG Based Biometrics Verification System Using LabVIEW"** submitted in partial fulfillment of the requirement for the award of the degree of **Master of Engineering in Electronic Instrumentation and Control Engineering** at **Thapar University, Patiala**, is an original record under supervision and guidance of **Mr. Sunil Kumar Singla (Sr. Lecturer).***

The matter embodied in this report has not been submitted anywhere for the award of any degree.

Date: 14/07/09

(Ankit Sharma)
Roll No - 80751005

It is certified that the above statement made by the student is correct to the best of our knowledge and belief.

(Sunil Kumar Singla)
Sr. Lecturer, EIED
(Supervisor)
Thapar University, Patiala

S. Ghosh 14/7/09

(Dr. Smarajit Ghosh)
Professor & Head, EIED
Thapar University, Patiala

(Dr. R. K. Sharma) 16/7
Dean of Academic Affairs
Thapar University, Patiala

ACKNOWLEDGEMENT

The real spirit of achieving a goal is through the way of excellence and austerous discipline. I would have never succeeded in completing my task without the cooperation, encouragement and help provided to me by various personalities.

First of all, I render my gratitude to the ALMIGHTY who bestowed self-confidence, ability and strength in me to complete this work. Without his grace this would never come to be today's reality.

With deep sense of gratitude I express my sincere thanks to my esteemed and worthy Supervisor **Mr. Sunil Kumar Singla (Sr. Lecturer)** in the Department of Electrical and Instrumentation Engineering for his valuable guidance in carrying out this work under his effective supervision, encouragement, enlightenment and cooperation. Most of the novel ideas and solutions found in this thesis are the result of our numerous stimulating discussions. His feedback and editorial comments were also invaluable for writing of this thesis.

I shall be failing in my duties if I do not express my deep sense of gratitude towards **Dr. Smarajit Ghosh,** Professor and Head of Electrical and Instrumentation Department who has been a constant source of inspiration for me throughout this work.

I am grateful to **Dr. R.K. Sharma**, Dean of Academic Affair for his constant encouragement that was of great importance in the completion of the thesis.

I extend my thanks to **Dr. K.K. Raina**, Deputy Director and **Dr. Abhijit Mukherjee**, Director, Thapar University for their valuable support that made me consistent performer.

I am also thankful to all the staff members of the Department for their full cooperation and help.

My greatest thanks are to all who wished me success especially my parents, my siblings, my junior Rahul Dev Nigam, Yatendra Rawal & Ankit Sharma, my batch mates Manish Sharma, Rajiv Yadav, Vivek Chaudhary for their support and care.

Place: TU, Patiala

ANKIT SHARMA

ABSTRACT

Now days, Biometrics is being used extensively for the purpose of security. Biometrics deals with identifying individuals with their physiological such as fingerprint DNA, ECG etc or behavioral traits i.e. rhythm, gait, voice etc. But some of these biometrics can be copied e.g. voice and fingerprint. They do not provide the guarantee of liveness of the subject e.g. fingerprint of a person who is dead can be taken. So the liveness of the object becomes a necessary requirement for the completion of the biometric system.

ECG has the property of liveness. It cannot be collected without the knowledge of the person and it varies from the person to person even in identical twins. Also ECG based biometric system can be easily cascaded with other biometric systems to enhance the reliability and security of the system

In the present work an ECG based biometric system has been developed. The developed system uses the LabVIEW (Laboratory Virtual Instrument Engineering Workbench) 7.1 platform. The developed system is user friendly and provides the result in real time. A database of 20 person having 10 samples per person has been created. The experiments conducted on the above database suggest that an accuracy of 97% has been achieved with the developed system.

LIST OF CONTENTS

LIST OF FIGURE

LIST OF TABLES

Chapter 1

Introduction

1.1 Introduction

Humans recognize each other according to their various characteristics such as by their face when we meet them and by their voice as we speak to them. Identity verification (authentication) in computer systems has been traditionally based on something that one has (key, magnetic or chip card) or one knows (PIN, password). Things like keys or cards, however, tend to get stolen and passwords are often forgotten or disclosed. To achieve more reliable verification or identification one should use something that really characterizes the given person.

1.1.1 Biometrics:

The term "biometrics" is derived from the Greek words bio (life) and metric or metry (to measure). Interestingly, the term "biometrics" [1] was not used to describe these technologies until the 1980s.

Biometrics refers to methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In information technology, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric characteristics can be divided in two main classes:

- Physiological are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, ECG, hand and palm geometry, iris recognition, which has largely replaced retina, and odor/scent.
- Behavioral are related to the behavior of a person. Examples include, but are not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics for this class of biometrics.

Biometric technology involves acquire and storage of useful features of an individual for subsequently recognizing that individual by automated means.

Automated methods of recognizing a person based on a biological or behavioral characteristic is the basic tenet underlying biometrics. Biometric authentication is the "automatic," "real-time," subset of the broader field of human identification [2]. Humans recognize each other according to their various characteristics. For example, friends, family, and co-workers recognize each other by faces and voices.

A biometric system is essentially a pattern recognition system that recognizes a individual by comparing the binary code of a uniquely specific biological or physical characteristic to the binary code of the stored characteristic. Samples are taken from individuals to check if there is similarity to biometric references previously taken from known individuals. The system then applies a specialized mathematical algorithm to the sample and converts it into a binary code and then compares it to the template sample to determine if the individual can be recognized. A reference model or reference containing the biometric properties of a person is stored in the system (generally after data compression) by recording his/her characteristics. These characteristics may be acquired several times during enrollment in order to get a reference profile that corresponds most with reality.

Establishing human identity (unique one with a person already known to the system) reliably has become a major challenge for a modern-day society. The explosive growth in Internet connectivity and human mobility has led to new models of person-to-person interaction that require new ways of proving identity, establishing trust, and authorizing access. Biometric technologies developed in response to this growing worldwide demand for automated human identification include—finger, face, hand, iris, ECG, DNA and other identifiers. All of these rely on the science of pattern recognition to establish an individual's identity based on stable physical patterns on his/her body. Today's technology has reached a level of maturity that biometrics are now relied upon by an increasing number of applications in security, identity programs, and identity management systems [3].

This measurable characteristic, the biometric, can be primarily anatomical—such as eye, face, finger image, hand, and voice—or primarily behavioral—such as signature and typing rhythm, but most biometrics combine both anatomical and behavioral components. The biometric system must be able to identify a person based on one or a combination of these biometric identifiers quickly, automatically, and with little or no human intervention in the decision.

With biometric technology, a more robust level of security and protection can be achieved in the identification component of access control, ID, and verification programs.

Three basic means or levels of identification are often referred to in identity management function [4]:

- The lowest level is defined as “something you have” in your possession, such as an ID badge with a photograph on it.
- The second level is “something you know,” such as a password used with computer login or PIN code to use at a bank ATM.
- The highest level is “who you are,” which encompasses biometrics - the measurement of physical characteristics or traits.

1.1.2 Process for Biometrics Technology

Biometrics Technology is used to identify individuals as discussed earlier. For this process the first step is to enroll those individual in the memory of the system. In this step acquire the particular biological signal from that individual, process that to find out its features and then store these features in the memory of program so they can be used in verification process. Generally multiple readings are taken in enrollment process so that their class can be made.

Second step is to identify the person. In this step again we take that particular biological signal from the test person, process that for extract feature from it, and then compare the features from the references (features which are stored in memory at the time of enrollment). If the coming features are match with the references or lie in the set range of references then the person is true and if didn’t match then it is false.

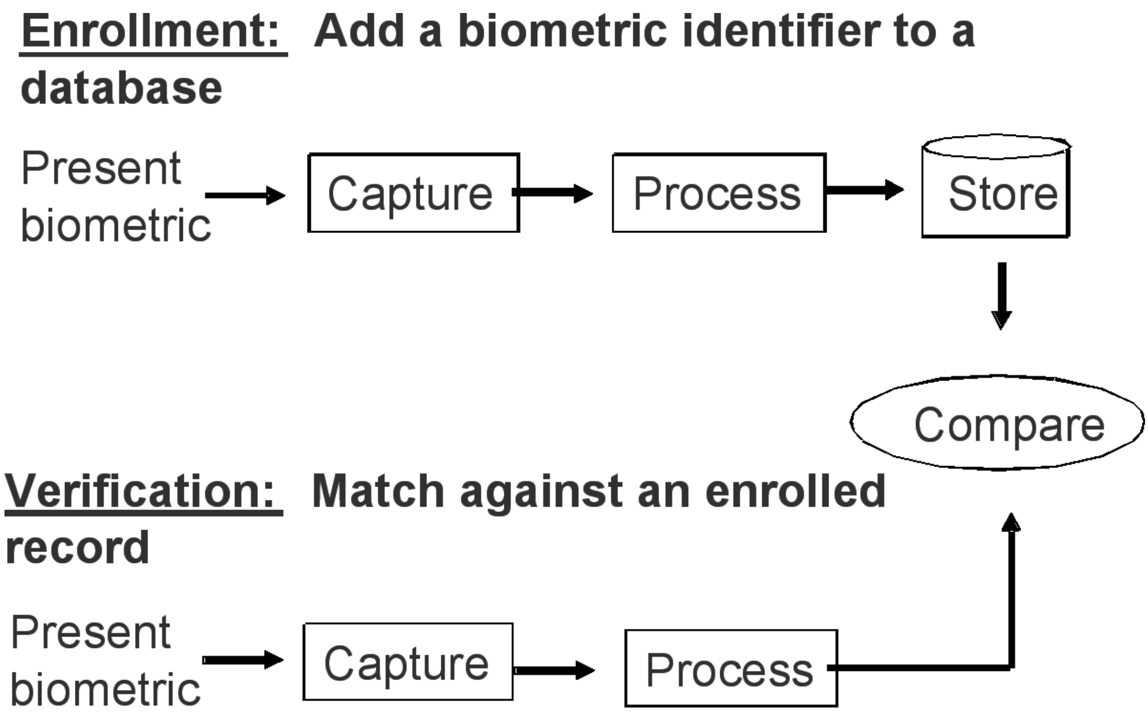


Figure1.1 Biometrics technology process

1.1.2.1 Identification and Authentication

Identification and authentication in the electronic sense ensures that systems have a way of making sure that you are who you say you are. Solutions to achieve this range from traditional username/password regimes to the use of more complex devices such as tokens and biometric scanners.

Identification and authentication (also known as verification) are both used to declare the identity of a user, as in figure 2. Since the two terms identification and authentication are easily confused, we have the following definitions [7]:

1.1.2.1.1 Identification

In an identification system, an individual is recognized by comparing with an entire database of templates to find a match. The system conducts one-to-many comparisons to establish the identity of the individual. The individual to be identified does not have to claim an identity (Who am I?) [7].

1.1.2.1.2 Authentication (verification)

In a verification system, the individual to be identified has to claim his/her identity (Am I whom I claim to be?) and this template is then compared to the individual's biometric characteristics. The system conducts one-to-one comparisons to establish the identity of the individual [7].

Before a system is able to verify/identify the specific biometric of a person, the system requires something to compare it with. Therefore, a profile or template containing the biometric properties is stored in the system. Recording the characteristics of a person is called enrolment as in figure 2 [7].

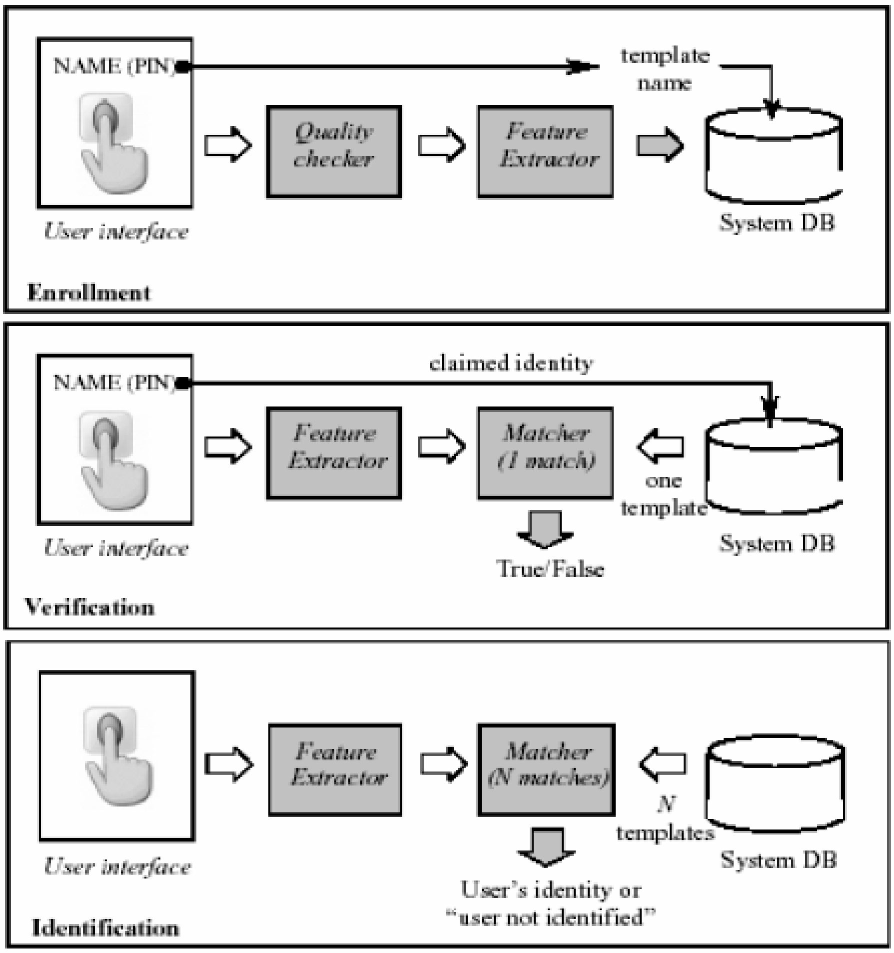


Figure 1.2 Enrolment, verification, and identification

1.1.3 Different type of Biometrics

1.1.3.1 Physiological

a. Fingerprint

A fingerprint is a pattern of ridges and furrows located on the tip of each finger. Fingerprints were used for personal identification for many centuries and the matching accuracy was very high [5]. The fingerprint biometric is an automated digital version of the old ink-and- paper method used for more than a century for identification, primarily by law enforcement agencies. The biometric device involves users placing their finger on a platen for the print to be electronically read. The minutiae are then extracted by the vendor's algorithm, which also makes a fingerprint pattern analysis. Fingerprint biometrics currently has three main application arenas: large-scale Automated Finger Imaging Systems (AFIS) generally used for law enforcement purposes, fraud prevention in entitlement programs, and physical and computer access.

b. Face recognition

Facial recognition records the spatial geometry of distinguishing features of the face. Different vendors use different methods of facial recognition, however, all focus on measures of key features of the face. Because a person's face can be captured by a camera from some distance away, facial recognition has a clandestine or covert capability (i.e. the subject does not necessarily know he has been observed). For this reason, facial recognition has been used in projects to identify card counters or other undesirables in casinos, shoplifters in stores, criminals and terrorists in urban areas.

c. DNA

Deoxyribonucleic acid (DNA) is a nucleic acid that contains the genetic instructions used in the development and functioning of all known living organisms and some viruses. The main role of DNA molecules is the long-term storage of information. DNA is often compared to a set of blueprints or a recipe, or a code, since it contains the instructions needed to construct other components of cells, such as proteins and RNA molecules. The DNA segments that carry this genetic information are called genes, but other DNA sequences have structural purposes, or are involved in regulating the use of this genetic information.DNA is unique to every individual on the planet only identical twins share the same DNA. It can be easily obtained from a variety of sources. It is readily used in forensics to match crime scene evidence to individuals. It does not change during the life!

d. ECG:

The way the heart beats is a unique & private feature of an individual. ECG has various properties which are helpful in biometrics system. Identical twins might have different and distinct electrical activities in their hearts. The Heart is hidden; it is not possible to easily capture the characteristics of an individual's heart without his\her consent. Everybody has a heart. Unlike a fingerprint, some individuals might be disabled and have no hands and thus no fingerprints.

e. Hand and Finger geometry

Hand or finger geometry is an automated measurement of many dimensions of the hand and fingers. Neither of these methods takes actual prints of the palm or fingers. Spatial geometry is examined as the user puts his hand on the sensor's surface and uses guiding poles between the fingers to properly place the hand and initiate the reading. Finger geometry usually measures two or three fingers. Hand geometry is a well-developed technology that has been thoroughly field-tested and is easily accepted by users. Because hand and finger geometry have a low degree of distinctiveness, the technology is not well-suited for identification applications.

f. Iris recognition

The iris begins to form in the third month of gestation and the structures creating its pattern are largely complete by the eight month. Its complex pattern can contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette [6]. Iris scanning is less intrusive than retinal because the iris is easily visible from several meters away. Responses of the iris to changes in light can provide an important secondary verification that the iris presented belongs to a live subject. Irises of identical twins are different, which is another advantage. Newer systems have become more user-friendly and cost-effective.

