ECG-Based Authentication

17

Fahim Sufi, Ibrahim Khalil, and Jiankun Hu

Contents

A biometric system performs template matching of acquired biometric data against template biometric data [17.1]. These biometric data can be acquired from several sources like deoxyribonucleic acid (DNA), ear, face, facial thermogram, fingerprints, gait, hand geometry, hand veins, iris, keystroke, odor, palm print, retina, signature, voice, etc. According to previous research, DNA, iris and odor provide high measurement for biometric identifiers including universalities, distinctiveness and performance [17.1]. DNA provides a one dimensional ultimate unique code for accurate identification for a person, except for the case of identical twins. In biological terms "Central Dogma" refers to the basic concept that, in nature, genetic information generally flows from the DNA to RNA (ribonucleic acid) to protein. Eventually protein is responsible for the uniqueness provided by other biometric data (finger print, iris, face, retina, etc.). Therefore, it can be inferred that the uniqueness provided by the existing biometric entities is inherited from the uniqueness of DNA. It is imperative to note that shape of the hand or palm print or face or even the shape of particular organs like the heart has distinctive features
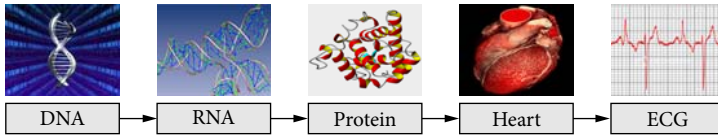
Fig. 17.1 Inheritance Model of ECG biometric from DNA biometric

which can be useful for successful identification. The composition, mechanism and electrical activity of the human heart inherit uniqueness from the individuality of DNA. An electrocardiogram (ECG) represents the electrical activities of the heart. Figure 17.1 shows the inheritance of uniqueness for ECG inherited from the DNA.

However, we can not infer this inheritance logic to be true for all the biometric entities especially for the case of identical twins, where the DNAs are identical. Nevertheless most of biometrics have demonstrated such uniqueness.

Biometrics has been a topic of research for the last 2 decades [17.2–16]. Biometric data can be acquired from several sources like DNA, ear, face, facial thermogram, fingerprints, gait, hand geometry, hand veins, iris, keystroke, odor, palm print, retina, signature, voice, etc. In recent years, fingerprints and iris have been most pervasively used in biometric authentications. Chan et al. [17.3] has already shown that person identification from ECG acquired from a finger is possible. Apart from reinforcing a stronger authentication technique by being a part of multimodal authentication, ECG can also be used as a stand alone biometric authentication system [17.2–16]. ECG is an emerging biometric security mechanism. It is yet to establish a system level framework as a new knowledge base. This chapter attempts to address this issue. This chapter is based on many publication materials including our previous work on this topic. It also intends to provide a comprehensive reference that is suitable both for the academic research and textbook for senior undergraduate and postgraduate studying in the computer security courses. The remaining of this chapter is organized as following. In Sect. 17.1, background knowledge of ECG is introduced. Section 17.2, provides a short review for ECG based biometric. Gradually, a more detailed classification of existing techniques in ECG based biometric is drawn on Sect. 17.3. A comprehensive comparison of existing ECG biometric is detailed in Sect. 17.4. In Sect. 17.5 some of the open issues in ECG based biometric are discussed. These issues are of particu-

lar importance to the researchers currently endeavoring for a better mechanism for ECG based human identification. Section 17.7 discusses application of ECG based biometrics to security. Conclusions are given in Sect. 17.8.

17.1 Background of ECG

ECG based biometric is a recent topic for research. As shown in [17.4, 5, 8], Inter Pulse Interval (IPI) or Heart Rate Variability (HRV) can be efficiently used to identify individuals serving the purpose of a biometric entity. IPI or HRV can easily be obtained from ECG signals. Unlike many biometric entities (like finger print, palm print, iris), ECG based biometric is suitable across a wider community of people including amputees. Therefore, people without hands can be successfully identified by existing ECG based biometric, even though he might be missing his finger. Reference [17.4, 5] successfully shows that IPI (heart signal) can be collected from literally any part of the body (e.g., finger, toe, chest, wrist). Using these principles, a researcher has enforced security within a body area network (BAN) comprising of multiple sensor nodes. Apart from this obvious advantage of versatile acquisition from an individual, ECG based biometric has other benefits like lower template size, minimal computational requirement, etc. [17.17, 18].

The ECG is the graphical record of the electrical impulses of the heart. Electrical activity of the heart is represented by the ECG signal. A scientist from The Netherlands, Willem Einthoven, first assigned different letters to different deflections of the ECG wave. This ECG signature is represented by PQRST, as seen in Fig. 17.2.