A careful balance of light, focus, resolution and contrast is necessary to extract a feature vector from localized image. While the iris seems to be consistent throughout adulthood, it varies somewhat up to adolescence.

1.1.3.2 Behavioral

g. Voice

Voice or speaker recognition uses vocal characteristics to identify individuals using a pass-phrase. A telephone or microphone can serve as a sensor, which makes it a relatively cheap and easily deployable technology. However, voice recognition can be affected by environmental factors such as background noise. This technology has been the focus of considerable efforts on the part of the telecommunications industry and the U.S. government's intelligence community, which continue to work on improving reliability.

h. Keystroke

Keystroke dynamics is an automated method of examining an individual's keystrokes on a keyboard. This technology examines such dynamics as speed and pressure, the total time taken to type particular words, and the time elapsed between hitting certain keys. This technology's algorithms are still being developed to improve robustness and distinctiveness. One potentially useful application that may emerge is computer access, where this biometric could be used to verify the computer user's identity continuously.

i. Signature

Dynamic signature verification is an automated method of measuring an individual's signature. This technology examines such dynamics as speed, direction, and pressure of writing; the time that the stylus is in and out of contact with the "paper," the total time taken to make the signature; and where the stylus is raised from and lowered onto the "paper."

1.1.4 Biometric Modules

There are four modules by which a biometric system works. As figure 3 shows there are basically four main modules but depend upon different application it can be varied [8].

a. Sensor Module

It captures the biometric data of an individual. An example is a fingerprint sensor that images the ridge and valley structure of a user's finger.

b. Feature Extraction Module

In which the acquired biometric data is processed to extract a set of salient or discriminatory features. For example, the position and orientation of minutiae points (local ridge and valley singularities) in a fingerprint image are extracted in the feature extraction module of a fingerprint based biometric system.

c. Matcher Module

In which the features during recognition are compared against the stored templates to generate matching scores. For example, in the matching module of a fingerprint based biometric system, the number of matching minutiae between the input and the template fingerprint images is determined and a matching score is reported. The matcher module also encapsulates a decision-making module, in which a user's claimed identity is confirmed (verification) or a user's identity is established (identification) based on the database.

d. System Database Module

It is used by the biometric system to store the biometric templates of the enrolled user. The enrolment module is responsible for enrolling individual into the biometric system database. During the enrolment phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a digital representation (feature values) of the characteristic. The data capture during the enrolment process may or may not be supervised by a human depending on the application.

A quality check is generally performed to ensure that the acquired sample can be reliably processed by successive stages. In order to facilitate matching, a feature extractor to generate a compact but expressive representation, called a template, further processes the input digital representation.

Depending on the application, the template may be stored in the central database of the biometric system or be recorded on a smart card issued to the individual [9]. Usually, multiple templates of an individual are stored to account for variation observed in the biometric trait and the templates in the database may be updated over time.

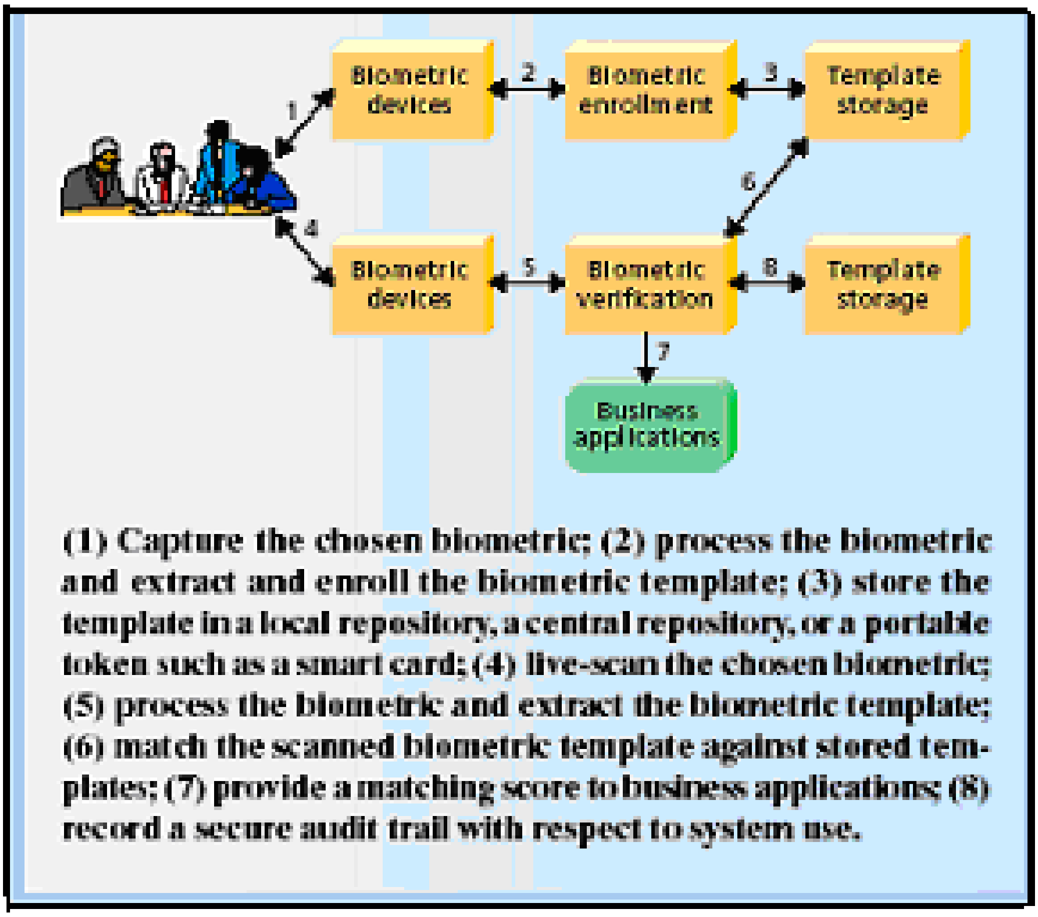


Figure 1.3 Biometric Modules

1.1.5 Application of Biometric Systems

The applications of biometrics can be divided into the following three main groups:

Commercial applications such as computer network login, electronic data security, e-commerce, Internet access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, distance learning, etc.

Government applications such as national ID card, correctional facility, driver's license, social security, welfare-disbursement, border control, passport control, etc.

Forensic applications such as corpse identification, criminal investigation, terrorist Identification, parenthood determination, missing children, etc.. Traditionally, commercial applications have used knowledge based systems (e.g., PINs and passwords), government applications have used token based systems (e.g., ID cards and badges), and forensic applications have relied on human experts to match biometric features. Biometric systems are increasingly deployed in large scale civilian applications. The Schiphol Privium scheme at the Amsterdam airport, for example, employs iris scan cards to speed up the passport and visa control producers. The passengers enrolled in this scheme insert their card at the gate and look into the camera; the camera acquires the image of the traveller's eye and processes it to locate the iris, and compute the iris code the computed iris code is compared with the data residing in the card to complete user verification. A similar scheme is also being used to verify the identity of Schiphol airport employees working in high-security areas. Thus, biometric systems can be used to enhance user convenience while improving security.

1.1.6 Comparison between various biometrics

Various type of biometrics is shown in figure 1.4 with respect to their cost and accuracy. The class of selected biometric for a particular application is based upon these factors and availability of that particular biometric. For high secure system we can use multiple biometrics in a single application. It will enhance the accuracy and cost and decrease the speed of system.

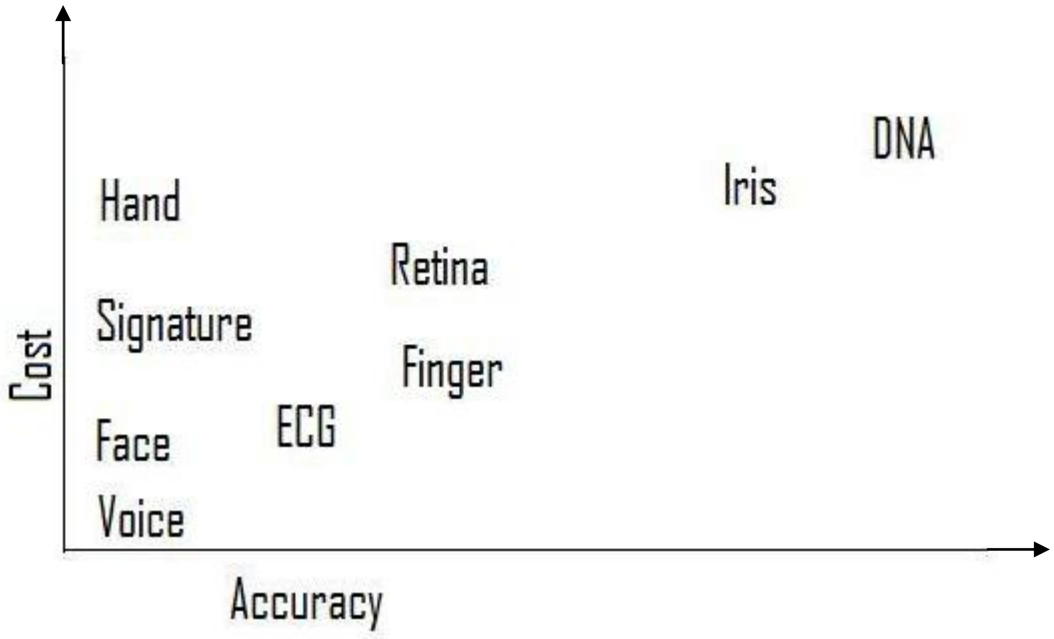


Figure 1.4 Comparisons on the Bases of Cost and Accuracy between Various Biometrics

1.1.7 Errors and Error Rates

No biometric system can recognize a person absolutely. While it appears to give a simple yes or no answer, it is, in fact, measuring how similar the current biometric data is to the record stored in the database and makes a decision according to the probability that the biometric sample comes from the same person that provided the stored biometric template. While there are several types of errors that occur in biometric systems, there are two major classes of errors that relate to the system's accuracy- Comparison errors and decision errors

The errors discussed below have error "rates" associated with them. Thus, a False Match has a False Match Rate (FMR) associated with it, a False Non-Match a False Non- Match Rate (FNMR) and so on. These rates are established by extensive testing, and are nothing more than how often these errors have been shown to occur during testing. Expressed mathematically, a rate is the expected probability that this error will occur in this biometric system. These rates provide quantifiable metrics that allow one to compare the effectiveness of various technologies and the various products therein.

a. Comparison errors are erroneous matches or no matches

That could be considered “machine functions,” or more semantically correct, machine malfunctions.

A false match is an erroneous conclusion by the biometric system that a template stored in its database is from the same person that has just presented a biometric sample, when in fact, it is not.

A false non-match is an erroneous conclusion by the biometric system that a template stored in its database is not from the same person that has just presented a biometric sample, when in fact, it is.

b. Decision errors

These are erroneous conclusions arising from comparison errors. The definitions of decision errors depend upon the application (the premise by which a subject uses the system).

A false accept in an application such as access control, where the subject makes a “positive” claim of enrollment is an erroneous conclusion by the biometric system that a template stored in its database is from the same person that has just presented a biometric sample, when in fact, it is not. A false accept rate (FAR), is the expected probability that this will occur in this particular biometric system, in this application. In a positive identification application, false accept is the same as false match.

A false accepts rate (FAR) is the expected probability that this will occur in this particular biometric system, in this application. In a Negative identification application, false accept is the same as a false non-match, although the rates may be different depending upon the number of comparison attempts made in reaching the “accept” decision.

A false reject in a positive identification application such as access control is an erroneous conclusion by the biometric system that a template stored in its database is not from the same person that has just presented a biometric sample, when in fact, it is. A false reject rate (FRR), is the expected probability that this will occur in this particular biometric system, in this application. In a positive identification application, false reject is the same as false non-match. . A false reject rate (FRR), is the expected probability that this will occur in this particular biometric system, in this application. In a negative identification application, false reject is the same as false match, although their rates may be different depending upon the number of comparisons required to make a “reject” decision.

1.2 Problem Formulation

Different biometrics has different properties. Some of them are easily available to collect as signature, voice. They can be copied and due to which the security of the system is decreases. Fingerprints can be collected from a glass or any surface and then can be copied; also the knowledge of living is necessary in a biometrics system. ECG is different in twins (as in the case of DNA, it is same). These qualities of ECG initiate interest in ECG as biometrics. The aim of this thesis is to

i). Study the different methods/ techniques of ECG biometrics system.
ii). Study the different pre processing techniques of a signal.
iii). Develop and test the ECG biometrics system using LabVIEW.
iv). Test the developed system for its validity on the database stored for the purpose.

Chapter 2

Literature Survey

2.1 Introduction

Electrocardiography (ECG) is the recording of the electrical activity of the heart by using electrodes with respect to time. Skin electrodes are used to record ECG. The etymology of the word is derived from electro, because it is related to electrical activity, cardio related to heart; graph a Greek root meaning "to write".

Electrical impulses in the heart are generated in the sinoatrial node and passes through the intrinsic conducting system to the heart muscle. Myocardial muscle fibers are stimulated by these impulses then contract and thus induce systole. The electrical waves can be measured by placing skin electrode on body. An ECG displays the voltage between pairs of these electrodes, and the muscle activity that they measure, from different directions, also understood as vectors. This display indicates the overall rhythm of the heart and abnormality in different parts of the heart muscle. ECG is used to measure and diagnose abnormal rhythms of the heart, particularly abnormal rhythms caused by damage to the conductive tissue that carries electrical signals.

2.2 History of ECG

The ECG machine has a rich history that has lead to its prominent future in medical equipment and supplies. In 1856 Kollicker and Mueller discovered the electrical activity of the heart when a frog sciatic nerve/gastrocenemius preparation fell onto an isolated frog heart and both muscles contracted synchronously.

Alexander Birmick Muirhead is reported to have attached wires to a feverish patient's wrist to obtain a record of the patient's heartbeat while studying for his Doctor of Science (in electricity) in 1872 at St Bartholomew's Hospital [10]. This activity was directly recorded and visualized using a Lippmann capillary electrometer by the British physiologist John Burdon Sanderson [11]. The first to systematically approach the heart from an electrical point-of-view was Augustus Waller, working in St Mary's Hospital in

Paddington, London [12]. His electrocardiograph machine consisted of a Lippmann capillary electrometer fixed to a projector. The trace from the heartbeat was projected onto a photographic plate which was itself fixed to a toy train. This allowed a heartbeat to be recorded in real time. In 1911 he still saw little clinical application for his work.

An initial breakthrough came when Willem Einthoven, working in Leiden, used the string galvanometer that he invented in 1903. This device was much more sensitive than both the capillary electrometer that Waller used and the string galvanometer that had been invented separately in 1897 by the French engineer Clement Ader [13].

Einthoven assigned the letters P, Q, R, S and T to the various deflections, and described the electrocardiographic features of a number of cardiovascular disorders. In 1924, he was awarded the Nobel Prize in Medicine for his discovery.

Though the basic principles of that era are still in use today, there have been many advances in electrocardiography over the years. The instrumentation, for example, has evolved from a cumbersome laboratory apparatus to compact electronic systems that often include computerized interpretation of the electrocardiogram.

2.3 ECG as Biometrics

From last few years, the electrocardiogram (ECG) has been suggested as a new biometric [14]-[20]. The ECG has some properties. The ECG is usually monitored in medically related applications; therefore, without any additional data requirements, a person’s identity could be verified during online ECG monitoring or through medical records, prior to drug administration or other medical procedures. The ECG information would provide a method for liveness detection, increasing system reliability [21].

2.3.1 Requirement of Liveness of a Biometric

Liveness checks are a technological countermeasure to spoofing using artifacts. They apply most obviously to biological biometrics such as finger, face, hand and iris, though they might also protect behavioral biometrics in cases where mimicry might be performed by an artificial device (e.g. a signature signing machine). Research by Putte and Keuning [22] that tested several fingerprint sensors to check whether they accept an artificially created (dummy) finger instead of a real finger, provides proof of just how crucial liveness testing is but also just how ineffective these liveness mechanisms currently is. The authors [22] describe methods to create dummy fingers with and without the cooperation of the real owner of the biometric. Similarly iris biometrics can give false identification with the help of contact lenses.

Liveness checks may detect physical properties of the live biometric, e.g. electrical measurement, thermal measurement, moisture, reflection or absorbance of light or other radiation, the presence of a natural spontaneous signal such as pulse, or the response to an external stimulus e.g. contraction of the pupil in response to light, muscular contraction in response to electrical signal etc. These Liveness checks in most cases simply don’t measure up to the challenges of the technological advanced, twenty first century criminals of our modern age. A better and more efficient way for a system to be sure that the live biometric of a user is presented at all times is needed.

2.3.2 How ECG biometric system developed

The electrocardiogram (ECG) is a technique of recording bioelectric currents generated by the heart. Clinicians can evaluate the conditions of a patient's heart from the ECG and perform further diagnosis. ECG records are obtained by sampling the bioelectric currents sensed by several electrodes, known as leads. An ECG signal is shown in figure 2.1.

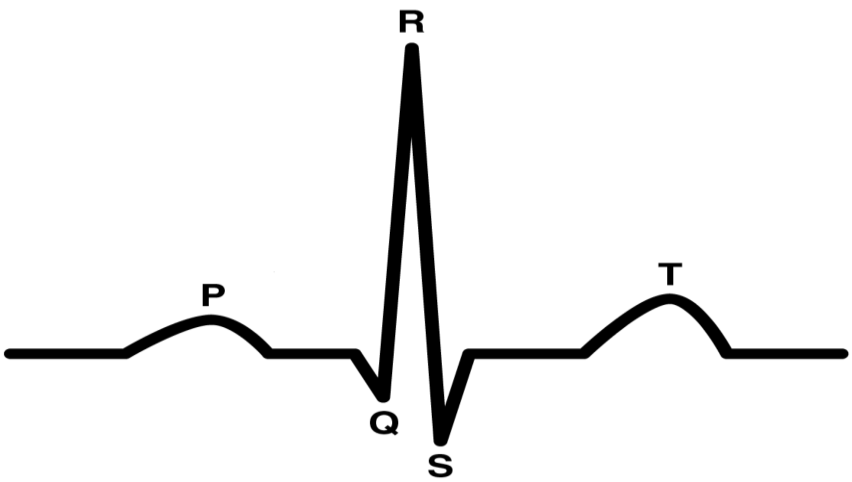


Figure 2.1 Standard ECG waveform

Generally, the recorded ECG signal is often contaminated by noise and artifacts that can be within the frequency band of interest and manifest with similar characteristics as the ECG signal itself. In order to extract useful information from the noisy ECG signals, you need to process the raw ECG signals.

ECG signal processing can be roughly divided into two stages by functionality: preprocessing and feature extraction (as shown in Figure 2.2). The preprocessing stage removes or suppresses noise from the raw ECG signal and the feature extraction stage extracts diagnostic information from the ECG signal.

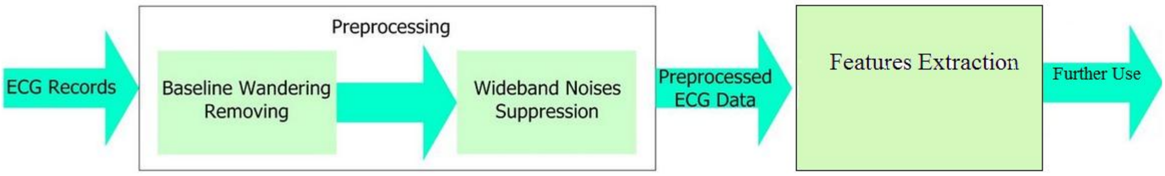


Figure 2.2 Preprocessing of ECG signal

With LabVIEW and related toolkits, such as the Advanced Signal Processing Toolkit (ASPT) and the Digital Filter Design Toolkit (DFDT), one can conveniently build signal processing applications for both stages, including baseline wandering removing, noise cancellation, QRS complexes detection etc.

2.3.2.1 Preprocessing ECG Signals

Preprocessing ECG signals helps remove contaminants from the ECG signals. Broadly speaking, ECG contaminants can be classified into the following categories:

- Power line interference
- Electrode pop or contact noise
- Patient–electrode motion artifacts
- Electromyographic (EMG) noise
- Baseline wandering

Among these noises, the power line interference and the baseline wandering are the most significant and can strongly affect ECG signal analysis. Except for these two noises, other noises may be wideband and usually a complex stochastic process which also distort the ECG signal. The power line interference is narrow-band noise centered at 60 Hz (or 50 Hz) with a bandwidth of less than 1 Hz. Usually the ECG signal acquisition hardware can remove the power line interference. However the baseline wandering and other wideband noises are not easy to be suppressed by hardware equipments. Instead, the software scheme is more powerful and feasible for offline ECG signal processing. Can be use the following methods to remove baseline wandering and the other wideband noise.

2.3.2.1.1 Removing Baseline Wandering

Baseline wandering usually comes from respiration at frequencies wandering between 0.15 and 0.3 Hz, and can be suppressed by a highpass digital filter. Also one can use the wavelet transform to remove baseline wandering by eliminating the trend of the ECG signal. Removal of baseline wandering is necessary because without it features cannot be extracted.

a. Digital Filter Approach

The LabVIEW DFDT provides an intuitive and interactive way to design and implement finite impulse response (FIR) or infinite impulse response (IIR) filters easily and effectively. For example, you can use the Classical Filter Design Express VI to design a Kaiser Window FIR highpass filter to remove the baseline wandering.

b. Wavelet Transform Approach

In addition to digital filters, the wavelet transform is also an effective way to remove signals within specific sub bands. The LabVIEW ASPT provides the WA Detrend VI which can remove the low frequency trend of a signal

This example uses the Daubechies6 (db06) wavelet because this wavelet is similar to the real ECG signal. In this example, the ECG signal has a sampling duration of 60 seconds, and 12000 sampling points in total; therefore the trend level is 0.5 according to the following equation:

$$\text{Trend level} = \frac{\log_2 2t}{\log_2 n} \qquad (2.1)$$

Where t is the sampling duration and N is the number of sampling points. Figure 3 shows the original ECG signal and the resulting ECG signals processed by the digital filter-based and wavelet transform-based approaches. Also it can be observed that the resulting ECG signals contain little baseline wandering information but retain the main characteristics of the original ECG signal. It is also observed that the wavelet transform-based approach is better because this approach introduces no latency and less distortion than the digital filter-based approach.

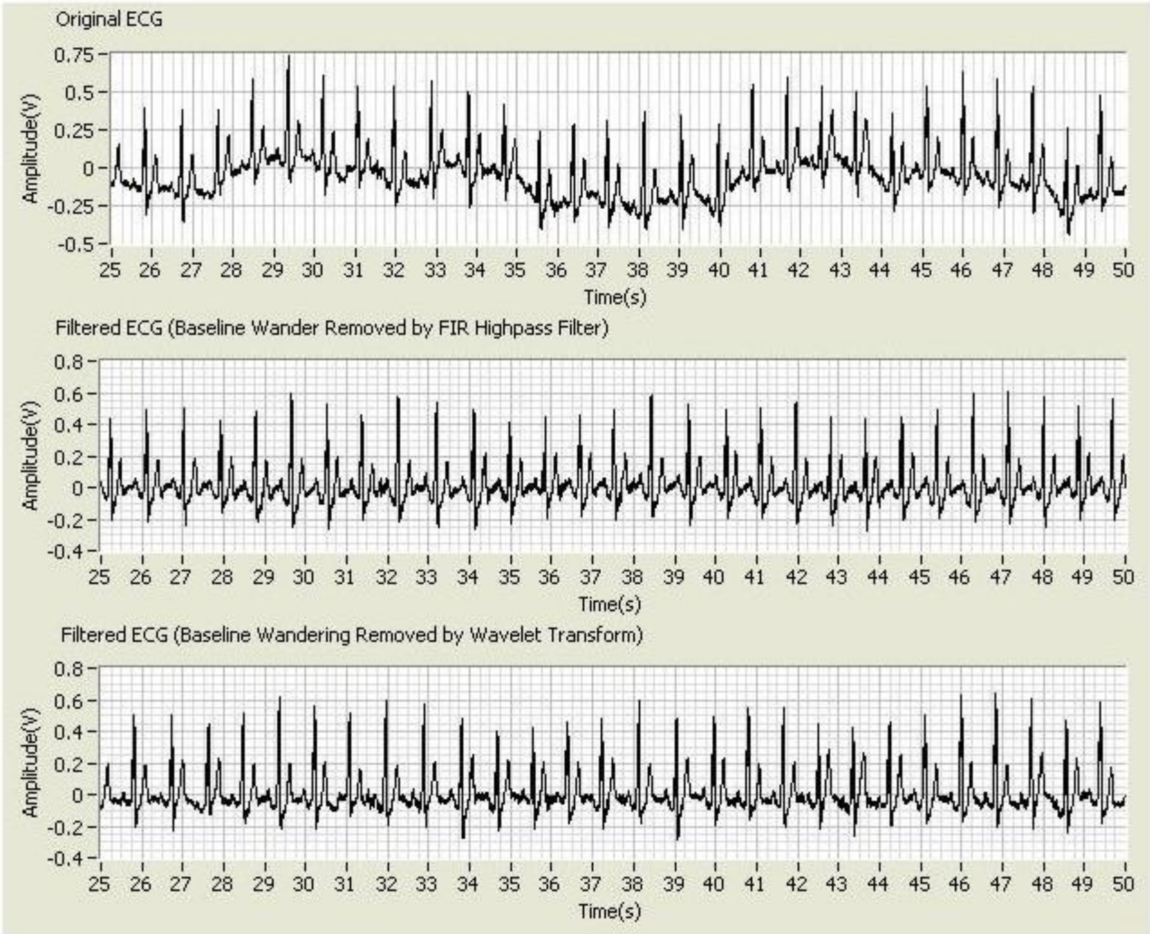


Figure 2.3 ECG waveforms with baseline wandering, and after removed by both techniques.

2.3.2.1.2 Removing Wideband Noise

After removing baseline wandering, the resulting ECG signal is more stationary and explicit than the original signal. However, some other types of noise might still affect feature extraction of the ECG signal. The noise may be complex stochastic processes within a wideband, so cannot be removed by using traditional digital filters. To remove the wideband noises, one can use the Wavelet Denoise Express VI.

This Express VI first decomposes the ECG signal into several subbands by applying the wavelet transform, and then modifies each wavelet coefficient by applying a threshold or shrinkage function, and finally reconstructs the denoised signal. The following figure shows an example of applying the undecimated wavelet transform (UWT) to the ECG signal.

2.3.2.2 Feature Extraction from ECG Signal

ECG varies among individuals due to their different anatomy and physiology of the heart. Normally, a progressive change in individual anatomy takes place from birth to adolescence (~ 16 years of age). It has resulted that some features of ECG varies during aging. There is a change in normal limits of ECG parameters with age and sex [23]. A progressive change from childhood to adult has been reported [24]. These changes are not consistent and vary from one individual to another. These effects are particularly reflected in P wave duration and PR interval. For ECG as biometrics some of available features are selected, processed, recoded, and compared. The selected features are chosen by the different class of ECG features, some of which are discussed below.

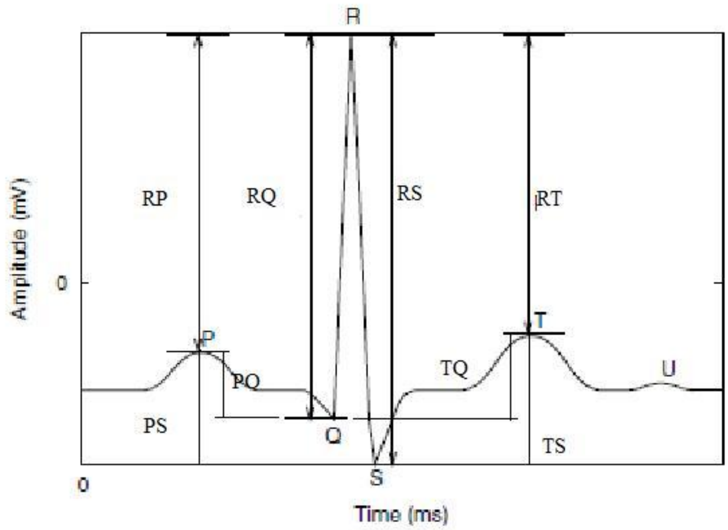


Figure 2.4 Amplitude features of the ECG

In figure 2.4 amplitude features of the ECG signal are shown. These show the difference of amplitude of two amplitude of -two peaks, or a peak and a valley, or two valleys.

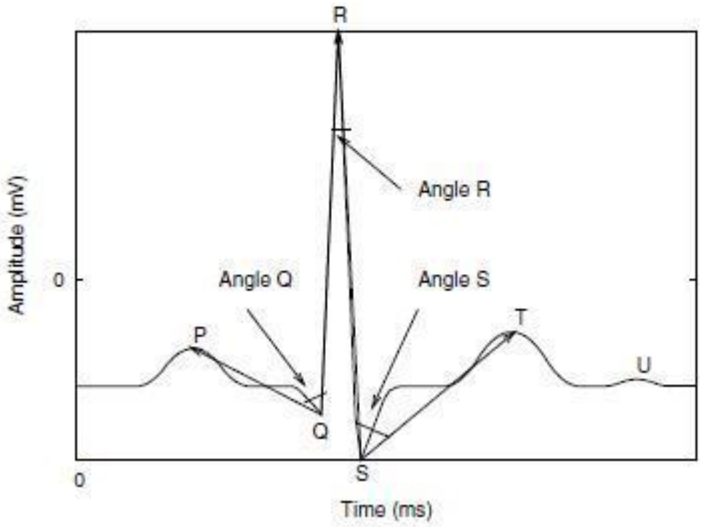


Figure 2.5 Angle feature of ECG signal

In figure 2.5 angle feature of ECG signal are shown. These features are generated by measure angle between PQR, QRS, and RST point of the ECG signal.

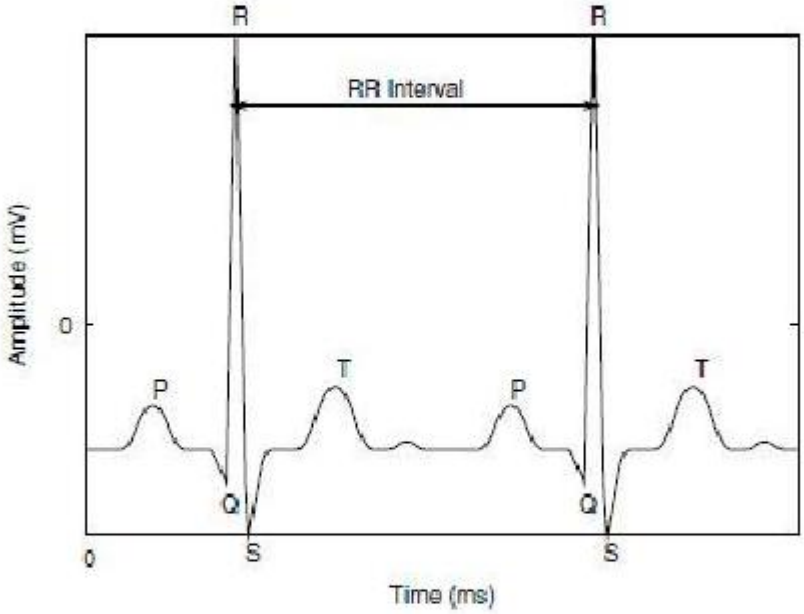


Figure 2.6 RR interval of the ECG signal

In figure 2.6 the RR interval of the ECG signal is shown. It is the time difference of two R peak in the ECG signal.

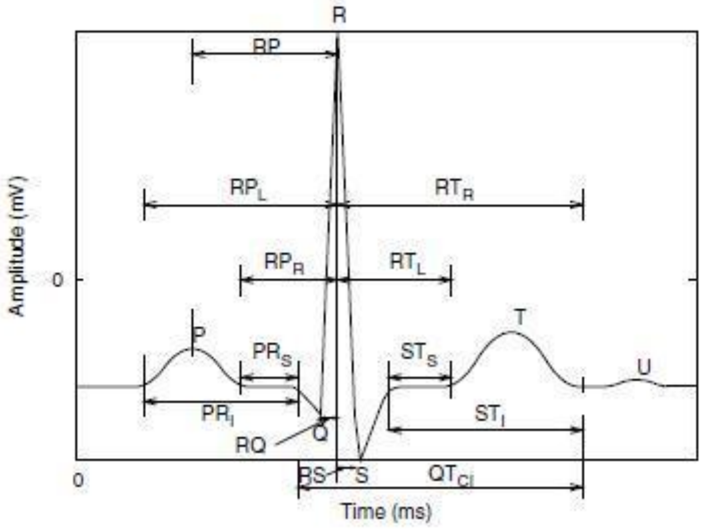


Figure 2.7 Internal features of ECG signal

The figure 2.7 shows the internal features of ECG signal. These are also the time differences between various peaks, valleys, and the duration of peaks.

2.4 Related Research in this Field

H.H.P. Silva, H.F.S. Gamboa, A.L.N. Fred presents a scheme of ECG measurement in biometrics [25]. In which each heartbeat waveform was sequentially segmented from the full recording, and after this, all individual waveforms were aligned by their *R* peaks. From the resulting collection of ECG heartbeat waveforms, the mean wave for groups of *10* heartbeat waveforms (without overlapping), was computed to minimize the effect of outliers. A labeled database was compiled, in which each pattern corresponds to a mean wave. For each mean waveform, the latency and amplitude for each of the *P-QRS-T* peaks were extracted. They get *92±0.7%* subject recognition rate.

D. Hatzinakos, K. Plataniotis, presents a scheme in which Existing solutions for biometric recognition from electrocardiogram (ECG) signals are based on temporal and amplitude distances between detected fiducial points[26]. Such methods rely heavily on the accuracy of fiducial detection, which is still an open problem due to the difficulty in exact localization of wave boundaries. The subject recognition rate is 98%.