17.1.1 Physiology of ECG

The human heart contains four chambers: left atrium, right atrium, left ventricle and right ventricle [17.19]. Blood enters the heart through two large veins, the inferior and superior vena cava, emptying
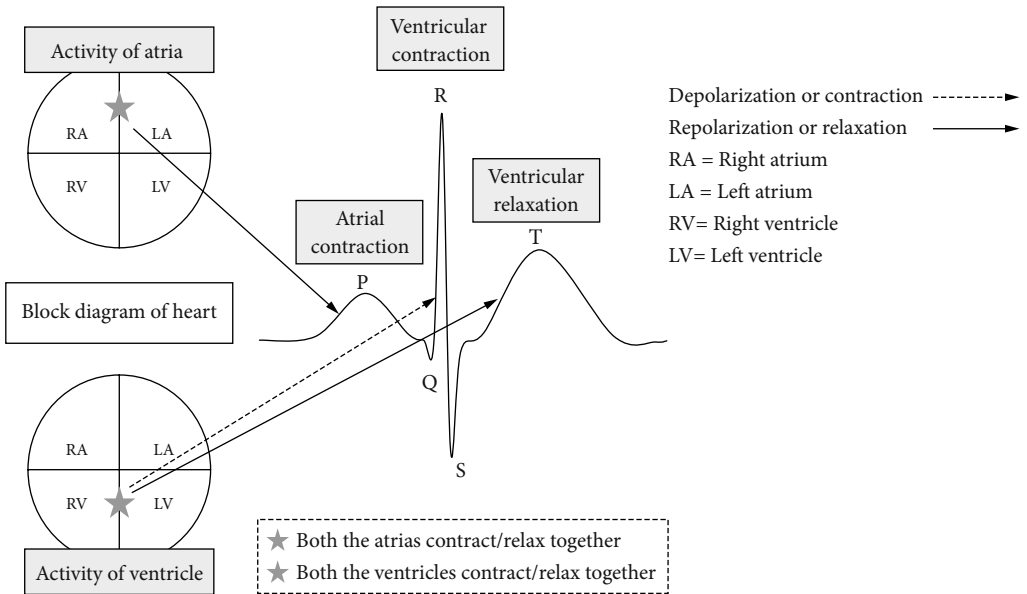
Fig. 17.2 Generation of an ECG from electrical activities of the heart

oxygen-poor blood from the body into the right atrium. From the right atrium, the oxygen deficient blood enters the right ventricle. The right ventricle then pushes the blood into the lungs. Inside the lungs a process called 'gas exchange' occurs and the blood replenishes oxygen supply. The oxygen rich blood then enters left atria. From the left atria, blood rushes into the left ventricle. Finally, it is the left ventricle that forces the oxygenated blood to the rest of the body.

This mechanical activity of the human heart is powered by electrical stimulations inside the heart. Depolarization (electrical activity) of a specific portion of the heart (either atria or ventricle) results in mechanical contraction of that specific part. Again, repolarization results in the mechanical relaxation of the heart chambers. ECG acquisition devices basically pick up these electrical activities via sensors attached to the human skin and draws the electrical activities in millivolt ranges.

During the regular activity of the heart, both the atria contract together, followed by ventricular contraction (both the ventricles contract together). As seen in Fig. 17.2, atrial depolarization (electrical activity), which is caused by atrial contraction (mechanical), is traced as P waves from the ECG trace [17.19]. Likewise, ventricular depolarization

(electrical) or ventricular contraction (mechanical) is represented by the QRS complex [17.19]. Since, during the ventricular contraction, the heart pushes the blood to the rest of the body, the QRS complex appears to be more vigorous compared to the rather mild P wave [17.19]. After the contraction of the ventricles, both the ventricles return back to the relaxed position (caused by ventricular repolarization). This ventricular repolarization (electrical) or relaxation (mechanical) is identified by T waves. Atrial repolarization or relaxation is thought to be buried under the more vigorous QRS complex.

Physicians and cardiovascular experts can map an individual's ECG with his heart condition. To ascertain a patient's heart condition, doctors mainly rely on several criteria of the ECG feature waves that basically include P wave, QRS complex and T wave [17.19]. These features will be described in following sections.

Width of the Feature Waves

Each of the waves has normal duration. As the regular ECG trace is plotted in a time domain, wider waves represent longer duration for a particular wave. As an example, a normal QRS complex

is 0.06–0.10 sec (60–100 ms) in duration. On the ECG paper (on which the ECG is plotted), this normal duration is represented by 3 small square boxes (or less). A QRS covering 4 or more small squares are identified as longer time taken by the ventricles to contract. Wide QRS indicates many cardiovascular abnormalities like Wolff–Parkinson–White syndrome (WPS), Left Bundle Branch Block (LBBB), Right Bundle Branch Block (RBBB) etc. [17.19].

The PR interval is measured from the beginning of the P wave to the beginning of the QRS complex. It is usually 120–200 ms long. On an ECG tracing, this corresponds to 3–5 small boxes. A PR interval of > 200 ms may indicate a first degree heart block. On the ECG trace, width or duration of the feature waves are obtained from x axis deviations [17.19].

Amplitude of the Feature Waves

Amplitude of the waves refers to the actual measurement of the electrical activity within the heart. It is read in the millivolt range from the y axis of the ECG wave. In many cases the amplitude measurements are dependent on the sensitivity of the ECG sensors, material of the skin electrodes (e.g., gel, dry, etc.), moisture of the skin and several other factors (like presence of hair on the skin). Gel based skin electrodes are often preferred over dry metal electrodes for lower levels of impedance. However, independent of the acquisition devices or electrodes, the ratio of amplitudes of different feature waves can provide an understanding of the level of forces within different section of the heart.

Direction of the Feature Waves

Direction of the feature waves can often indicate certain heart conditions. As an example, inverted (or negative) T waves can be a sign of coronary ischemia, Wellens' syndrome, left ventricular hypertrophy, or central nervous system (CNS) disorder [17.19].

Slope or Curvature of the Feature Waves

The slope or curvature of the waves also suggests certain abnormalities. Tall or "tented" symmetrical T waves may indicate hyperkalemia. Flat T waves may indicate coronary ischemia or hypokalemia [17.19].

17.1.2 Rhythm Analysis

Apart from the morphology of the ECG feature waves, which represent activities of different segments of the heart, continuous beating of the heart creates a continuous ECG trace (Fig. 17.3). From these continuous ECG traces, morphology of beating can be ascertained. This beating of the heart can be regular or irregular. Irregularity of beat intervals, which is often termed as the RR interval, can inherit several patterns suggesting arrhythmia (a heart condition caused by irregular beating of the heart). The RR interval is the time difference between consecutive R peaks (the peak of the QRS complex). As it is seen from Fig. 17.3, an ECG wave contains the feature set, $F = P_m \cup (QRS)_m \cup T_m$.

$$P_m = \{P_1, P_2, P_3, P_4, P_5\}, \tag{17.1}$$

$$(QRS)_m = \{(QRS)_1, (QRS)_2, (QRS)_3, \\ (QRS)_4, (QRS)_5\}, \tag{17.2}$$

$$T_m = \{T_1, T_2, T_3, T_4, T_5\}. \tag{17.3}$$

Apart from the features, an ECG trace also contains the featureless portion, $\overline{F}$. In medical and biomedical terminology this featureless portion of ECG signal is often referred as isoelectric line or baseline. Now, the RR interval can be represented by Eq. (17.4).

$$RR_u = time\ of\ occurance(QRS)_m \\ - time\ of\ occurance(QRS)_{m-1}. \tag{17.4}$$

Instantaneous Heart Rate (IHR) is obtained from the reciprocal of continuous RR intervals. It is shown in Eq. (17.5). In Eq. (17.5) the value 60 comes from 60 s in 1 min.

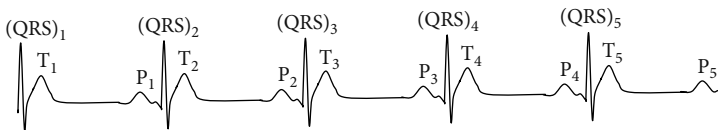$$IHR = \frac{60}{RR_1}, \frac{60}{RR_2}, \frac{60}{RR_3}, \dots, \frac{60}{RR_u}. \tag{17.5}$$

Fig. 17.3 Continuous beating of the heart

Cardiologists often refer to Heart Rate Variability (HRV) to obtain detailed understanding of the beat pattern. HRV is the beat-to-beat alterations in heart rate. HRV provides detailed understanding of Cardiovascular Autonomic Control and activities of the Autonomous Nervous System [17.20]. The importance of HRV was pervasively appreciated in the late 1980s, when it was confirmed that HRV was a strong predictor of mortality after an acute myocardial infarction [17.21]. Apart from these, recent research shows that HRV also provides indications for mental stress and respiratory functions of an individual [17.22, 23].

Originally, HRV was assessed manually from calculation of the mean RR interval and its standard deviation measured on short-term (e.g., 5. min) electrocardiograms. The smaller the standard deviation in RR intervals, the lower is the HRV. To date, over 26 different types of arithmetic manipulations of RR intervals have been used in the literature to represent HRV. In the last ten years, there have been more than 2,000 articles published on HRV. Calculation of HRV can be performed by the standard deviations of the normal mean RR interval obtained from successive 5-min periods over 24-h Holter recordings (called the SDANN index); the number of instances per hour in which two consecutive RR intervals differ by more than 50 ms over 24-h (called the pNN50 index); and numerous other ways. RR interval, IHR and HRV provide further indication of heart's activity as well as autonomous nervous control.