Bie, L., Pettersson O., Philipson L., Wide P [14] were among the first to manifest the applicability of ECGs as biometric. Their approach is to extract a set of temporal and amplitude features from heart beats that are normally used in clinical diagnosis. The features were obtained directly from a SIEMENS ECG equipment and their dimensionality was reduced by simple analysis of the correlation matrix. Further selection was based on experiments. The experimental setup involved 20 subjects of varying ages. A 100% human identification rate was achieved but the major drawback of the method was the lack of automatic recognition, since specific apparatus was used for feature extraction.

Shen [19] reported another method for one lead ECG identity verification. First, template matching was used to compute the correlation coefficient among *QRS* complexes in order to verify possible candidates. A decision based neural network (DBNN) was then used to strengthen the validation of the identity resulting from the first step. The experimental results of this system, tested on 20 subjects have provided a recognition rate of 95% for template matching, 80% for the DBNN and 100% for the combination of the two. This methodology was later extended by *Shen* [27] with a larger database containing 168 healthy subjects. The highest identification rate achieved in that work was 95.3%.

Wang [28] suggested an integration of analytic and appearance features from heart beats. The preprocessed ECG signal was subjected to fiducial points detection to measure temporal and amplitude distances. The classification performance showed that even though amplitude features have discriminative ability, analytic features are not sufficient for identification. Experiments were conducted on the extraction of appearance related characteristics with the help of either the principal component or LDA. When the two types of features were combined in a hierarchical scheme, a 100% subject and 98.9% heart beat recognition rates were reported for 13 subjects.

Chapter 3

System Implementation

3.1 Introduction

ECG based biometrics verification system is defined as deciding a person by his heartbeats who he claims to be. It is different than the other biometric verification systems as it also decides liveness of persons. In ECG based biometrics verification system; a person makes an identity claim (e.g., entering an employee number or presenting his smart card). Then his/her ECG is collected by Polyrite machine through surface electrodes. This signal is analyzed by a verification system that makes the binary decision to accept or reject the user's identity claim.

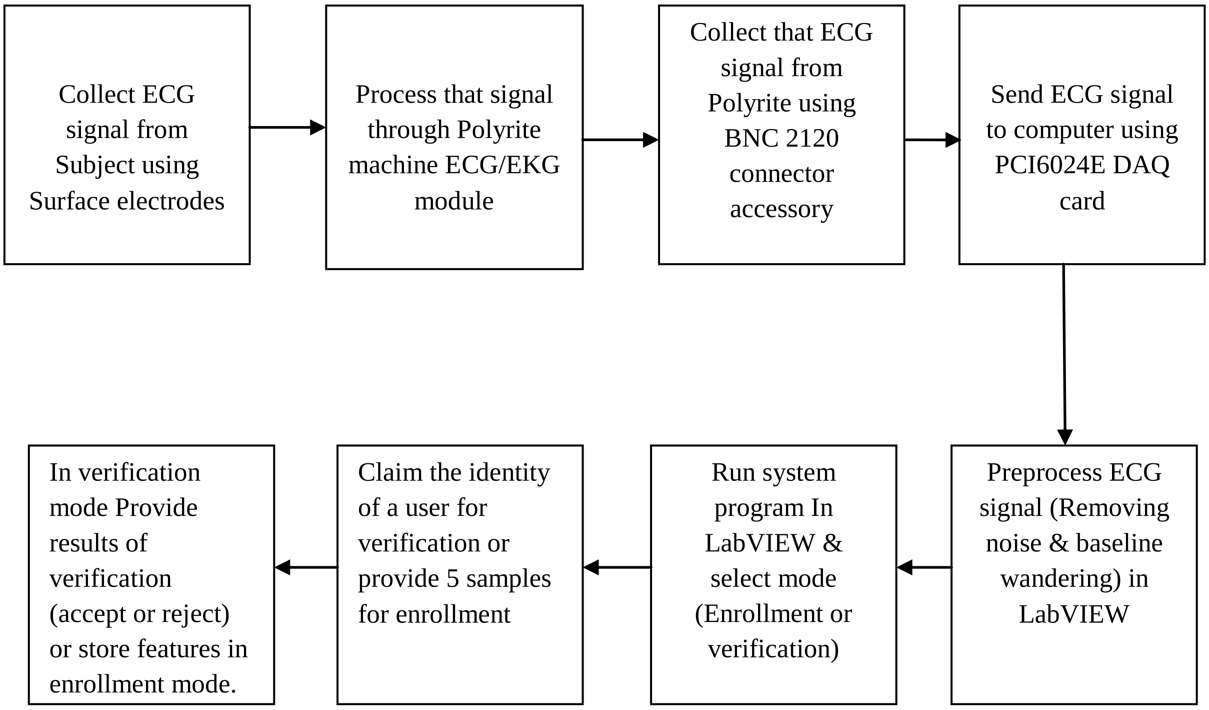


Figure 3.1 Block Diagram of ECG Based Biometrics Verification System

The block diagram an ECG Based Biometrics Verification System is shown in Figure 3.1. The person, who has previously enrolled in the system, presents an encrypted smart card containing his identification information. He then attempts to be authenticated by collecting ECG signal. This ECG signal processed through various stages for data Acquisition, filtering and baseline wandering removal. Prior to a verification session, users must enroll in the system (typically under supervised conditions). During this enrollment, ECG features are generated and stored for use in later verification sessions. There is also generally a tradeoff between recognition accuracy and the number of sample in enrollment-session.

This signal is analyzed by a verification system that makes the binary decision to accept or reject the user's identity claim.

3.2 Hardware requirements

The various hardware requirements for "ECG based biometric verification system" are.

1. Surface Electrodes with Connecting Leads
2. Polyrite machine
3. BNC 2120 connector accessory
4. PCI6024E DAQ card
5. P.C. with LabVIEW

3.2.1 Surface Electrodes with Connecting Leads

A surface electrode is a small device that is attached to the skin to measure or cause electrical activity in the tissue under it. The surface electrode including:

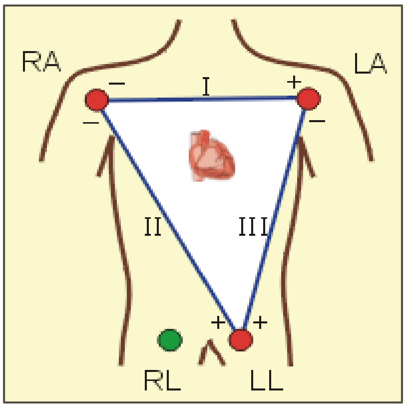
(a) A flexible, at least partially-conductive surface layer for physically contacting the skin surface, and for delivering electrical signal.

(b) An electrically conductive layer operatively connected to the partially-conductive surface layer, for transferring the electrical signal, wherein the at least partially-conductive surface layer has a thickness of less than 0.5 mm, and preferably contains a conductive gel or artificial skin.

These electrodes are connected with leads to collect the ECG signal.

3.2.1.1 3 Limb Leads (Bipolar)

In the normal electrode placement shown in figure 3.2, four electrodes are used to record the electrocardiogram; the electrode on the right leg is only for ground reference. Because the input of ECG recorder has only two input terminals, a selection must be made among the available active electrode. The bipolar limb lead selections first introduced by Einthoven are as follows:



Lead I: Left arm (LA) and Right Arm (RA)

Lead II: Left arm (LL) and Right Arm (RA)

Lead III: Left arm (LL) and Left arm (LA)

Figure 3.2 Electrodes Placement

These three leads are called Bipolar because for each lead the electrocardiogram is recorded from two electrodes and the third electrode is not connected. In each of this Lead position, The QRS of a normal heart is such that R wave is positive.

In working with electrocardiogram from these three basic limb leads, at any given instant of the cardiac cycle, the frontal plane representation of the electrical axis of the heart is two dimensional vector. Further, the ECG measured from any one of three basic limb leads is a time-variant single-dimensional component of that vector.

Whether the limb leads are attached to the end of the limb (wrists and ankles) or at the origin of the limb (shoulder or upper thigh) makes no difference in the recording because the limb can simply be viewed as a long wire conductor originating from a point on the trunk of the body.

3.2.1.2 3 Augmented Limb Leads (Unipolar)

In addition to the three bipolar limb leads described above, there are three augmented unipolar limb leads. These are termed unipolar leads because there is a single positive electrode that is referenced against a combination of the other limb electrodes. The positive electrodes for these augmented leads are located on the left arm (aV_L), the right arm (aV_R), and the left leg (aV_F). In practice, these are the same electrodes used for leads I, II and III. (The ECG machine does the actual switching and rearranging of the electrode designations). The three augmented unipolar leads, coupled with the three bipolar leads, constitute the six limb leads of the ECG. These leads record electrical activity along a single plane termed the frontal plane relative to the heart. Using the axial reference system and these six leads, it is simple to define the direction of an electrical vector at any given instant in time

3.2.2 PCI-6024E National Instruments Data Acquisition Card

National Instruments is one of the largest companies that provide electrical solutions. It is famous for providing data acquisition cards. Data acquisition cards are those cards that are used as interfaces between a plant and a computer in order to control the plant in real time environment. In the thesis the PCI-6024E DAQ card has been used. The 6024E features 16 channels of analog input, two channels of analog output, a 68-pin connector and eight lines of digital I/O. The PCI-6024E DAQ card uses the National Instruments DAQ-STC system timing controller for time-related functions. The DAQ-STC consists of three timing groups that control analog input, analog output, and general-purpose counter/timer functions. The three groups include a total of seven 24-bit and three 16-bit counters and a maximum timing resolution of 50 ns. The DAQ-STC makes possible such applications as buffered pulse generation, equivalent time sampling, and seamless changing of the sampling rate. In many DAQ systems, it is not easy to synchronize several measurement functions to a common trigger or timing event. Such devices have the Real-Time System Integration (RTSI) bus to solve this problem. In the PCI-6024E DAQ card, the RTSI bus consists of the National Instruments RTSI bus interface and a ribbon cable to route timing and trigger signals between several functions on as many as five DAQ devices in a computer.

In order to use the PCI-6024E DAQ card, it is required to have PCI interface and NI-DAQ 7.x drivers.

NI-DAQ maintains a consistent software interface so that one can change platforms with minimal modifications to the programming code. The user programmed application uses the NI-DAQ driver software, as illustrated in Figure 3.3

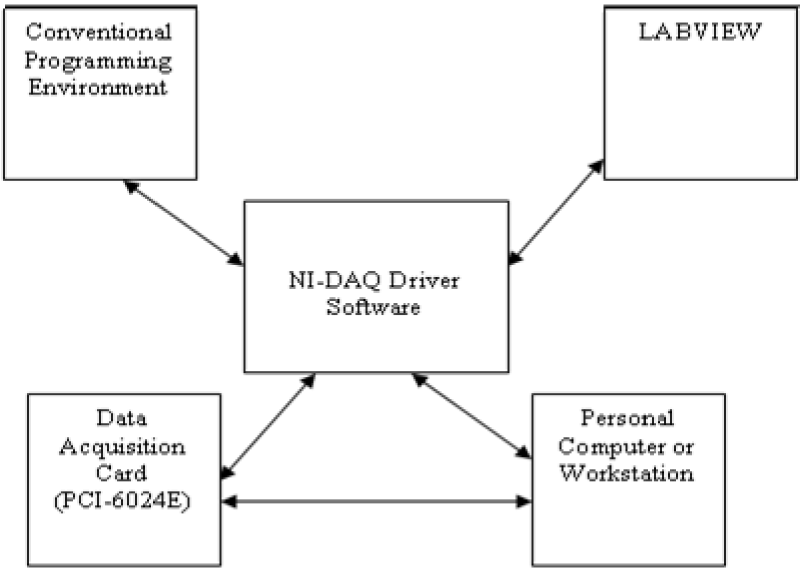


Figure 3.3 The relationship between the programming environment, NI-DAQ, and the PCI-6024E DAQ card

3.2.3 BNC-2120 Connector Accessory for Multifunction DAQ Devices

The BNC-2120 is a desktop or DIN rail-mountable accessory you can connect to E Series, S Series, and waveform generation Multifunction DAQ devices.

The BNC-2120 has the following features:

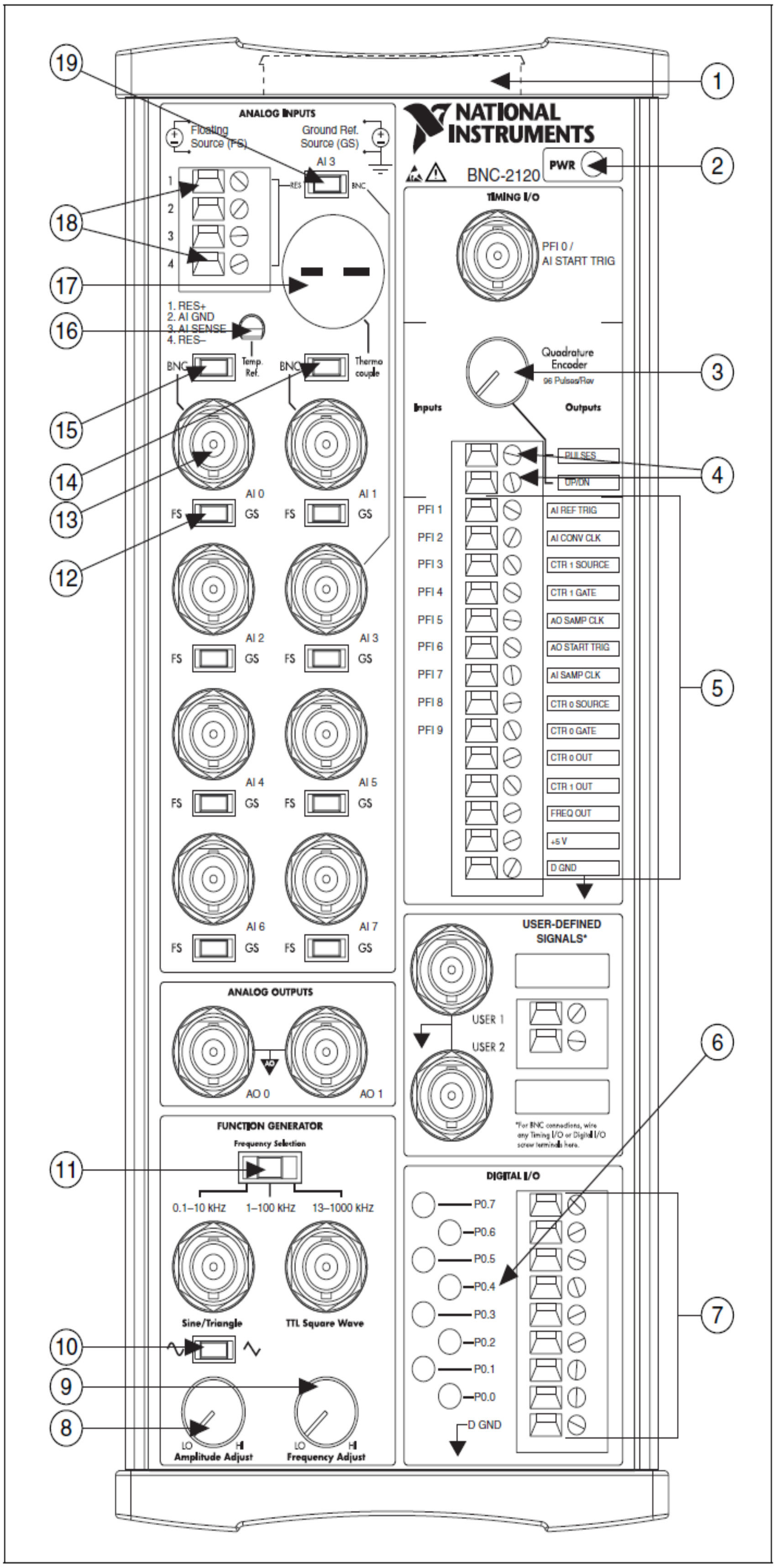
- Eight BNC connectors for analog input (AI) connection with the following optional features:
  - Thermocouple connector
  - Temperature reference
  - Resistor measurement screw terminals
- Two BNC connectors for analog output (AO) connection
- Screw terminals for digital input/output (DIO) connection with state indicators
- Screw terminals for Timing I/O connections
- Two user-defined BNC connectors
- A function generator with the following outputs:
  - Frequency-adjustable, TTL-compatible square wave
  - Frequency- and amplitude-adjustable sine wave or triangle wave
- Quadrature encoder

The BNC-2120 has a 68-pin input/output (I/O) connector that connects to your E Series, S Series, or waveform generation Multifunction DAQ device.

To set up and use BNC-2120 accessory, following are the requirements:

- BNC-2120 accessory
- BNC-2120 Installation Guide
- E Series, S Series, or waveform generation Multifunction DAQ device
- 68-position or 100-position cable
- BNC cables
- 24 AWG wire or smaller
- Wire strippers
- Flathead screwdriver (supplied)

The BNC-2120 has one 68-position connector on the rear panel to connect to DAQ device



1. 68-Position I/O Connector
2. Power Indicator LED
3. Quadrature Encoder Knob
4. Quadrature Encoder Output Screw Terminals
5. TIO Screw Terminals
6. DIO LED State Indicators
7. DIO Screw Terminals
8. Function Generator Amplitude Adjust Knob
9. Function Generator Frequency Adjust Knob
10. Sine/Triangle Waveform Selection Switch
11. Frequency Range Selection Switch
12. Floating Source (FS)/ Ground-Referenced Source (GS) Switch
13. BNC Connector
14. BNC/Thermocouple Selection Switch
15. BNC/Temperature Reference Selection Switch
16. Temperature Reference
17. Thermocouple Input Connector
18. Resistor Measurement Screw Terminals
19. Resistor/BNC Selection Switch

Figure 3.4 BNC 2120

3.2.4 Introduction of Polyrite

The POLYRITE Recorder is a highly sensitive oscillograph capable of simultaneously recording signals in different modes from many sources.

POLYRITE Recorders can be used by the medical profession for the recording of bioelectric potentials, in aerospace technology for recording telemetered information, in industry for recording of servo amplifier performance, all types of vibration pick-up and recording of temperature etc. The flexibility resulting out of modular construction of the POLYRITE allows a wide variety of physical phenomena to be recorded simultaneously.

The modular concept in construction allows the assembly to be custom tailored to exact performance requirements. Additional capabilities and functions can be added simply by acquiring the required amplifier modules appropriate transducers. Adaptation of the instrument for various uses merely requires the exchange of amplifiers and selection of suitable pick up devices. Widely diverse information can thus be recorded on a single instrument by the use of different amplifiers and appropriate transducers.

3.2.4.1 Basic Modules

Each separate record inscribed on the chart requires a separate channel, which consists of an amplifier and pen motor. The signal may be fed into the amplifier directly by the use of suitable electrodes or, if in the form of any energy other than electrical, it may be converted to electrical energy by the use of appropriate transducers and then fed into the amplifier. All modules are fully solid state and are designed using integrated circuits, high stability components and printed circuit boards. The technology used is true state-of-the art.

3.2.4.2 Amplifiers

The vertical pre-wired section houses the various amplifiers plug-in-modules and the power supply module. All interconnections between the amplifier channels and the recorder section channels are through pre-wired connectors. And the recorder section channels are through pre-wired connectors. Controls are kept to minimum at the same time ensuring a wide variety of adjustment.

Any number of channels can be selected as the polyrite is designed on a plug in modular system amplifier modules can be added subsequently depending upon requirements and resources.

The use of amplifier permits the widely different applications such as temperature measurements or the bioelectric potential measurement to be made with the same recording channel. A wide range of amplifiers is available to meet the most requirements; others are being constantly developed and designed to meet the specific applications.

3.2.4.3 Pen Motor

The heart of polyrite recording system, the pen motor is also designed in modular form and snaps into place in its receptacle. The pen motor is study and has smooth ball bearing movement.

The light weight ink writing capillary pens are 120mm effective length and have provision for fine adjustment of writing tension. Inkwells are placed in a composite receptacle and provided with pressure caps. A pen lift mechanism lifts all pens from the paper by manipulation of single lever.

Thus each pen motor consists of a stylus or pen that is immobilized by a torsion system mounted perpendicular to it. When a signal current from the amplifier flows through the coil the interaction of current and magnetic field rotates the coil against the torque of torsion system and causes a deflection in the stylus, which is proportional to the magnitude of the signal current. When the signal disappears the torsion system return the stylus system to its original position. When the stylus is in the contact with a moving charge, a fluctuating signal produces a continuous trace on which even minutes changes of signal amplitude can be readily detected.

3.2.4.4 Chart Drive

The chart drive is the unit, which moves the chart paper first and under the stylus of writing element. The polyrite ten speed chart drive gives precise paper speed by using a synchronous motor and a closed meshed gear system free from backlash.

3.2.4.5 Time and Event Channel

The time and event module is an optional accessory. This module permits double range time marking of 1 and 10 second (or 5 and 30 sec; or 10 sec and 1 minute). The event marker push button record the push button record the event by producing a 40 cycle wave for as long as the push button is depressed. This channel is also modular in construction and can be taken out by just unscrewing two thumb screws.

3.2.4.6 Circuit Analysis

The basic purpose of polyrite recorder is to amplify a very small signal and use it too cause a pen deflection that is proportional to the size of signal. It is translated into electrical signal by a transducer.

The very high CMRR of polyrite amplifier helps in eliminating 50 cycles interference, while at the same time not affecting the high frequency response of the amplifier.

3.2.4.7 Recorder Section

It refers to the complete horizontal assembly housing the chart drive mechanism and recording system.

3.2.4.8 Procedure

1) Connect the desired electrodes to the subject. Connect these to the input cable to the amplifier input connector
2) Turn the console MAINS ON
3) Turn the amplifier to STANDBY
4) In model 201 turn the ½ AMP HI FREQ. control to 75. The 35 and 15 positions may be used to eliminate high frequency artifacts. The 0.1, 0.5 etc. positions may be used for averaging
5) Turn 50 Hz FILTER OFF
6) Turn the INPUT switch to the time constant 1 for EKG, 0.03, for EMG, 0.1 or 0.3 EEG. In the Model 201 the DC position may be selected for recording DC Potentials. In this case use the BALANCE controls to nullify any offset

potentials

7) Calibrate the amplifier if needed
8) Select the desired position on the SENSITIVITY switch of the amplifier, when in don’t always select a lower SENSITIVITY and then increase later on if needed. Select 1 mV for EKG, 0.1 mV for EEG etc
9) Turn the USE CAL switch to USE
10) Adjust pen position as required, by rotating baseline control.
11) Set the chart speeds control on the console to the desired speed
12) Turn the amplifier ON
13) Turn the chart drive ON

3.2.5 PC

The speed of execution of verification system depends upon the computer in which the software is written. The minimum required clock and RAM for the system is that on which LabVIEW can run. The specifications of the used PC are 1.83 GHz clock frequency processor with 2.5 GB RAM.

3.2.6 Database

The database has been made by collecting ECG waveform of 20 individuals. 10 samples have been taken of each of them at different time for testing. Lead II (lead 3 bipolar) is selected for collecting data from the polyrite machine. In this way a database of 200 samples has been collected.

3.3 Software Platform

The software platform used by us was LabVIEW (Laboratory Virtual Instrument Engineering Workbench) 7.1.

3.3.1 LabVIEW

LabVIEW is a programming environment in which you create programs using a graphical notation (connecting functional nodes via wires through which data flows); in this regard, it differs from traditional programming languages like C, C++, or Java, in which you program with text. However, LabVIEW is much more than a programming language. It is an interactive program development and execution system designed for people, like scientists and engineers, who need to program as part of their jobs. The LabVIEW development environment works on computers running Windows, Mac OS X, or Linux. LabVIEW can create programs that run on those platforms, as well as Microsoft Pocket PC, Microsoft Windows CE, Palm OS, and a variety of embedded platforms, including Field Programmable Gate Arrays (FPGAs), Digital Signal Processors (DSPs), and microprocessors.

Using the very powerful graphical programming language that many LabVIEW users affectionately call "G" (for graphical), LabVIEW can increase your productivity by orders of magnitude. Programs that take weeks or months to write using conventional programming languages can be completed in hours using LabVIEW because it is specifically designed to take measurements, analyze data, and present results to the user. And because LabVIEW has such a versatile graphical user interface and is so easy to program with, it is also ideal for simulations, presentation of ideas, general programming, or even teaching basic programming concepts.

LabVIEW offers more flexibility than standard laboratory instruments because it is software-based.

LabVIEW also contains application-specific libraries of code for data acquisition (DAQ), General Purpose Interface Bus (GPIB), and serial instrument control, data analysis, data presentation, data storage, and communication over the Internet. The Analysis Library contains a multitude of useful functions, including signal generation; signal processing, filters, windows, statistics, regression, linear algebra, and array arithmetic.

3.3.2 How Does LabVIEW Work?

LabVIEW uses terminology, icons, and ideas familiar to scientists and engineers. It relies on graphical symbols rather than textual language to define a program's actions. Its execution is based on the principle of **dataflow**, in which functions execute only after receiving the necessary data. Because of these features, one can learn LabVIEW even if he/she has little or no programming experience. However, you will find that knowledge of programming fundamentals is very helpful.

A LabVIEW program consists of one or more **virtual instruments (VIs)**. Virtual instruments are called such because their appearance and operation often imitate actual physical instruments. However, behind the scenes, they are analogous to main programs, functions, and subroutines from popular programming languages like C or Basic. Hereafter, we will refer to a LabVIEW program as a "VI". Also, be aware that a LabVIEW program is always called a VI, whether its appearance or function relates to an actual instrument or not.

A VI has two main parts: a **front panel**, a **block diagram.**

- The **front panel** is the interactive user interface of a VI, so named because it simulates the front panel of a physical instrument (see Figure 3.5). The front panel can contain knobs, push buttons, graphs, and many other controls (which are user inputs) and indicators (which are program outputs). You can input data using a mouse and keyboard, and then view the results produced by your program on the screen.

- The **block diagram** is the VI's source code, constructed in LabVIEW's graphical programming language, (see Figure 3.6). The block diagram is the actual executable program. The components of a block diagram are lower-level VIs, built-in functions, constants, and program execution control structures. You draw wires to connect the appropriate objects together to define the flow of data between them. Front panel objects have corresponding terminals on the block diagram so data can pass from the user to the program and back to the user.

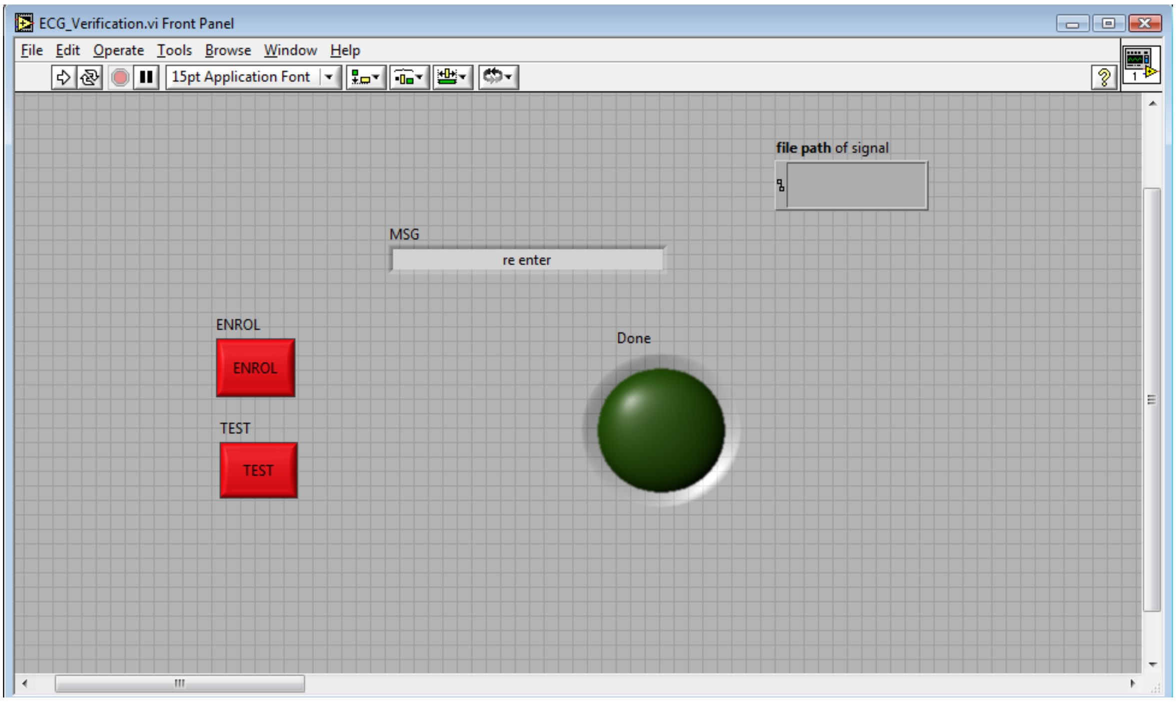


Figure 3.5 Front panel of ECG verification program.

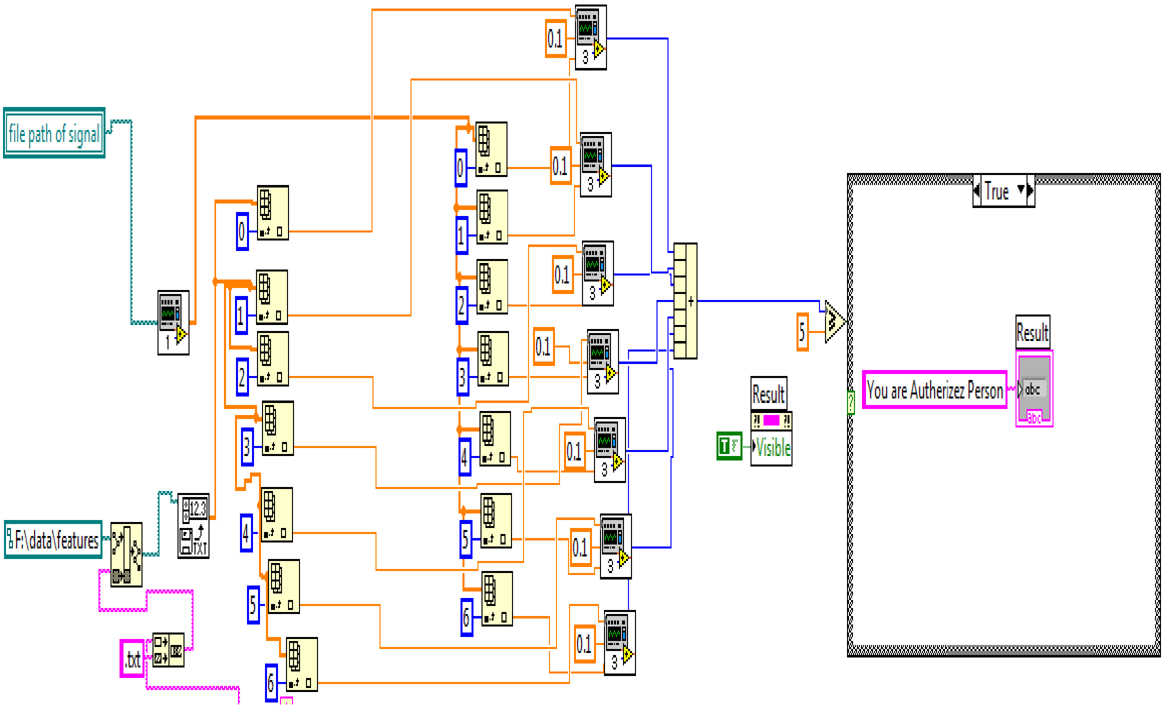


Figure 3.6 Block diagram of a VI

3.4 Software Implementation

LabVIEW software of ECG Verification includes two steps:

1) Enrollment
2) Testing

3.4.1 Enrollment

The various steps of enrollment are:

3.4.1.1 Enter the Name

The Enrollment does the registration of new user on to the system's user's database. Enrollment asks user's Name that is to be enrolled. After the person enters his name the system checks if the name previously exists in the database. If a match is found then the System prompts to enter the name again. This process is continued until the name has no match in the database.

3.4.1.2 Enter The Password

Enrolled user must have a password for access the system in future. The password has to save in user's database in enrollment process after registration of name.

3.4.1.3 Capturing the ECG signal

The system then asks for biometric signature i.e. ECG signal, of the user to be passed on to the system. The flow chart for capturing the ECG signal is shown in the figure 3.8 and various steps are given below

1) Configure the Input channel -: make a channel to measure the applied voltage on it, because ECG signal is a bio-potential, and can be measured in volts. The various steps for creating a channel are-:
    a. Open the measurement & automation software installed with LabVIEW base package.
    b. Go to Data Neighborhood option and select create new.
    c. Select virtual channel and set it's configuration

i. Select analog input
ii. Set channel name and description
iii. Select type of input(voltage)
iv. Select unit and max-min range of input
v. Select the option for scaling
vi. Select what DAQ hardware is used
vii. Select the channel on DAQ hardware
viii. Press finish button, channel is created.

2) Fix the electrodes at right place on the body of subject.
3) On the ECG/EKG module of the Polyrite machine. Set DC amplification. Select lead II bipolar for ECG recording.
4) Store data of 5 sec in text file.

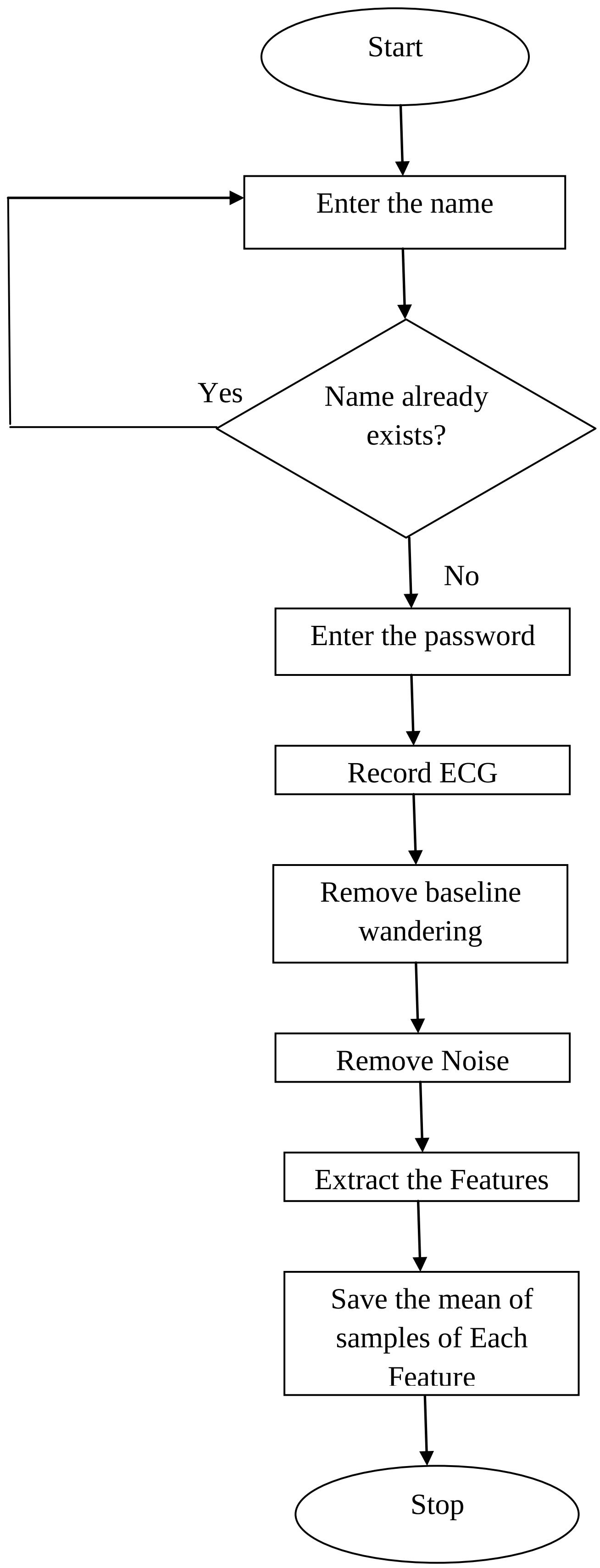


Figure 3.7 Flow Chart of Enrollment of a Person.

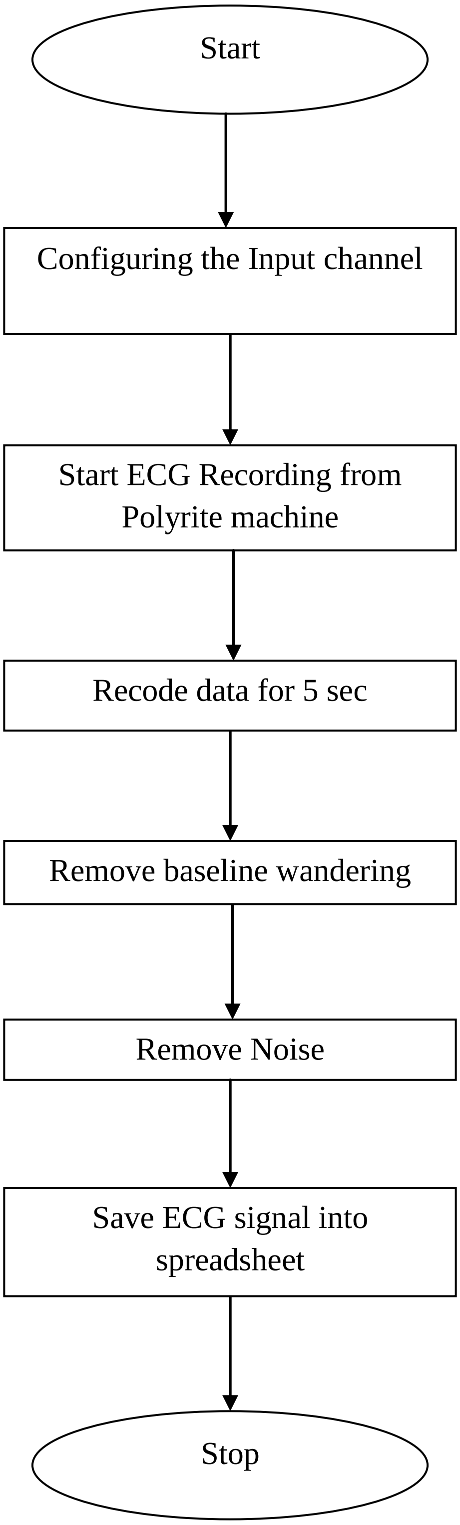


Figure 3.8 Flow Chart of Capturing the ECG Signal.

3.4.1.4 Removing Baseline Wandering

Baseline wandering usually comes from respiration at frequencies wandering between 0.15 and 0.3 Hz, and can be suppressed by a highpass digital filter. Also one can use the wavelet transform to remove baseline wandering by eliminating the trend of the ECG signal. Baseline wandering removal is necessary because without it features of the ECG wave cannot be extracted.

3.4.1.4.1 Digital Filter Approach

The LabVIEW DFDT (Digital Filter Design Toolkit) provides an intuitive and interactive way to design and implement finite impulse response (FIR) or infinite impulse response (IIR) filters easily and effectively. For example, one can use the Classical Filter Design Express VI to design a Kaiser Window FIR highpass filter to remove the baseline wandering. Figure 3.9 shows an example of the specifications of the highpass filter that is used to remove the baseline wandering and figure 3.10 shows block diagram of VI.

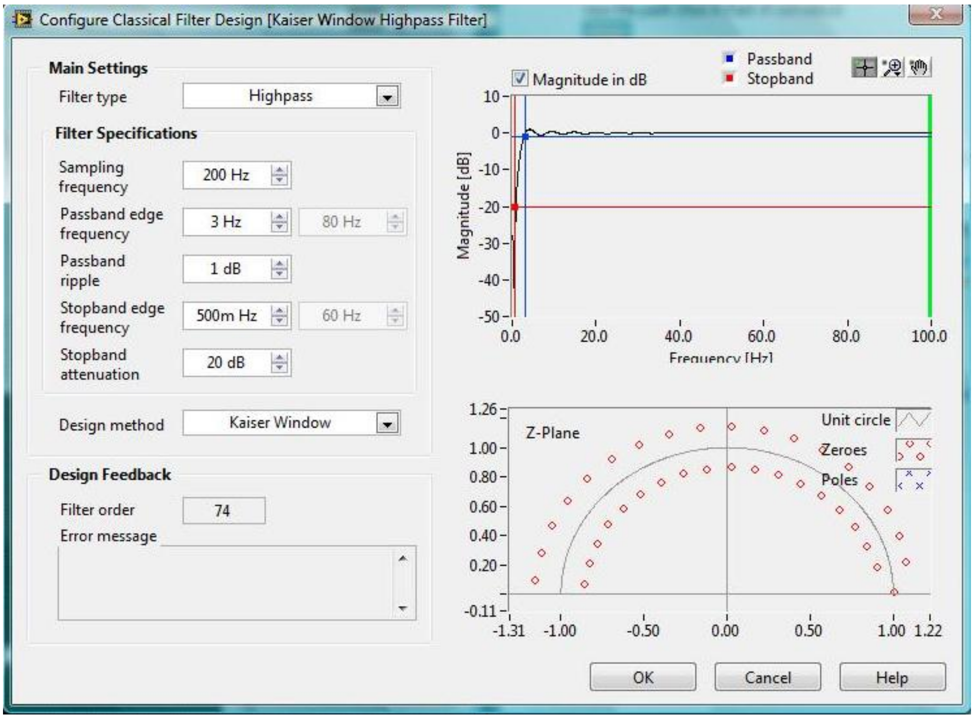


Figure 3.9 Kiser Window highpass filter

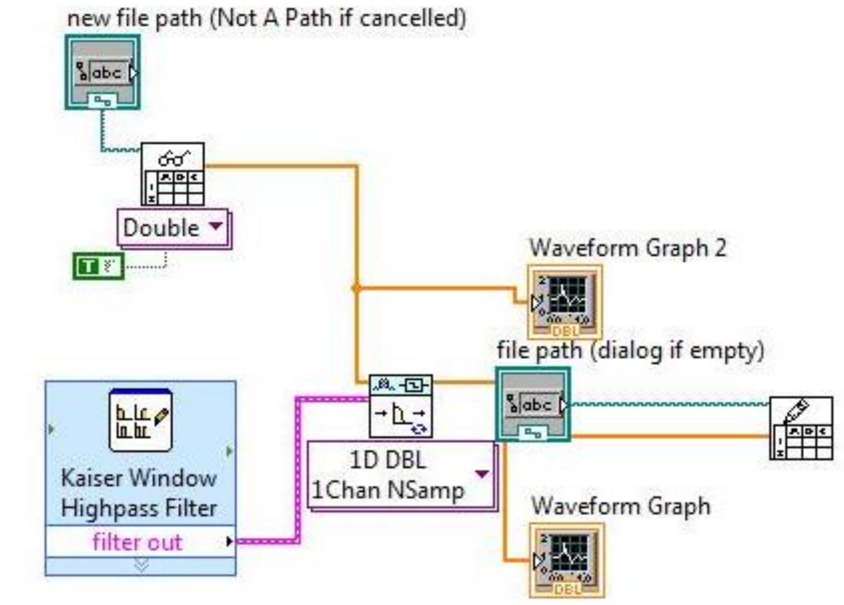


Figure 3.10 Block diagram for Baseline wandering removing VI.

3.4.1.5 Removing Wideband Noise

After remove baseline wandering, the resulting ECG signal is more stationary and explicit than the original signal. However, some other types of noise might still affect feature extraction of the ECG signal. The designed filter to remove these noises has three inputs and one output.

One input is the ECG signal that has to be filtered. Second input is sampling rate at which this signal is picked and the last input is Window cut off that decides how strongly filter will remove the glitches from the input signal. The output is filtered ECG signal. The block diagram of ECG filter VI is shown in the figure 3.11.

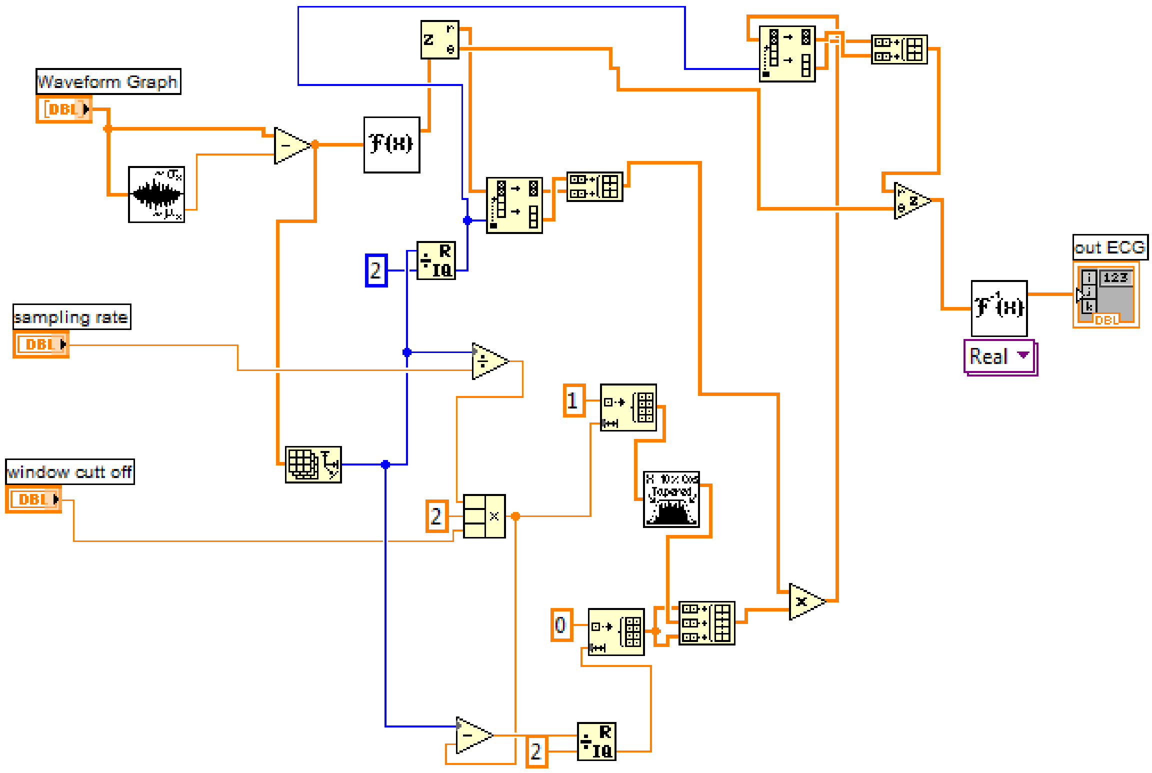
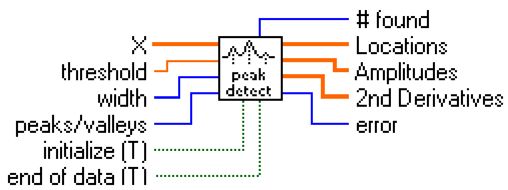


Figure 3.11 Filter for ECG signal

3.4.1.6 Extracting the Features

Features extraction is the next task after removing baseline wandering and noise from ECG signal. For this purpose Peak detector VI is used. This VI can detect peaks/valleys and their index from the applied signal. The flow diagram of features extracting process is shown in figure 3.13. The peak detector is discussed below.



X is the array of input values that represents the signal to be analyzed. The data can be a single array or consecutive blocks of data.

Threshold rejects peaks and valleys that are too small. For peaks, the VI ignores any peak found with a fitted amplitude that is less than threshold. The VI ignores valleys if the fitted trough is greater than threshold.

Peaks/valleys specify whether the VI looks for peaks (positive-going bumps) or valleys (negative-going bumps) in the input signal. The settings for this control are 0 (peaks) and 1 (valleys).

Locations contain the index locations of all peaks or valleys detected in the current block of data.

Amplitudes contain the amplitudes of peaks/valleys found in the current block of data.

3.4.1.7 Selected features for the system

It is observed that amplitude of P wave in ECG does not change with time. Similarly other amplitude features are changes on small scale. The internal features of ECG may vary if a person does any physical work and also changes with time (age). So selected features in this work are mostly amplitude feature, these are: PR amplitude, QR amplitude, RS amplitude, RT amplitude, RR interval, PS amplitude and TS amplitude. The selected features are shown in figure 3.12.

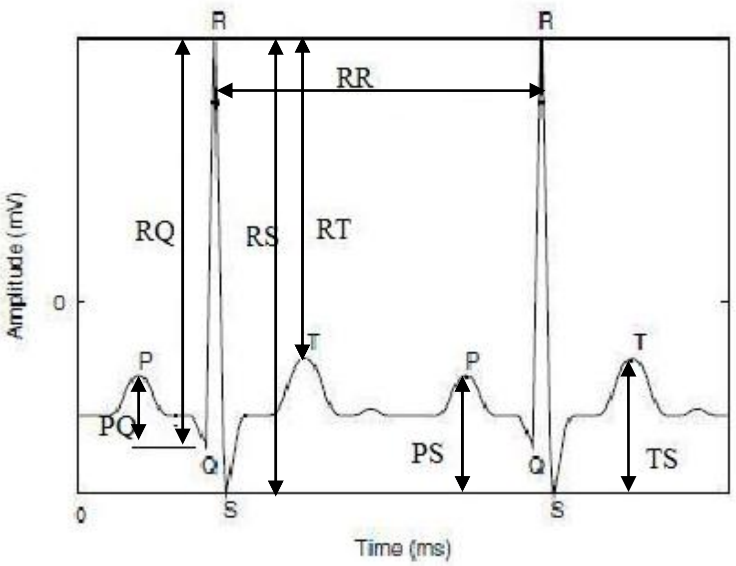


Figure 3.12 Selected Features from ECG

The features are calculated with the help of peak detector VI. Find out the largest peak in the wave record its amplitude and index, it is R peak. Calculate the relative index of two R peak, it is RR interval. Find out the peak before R peak it is P peak. Find out a valley between P and R peak, it is Q valley. Find out peak after R peak it is T peak and find out valley between R and T peak, it is s valley. Now all the features can be calculated with the help of these values.

After extracting features save them in the memory. Also take multiple readings in enrollment process so their mean can be calculated and used in verification process.

3.4.2 Testing

During testing the system, the system checks the claim of the person. The flow chart of testing the ECG signal is shown in figure 3.13. The various steps for testing are:

1) Entering of user name and the opening of data base.
2) Checking the correctness of name.
3) Enter the password.
4) Enter the ECG signal.
5) Extract the Features.
6) Count number of matched feature
7) Decision – Accept / Reject

3.4.2.1 Entering and Checking the correctness of name

First of all user enter his/her name and password, the system check name entered by the user is valid or not. If the name of the user matches with the enrolled user then the system proceeds further with the verification process, otherwise it stops giving a message: "You are not an enrolled user" and the testing ends. If the system finds a match then it opens the feature file corresponding to the user form the database.

3.4.2.2 Enter the ECG signal

Collect the ECG signal which is picked by surface electrodes and processed by polyrite machine using DAQ card. After it ECG signal is preprocessed by removing noise and baseline wandering.

3.4.2.3 Extract the Features

Extract the features from the ECG signal by the process discussed using peak detector VI and developed algorithm.

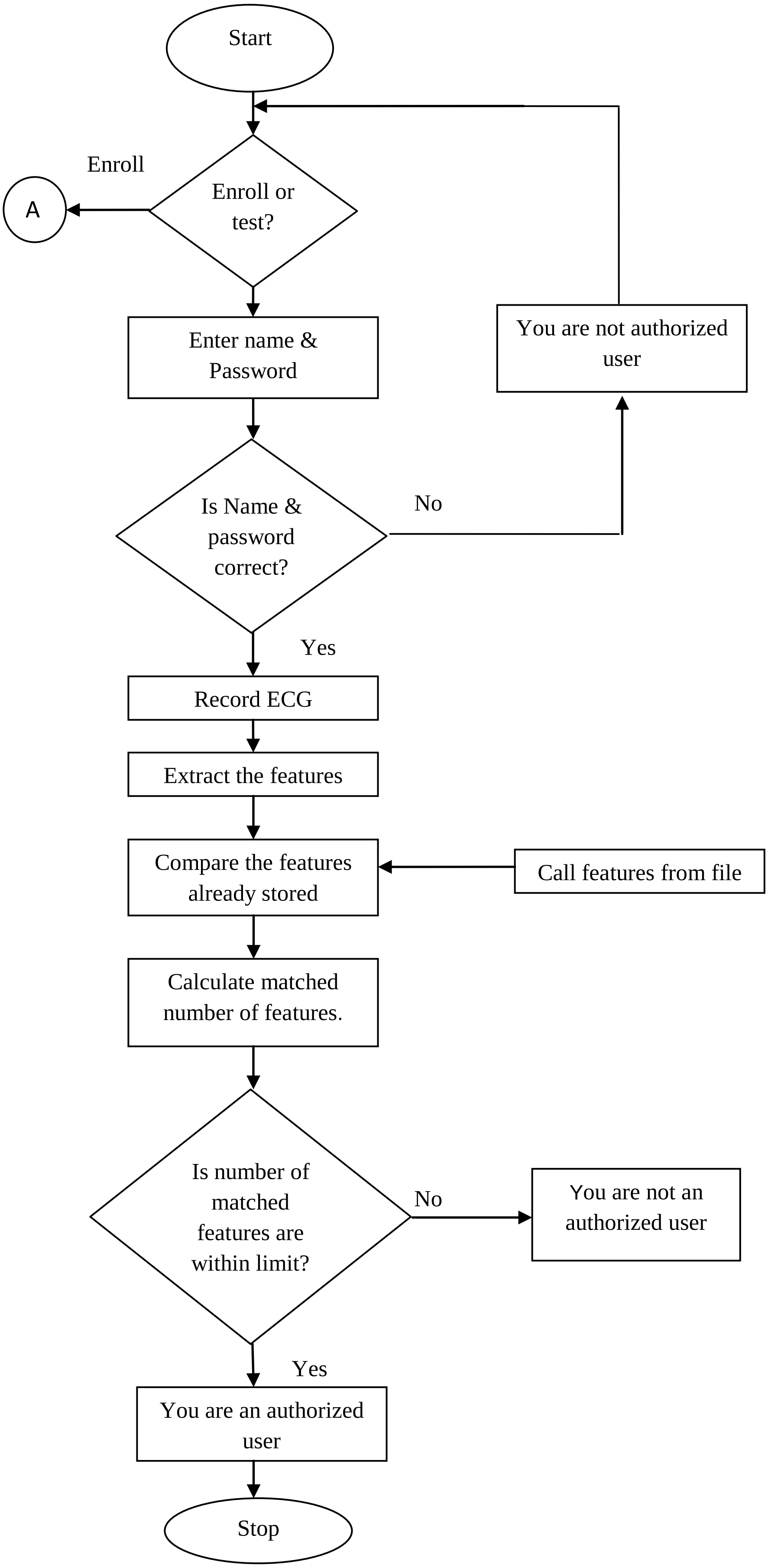


Figure 3.13 The Flow chart of the testing of a user weather he/she is authorized or not.

3.4.2.4 Count number of matched feature

Count the number of features laying in between ±10% of the stored reference mean of feature of subject during enrollment.

3.2.4.5 Decision – Accept / Reject

There are seven features selected in the algorithm. If five of them provide true result then accept the user and if it is less than five then reject him/her.

Chapter 4

Results and Discussion

4.1 Introduction

After performing various steps of the Verification System, the present algorithm's results are presented here. These experiments are performed on ECG data collected with the help of polyrite machine. Lead II bipolar ECG was recorded. And LabVIEW 7.1 was used for the program.

4.2 Enrollment

The first step in verification system is to enroll the user in the data base. The steps of user enrollment in the data base are given below.

- Press ENROL button. Shown in figure 4.1.

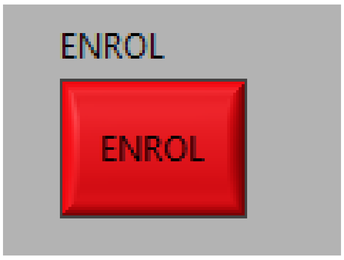


Figure 4.1 Enrollment button.

- Enter the Name as per direction of displayed message and then press done as shown in figure 4.2.

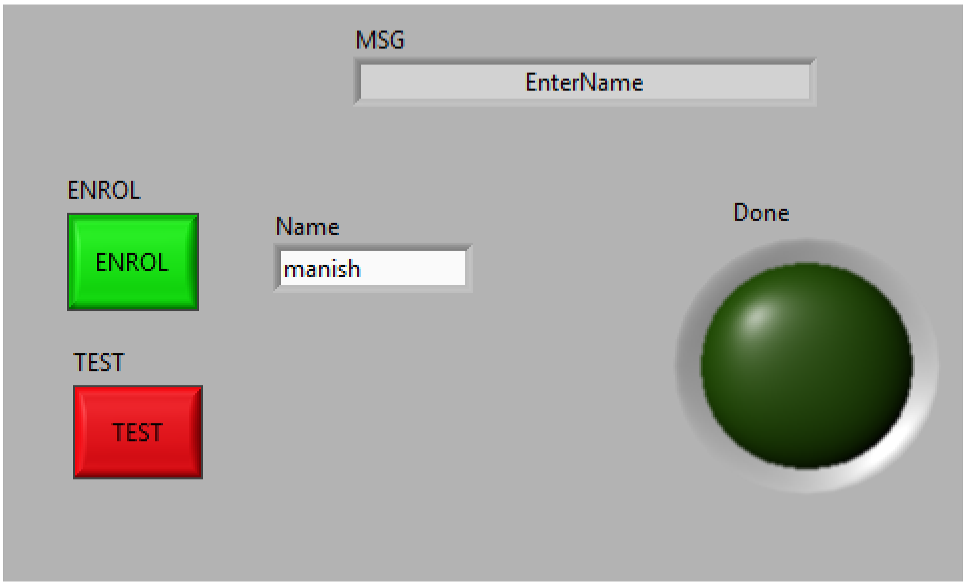


Figure 4.2 Figure showing name entering in Enrollment process

- Enter the password as per direction of displayed message.
- Enter the path of file from where ECG signal have to read for enrollment or record ECG form subject, it will take 5 ECG samples of ECG in enrollment process. This step is shown in figure 4.3.

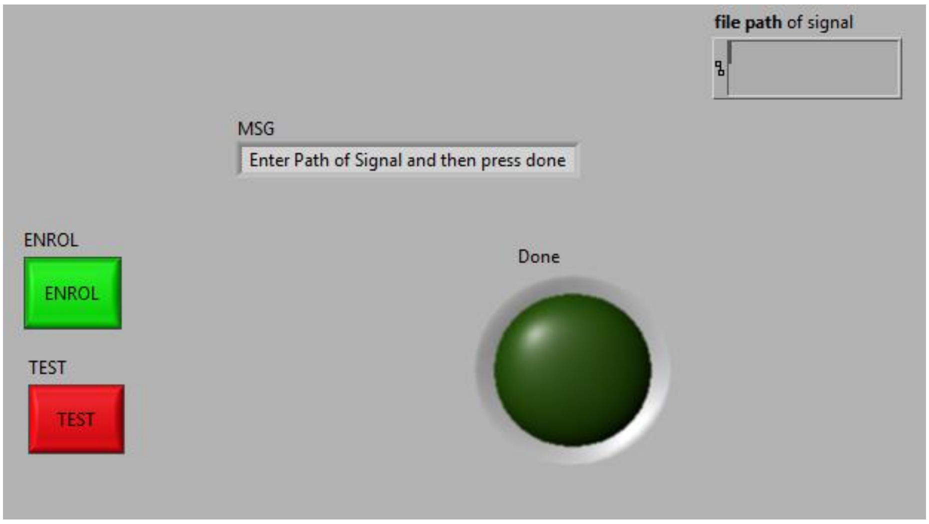


Figure 4.3 Figure showing acquiring ECG signal in Enrollment process

The ECG signal which is recoded in LabVIEW is shown in figure 4.4.

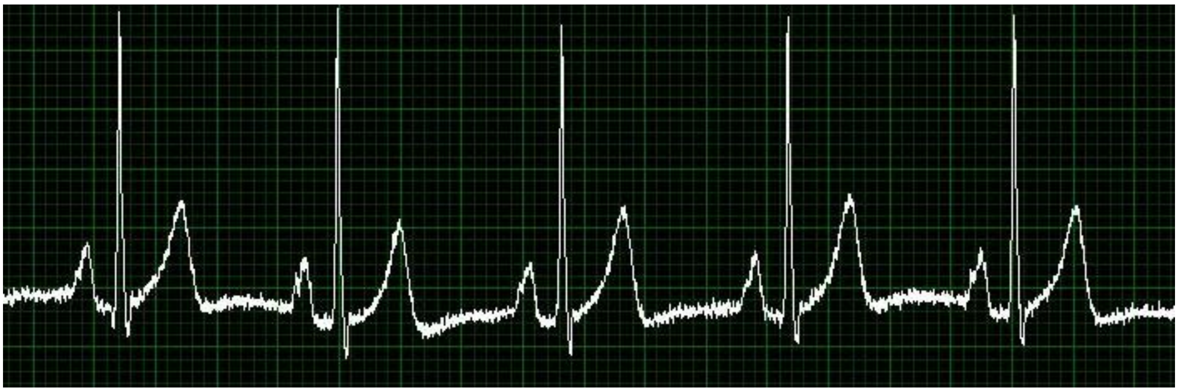


Figure: 4.4 Input ECG signals for Enrollment.

4.2.1 Baseline Wandering Removing

After ECG signal is recoded the first step is to remove baseline wandering. The waveform after the baseline wandering removal is shown in figure 4.5.

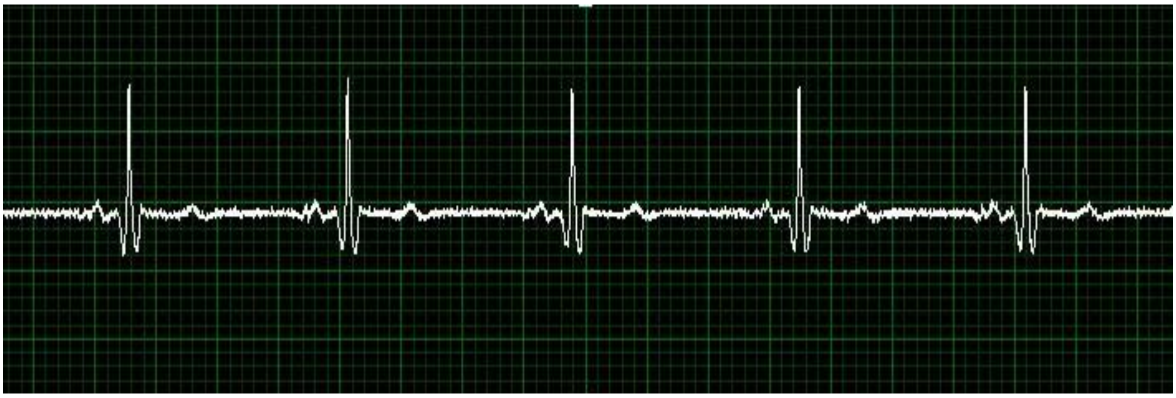


Figure 4.5 ECG signal after remove Baseline Wandering

4.2.2 Noise Removing

Noise is another problem after baseline wandering which can affect the feature extraction. So the filtration of ECG signal is necessary. Digital filtration is used in this approach. The figure 4.6 shows the ECG wave after filtration.

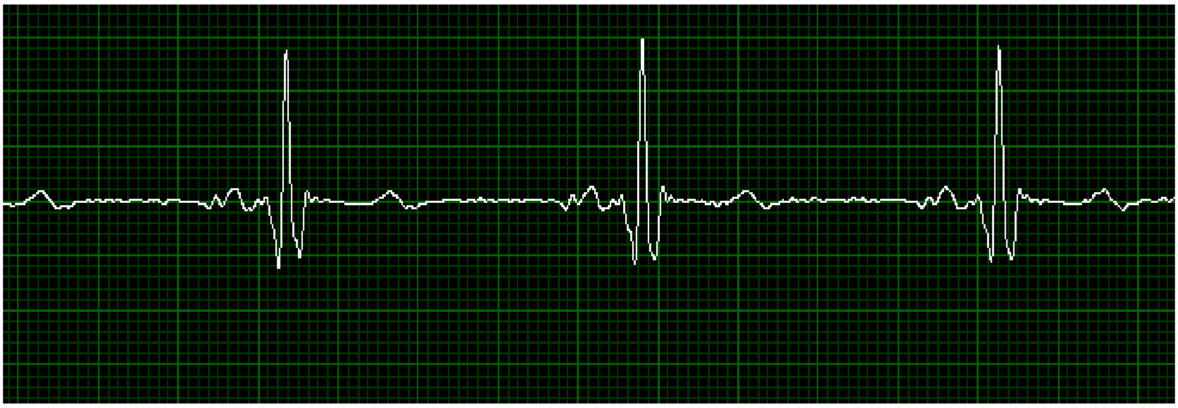


Figure 4.6 ECG wave after Filtration

4.2.3 Feature Extraction

Feature extraction is the important task in verification system. In enrollment process we take 5 samples from a particular subject extract feature from each signal, then take mean of these five reading and save this data in memory as features. The collected features of a specific person are shown in table 4.1.

Table 4.1 Different feature values of a person.

Attempts	Features						
	PR	QR	RS	RT	RR	PS	TS
1st	1.45168	2.21450	2.25158	1.43626	906.903	0.799900	0.815319
2nd	1.42349	2.09299	2.22510	1.37487	937.989	0.701606	0.850224
3rd	1.38091	2.04855	2.10333	1.32654	908.027	0.722423	0.776795
4th	1.32386	1.95430	2.01531	1.30656	931.096	0.691450	0.708755
5th	1.30184	1.91018	1.92221	1.27026	964.090	0.620367	0.651950

Mean of these features are shown in table 4.2

Table 4.2 Mean of selected features of a specific subject

	Features						
	PR	QR	RS	RT	RR	PS	TS
Means	1.35744	2.04539	2.02366	1.32184	920.174	0.666222	0.701816

These means are the true features which are stored in computer memory. Calculated values of features of all 20 subjects are shown in table 4.3

Table 4.3 Extracted Features of different subjects

Subject	Features						
	PR	QR	RS	RT	RR	PS	TS
Arpit	1.86317	3.34588	2.71037	1.8338	798.907	0.847203	0.876489
Gauri	2.32498	4.04857	3.44104	2.33037	701.577	1.11606	1.11066
Mohit	1.81446	2.86525	2.42702	1.78187	682.084	0.612563	0.64515
Sachin	1.28027	1.95856	2.04706	1.17829	703.183	0.766782	0.868763
Tiwari	2.10934	3.69789	3.1254	2.09417	791.458	1.01606	1.03123
Banga	1.39743	2.07143	1.89451	1.27138	1135.09	0.497089	0.62313
Ankit	1.45911	2.30484	1.88505	1.38883	691.137	0.42594	0.496224
Mishra	2.7531	4.38531	4.02811	2.77792	789.235	1.27501	1.25019
Manish	1.35744	2.04539	2.02366	1.32184	920.174	0.666222	0.701816
Mukesh	1.02837	1.47654	1.5948	1.02762	825.656	0.566434	0.567179
Ojha	1.78449	3.2143	3.07183	1.79239	932.19	1.28734	1.27944
Panday	1.71369	2.26694	2.88027	1.57601	718.303	1.16658	1.30426
Rahul	1.39975	1.94104	2.05747	1.33238	787.171	0.657727	0.72509
Rajive	1.7061	2.76527	2.62869	1.64658	871.155	0.92259	0.982109
Saini	1.0601	1.41805	2.44731	0.905261	923.083	1.38721	1.54205
Saurabh	1.50971	2.49336	2.12827	1.44788	782.072	0.618566	0.680394
solanky	1.48516	2.4208	2.22353	1.48078	787.528	0.738375	0.742754
Vishnoi	1.24325	2.24022	1.78881	1.21024	812.367	0.545561	0.578571
Vivek	1.90889	3.03207	2.84017	1.93515	822.969	0.931281	0.905027
Yatendra	1.4182	2.24748	2.222	1.25683	768.693	0.803807	0.965172

4.3 Testing

Testing is done by comparing the stored features with the new one. If the coming feature is laying in between ±10% of the stored reference mean of feature of subject then it is assumed true. The testing follows these steps.

- Press test button for verification. As shown in figure 4.7

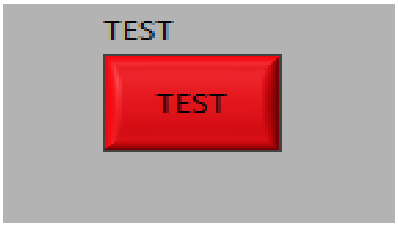


Figure 4.7 Test button.

- Enter Name & password of the person as shown in figure 4.8 and then press Done

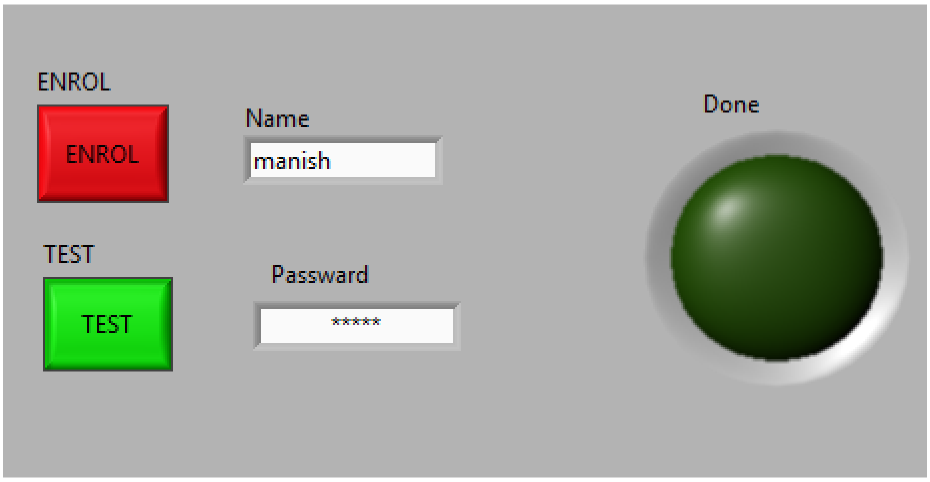
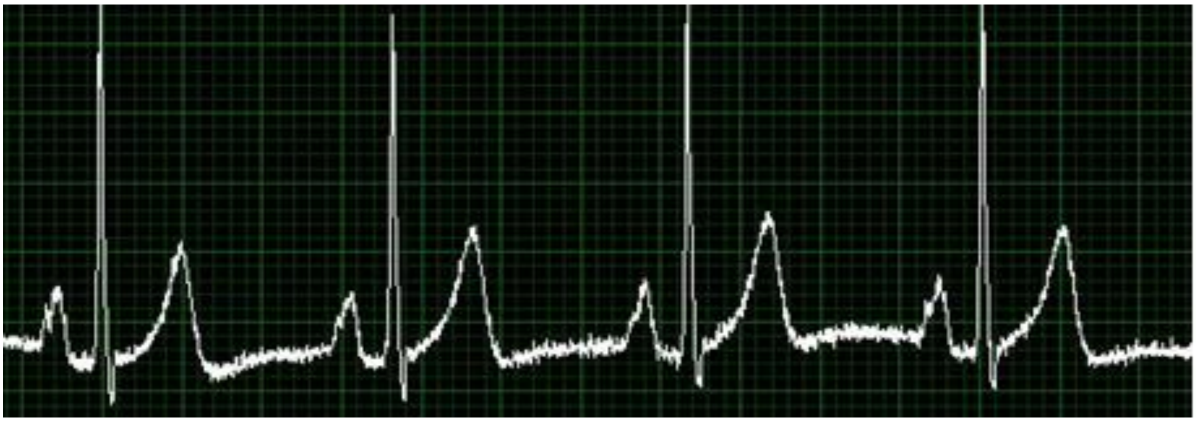
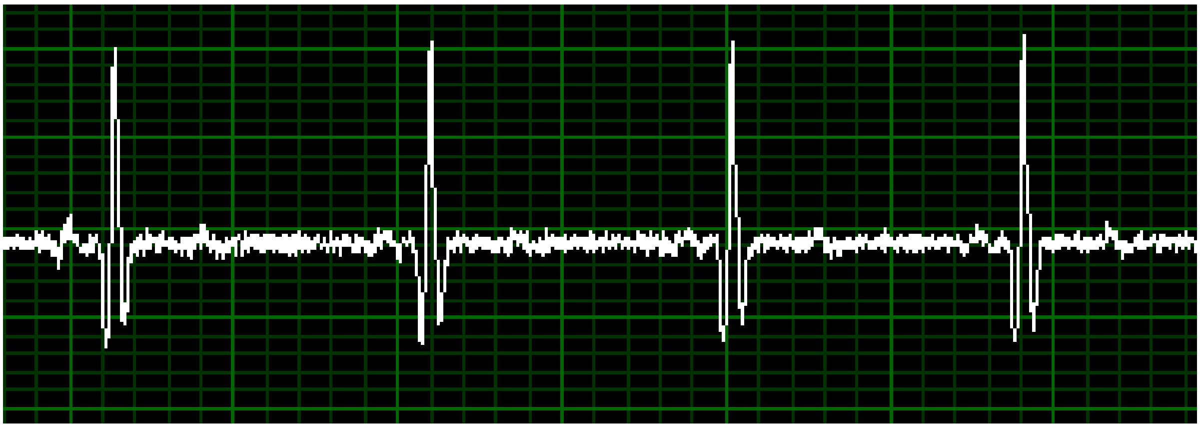


Figure 4.8 Front panel of entering name and password in verification process.

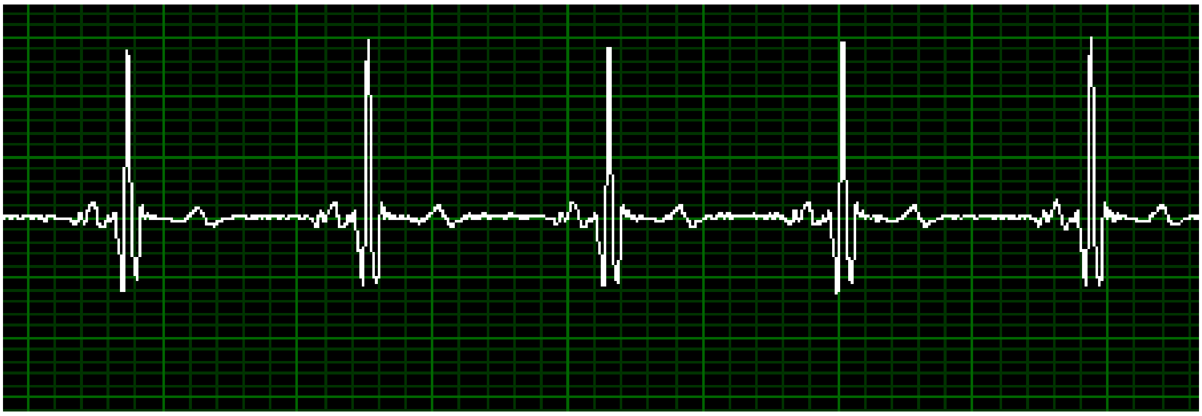
- Check weather Name exists and password are correct.
- Enter ECG, Preprocessed the signal the figure 4.9 (A) shows ECG signal for verification, figure 4.9 (B) shows ECG signal after baseline wandering removal and figure 4.9 (C) shows ECG signal after filtration.



(A)



(B)



(C)

Figure 4.9 ECG signal at different stages of verification. (A) Input signal, (B) ECG signal after baseline wandering removal, (C) ECG signal after noise removal.

- Extract Features. The extracted features of the ECG are shown in table 4.4.

Table 4.4 Features calculated in Verification.

Features						
PR	QR	RS	RT	RR	PS	TS
1.32892	2.05568	1.95435	1.31306	890.617	0.625424	0.641282

- Open file of stored features, the stored features are shown in table 4.5

Table 4.5 Features retrieved from computer memory.

Features						
PR	QR	RS	RT	RR	PS	TS
1.35744	2.04539	2.02366	1.32184	920.174	0.666222	0.701816

- Calculate the True result of features after comparison. All the features received in verification process are in the range of ±10% of features stored in computer memory in the above case 7 out of 7 features are matched.
- The person will be accepted if at least 5 out of 7 features are matched. In the above case the person is verified manish (as per the claim).

4.4 Result of Verification

The result of verification process of all individual has been shown in table 4.6. Here result of each individual is shown, they were verified in different cases. The presented value is number of matching of given person to the selected person out of 10 times. In red color the number of matching of individual is presented by own self. The values of presented in black color is shows the number of matching of individuals with others. The values presented in green color shows numbers of false accept.

Table 4.6 The result of verification process

	Arpit	Gauri	Mohit	Sachin	Tiwari	Banga	Ankit	Mishra	Manish	Mukesh	Ojha	Panday	Rahul	Rajive	Saini	Saurabh	solanky	Vishnoi	Vivek	Yatendra
Arpit	10	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	3	0
Gauri	0	9	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mohit	0	0	10	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
Sachin	0	0	0	10	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	2
Tiwari	0	2	0	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0
Banga	0	0	0	0	0	10	0	0	5	0	0	0	0	0	0	0	0	1	0	0
Ankit	0	0	0	0	0	4	9	0	0	0	0	0	0	0	0	0	0	2	0	0
Mishra	0	1	0	0	0	0	0	10	0	0	0	0	0	0	0	0	0	0	0	0
Manish	0	0	0	1	0	3	0	0	9	0	0	0	4	0	0	4	4	1	0	1
Mukesh	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0	0	0	1	0	0
Ojha	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0	0	0	0	0
Panday	0	0	0	0	0	0	0	0	0	0	1	9	0	0	0	0	0	0	0	0
Rahul	4	0	0	3	0	3	0	0	3	0	0	0	10	0	0	4	4	0	0	0
Rajive	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0	4	0
Saini	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0
Saurabh	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	10	3	1	0	4
Solanky	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	3	10	0	0	5
Vishnoi	0	0	0	0	0	4	0	0	1	0	0	0	0	0	0	0	0	9	0	0
Vivek	4	0	0	0	2	0	0	0	2	0	2	0	0	2	0	0	0	0	10	0
Yatendra	0	0	0	4	0	0	0	0	0	0	0	0	2	0	0	1	1	0	0	9

The experiment conducted on the collected database in the laboratory of 20 persons of different age having 10 samples each person. From the above table it is concluded that

1. 122 false verifications are accepted out of 3800. So its FAR is3.21%.
2. 6 true verifications are rejected out of 200. So its FRR is 3%.
3. Obtain an accuracy of 97%.

Chapter 5

Conclusion and Future Scope

5.1 Conclusion

The work discussed here "ECG based biometric verification system using LabVIEW" is a part of biometrics security system. The aim of this work was develop a biometric system, which can to detect the liveness of the subject so that someone cannot copy it. It enhances the security of the system and also provides the way for research in this field.

The system was implemented on LabVIEW 7.1. After collection ECG signal, it was preprocessed to remove noise and baseline wandering. Then it is used of extracting features. In enrollment we take 5 samples of each subject so that mean of their features can be calculated. These features are stored in the memory for future verification process. In verification again repeat the process till feature extraction. After it is compared with the stored file for that subject and provide the decision that user is right or wrong. The experiment conducted on the collected database in the laboratory of 20 persons of different age having 10 samples each reveals that accuracy of 97% can be achieved with the proposed algorithm.

5.2 Future Scope

ECG based biometrics verification system using LabVIEW is an efficient program. It provides 97% accuracy. Still there are chance to improve the system.

1. In this work the ECG signal was collected through chest leads, it can be collected through chest leads in order to enhance accuracy.
2. Wavelet transform approach may be used in order to remove baseline wandering.

References

1. James L. Wayman in Biometrics-Now and Then: “The Development of Biometrics Over the Last 40 Years”. New York Times article:
2. James L.Wayman, “Fundamentals of Biometric Authentication Technologies”. National Biometric Test Center.
3. Joseph Atick, From “The Science and Technology of Biometrics and Managing Human Identity”.
4. Biometric Technology Application Manual Volume One: Biometric Basics Compiled and Published by: National Biometric Security Project
5. D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, A. K. Jain, “FVC2002: Fingerprint Verification Competition,” Proc. Int. Conf. Pattern Recognition (ICPR), Quebec City, QC, Canada, , pp.744-747, Aug.2002.
6. J. Daugman, “How Iris Recognition Works”, IEEE Transaction on Circuits and Systems for Video Technology, Vol.14, no.1, pp.21-30, Jan.2004.
7. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, “Handbook of Fingerprint”, Springer, New York. 2003.
8. A.K. Jain, A. Ross and S. Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video Based Biometrics, vol.14, no.1, pp.4-20, Jan.2004.
9. S. Liu and M. Silverman, “A Practical Guide to Biometric Security Technology,” IEEE Journal on IT Professional, vol.3, no.1, pp.27-32, Jan.-Feb. 2001.
10. Ronald M. Birse, rev. Patricia E. Knowlden Oxford Dictionary of National Biography 2004
11. Burdon Sanderson J "Experimental results relating to the rhythmical and excitatory motions of the ventricle of the frog heart". Proc Roy Soc Lond 27: 410–14. 1878.
12. Waller AD, J Physiol Lond "A demonstration on man of electromotive changes accompanying the heart's beat". 8: 229–34. 1887.

13. Einthoven W. "Un nouveau galvanometre." Arch Neerl Sc Ex Nat; 6:625, 1901
14. L. Biel, O. Pettersson, L. Philipson, P. Wide, "ECG Analysis: A New Approach in Human Identification", IEEE Trans Instrum Meas, vol. 50, pp. 808-812, 2001.
15. J. M. Irvine, B. K. Wiederhold, L. W. Gavshon, S. Israel, S. B. McGehee, R. Meyer, M. D. Wiederhold, "Heart rate variability: A new biometric for human identification", Proc Intl Conf Artif Intell, pp. 1106-1111, 2001.
16. S. A. Israel, W. T. Scruggs, W. J. Worck, J. M. Irvine, "Fusing Face and ECG for Person Identification", Proc IEEE App Imag Paternt Recogn Workshop, pp. 226, 2003.
17. M. Kyoso, A. Uchiyama, "Development of an ECG identification system", Proc IEEE EMBS Conf, vol. 4, pp. 3721-3723, 2001.
18. M. Kyoso "A technique for avoiding false acceptance in ECG identification", Proc IEEE EMBS Asian-Pacific Conf on Biomedical Engineering, pp. 190-191, 2003.
19. T. W. Shen, W. J. Tompkins, Y. H. Hu, "One-Lead ECG for Identity Verification", Proc IEEE EMBS/BMES Conf, pp 62-63, 2002.
20. A. D. C. Chan, M. H. Hamdy, A. Badre, V. Badee, "Wavelet distance measure for person identification using electrocardiograms," submitted to IEEE Trans Instrum Meas, 2005.
21. V. Matyas Jr., Z. Riha, "Toward reliable user authentication through biometrics", IEEE Security & Privacy Magazine, vol. 1, pp. 45-49, 2003.
22. T. Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned", Fourth Working Conf. Smart Card Research and Adv. App., pp. 289-303. 2000.
23. Yogendra Narain Singh and Phalguni Gupta, "ECG to Individual Identification".
24. F. D. David, "The Normal ECG in Childhood and Adolescence", Heart, vol. 91, 2005, pp. 1626-1630.
25. H.H.P. Silva, H.F.S. Gamboa, A.L.N. Fred "Applicability of Lead V2 ECG Measurements in Biometrics".
26. D. Hatzinakos, (dimitris@comm.utoronto.ca), K. Plataniotis, "ECG recognition and classification".
27. Shen, T., Tompkins, W.: "Biometric statistical study of one-lead ECG features and body mass index (BMI)". In: Engineering in Medicine and Biology Society. 27th Annual International Conference pp. 1162–1165. 2005

28. Wang, Y., Plataniotis, K.N., Hatzinakos, D.: “Integrating analytic and appearance attributes for human identification from ECG signal. In: Proceedings of Biometrics Symposiums (BSYM)”, Baltimore, September 2006