17.2 What Can ECG Based Biometrics Be Used for?

Like any other biometric entities, ECG based biometric compares the enrolment ECG against verification ECG or identification ECG. During verification stage the system validates the claimed identity of a particular person. The person provides a PIN or name or smart card to identify himself and his acquired ECG is matched (one-to-one matching) with his own ECG template, which was acquired during an earlier stage of enrolment. On the other hand, during the identification stage, an individual's biometric ECG is recorded and template matching is performed throughout the ECG template database. After this one-to-many matching, whenever a match is found within a set threshold, the individual is identified.

In the case of positive identification, a scoring value, rank or confidence level denotes the matching proximity between the acquired biometric entity (during verification or identification stage) and template. In the case of no match, the person remains unidentified. Throughout this chapter, the template ECG is referred to as enrolment ECG and the ECG acquired during the verification or identification stage is termed as recognition ECG. Before performing the matching between the enrolment ECG and recognition ECG, the unique ECG feature must be identified. After identifying the unique ECG features, pattern matching can be performed for the recognition task. This basic process is true for all biometric entities. As an example, for the finger print based biometric identification task, minutiae must be located first, on which the matching is performed later. From the literature, different groups of researchers have contributed to ECG based biometric recognition [17.2–18, 24, 25]. With a variety of existing ECG based biometric techniques, ECG based biometric can now be considered for industrial applications, especially for cardiovascular patient monitoring scenario [17.18].

17.3 Classification of ECG Based Biometric Techniques

Previous research has classified the ECG based biometric techniques in two ways [17.6]. The first classification is ECG biometric with Fiducial Point detection. Under this process, on set and off set of the feature waves are detected first. After locating all these points, feature wave duration, amplitude, curvature, direction, slope, etc., are obtained. These wave characteristics are saved as enrolment data. During the recognition phase, all this information is again extracted from the recognition ECG. At last, template matching of the ECG morphology is performed.

In the second type of ECG biometric, ECG features are extracted in the frequency domain. Therefore, the ECG signal in the time domain is first converted to the frequency domain, from where the desired ECG features are identified [17.3, 6, 24]. These frequency domain transformations may utilize various signal processing techniques like Fourier Transform, Wavelet Transform, Discrete Cosine Transform, etc.

However, modern ECG based biometrics can be derived from any of the following three classifica-

tions. ECG based biometric can be grouped into the following three classifications.

17.3.1 Direct Time Domain Feature Extraction

This classification again can be subdivided into two groups. The first group concentrates on extraction of intra beat morphological features and the second group considers on inter beat features (beat patterns).

ECG Morphology

The first subgroup includes only morphological features of the ECG as shown by previous researchers [17.2, 7, 12–14]. Direct time domain feature extraction is the first reported method for ECG based biometric as demonstrated by [17.2]. To reveal the time domain features, fiducial points (i.e. the PQRST signature along with their onsets and offsets) are detected first. After detecting these points from the ECG trace, different features like, P duration, P amplitude, QRS duration, QRS amplitude, T duration, T amplitude, etc., are detected (as seen in Fig. 17.4).

Many of the time domain features used for ECG based biometrics [17.2, 7, 12–14] are apparent from Fig. 17.4. These intervals (PQ interval, PR interval, QT interval), durations (P duration, QRS duration, T duration), amplitudes (P amplitude, QRS amplitude, T amplitude), slope (ST slope) and segment

(ST segment) are used as ECG features for biometric identifications. These ECG biometric features are the most primitive form of ECG features, since most of these time-domain features are used for cardiovascular diagnosis.

Uniqueness of Beating Patters

Apart from these ECG morphological features, there are some other features that can be found from the patterns of consecutive hear beats. RR interval, IHR and HRV are some of these parameters that have been described in Sect. 17.3.2. Reference [17.4, 5, 8] are ECG based biometric research falling into these categories. These variations of beat pattern occur for many reasons. One of the reasons is breathing pattern. There is a significant difference in our breathing pattern as well. These breathing patterns leave traces in our beating (heart rhythm) patterns.

In reference [17.8], the author has successfully utilized mean and variance of RR intervals for human identification purposes.

17.3.2 Frequency Domain Feature Extraction

Recently, signal processing techniques are being used to extract some of the subtle frequency domain features, which might not be as apparent as direct time domain features. Wavelet decomposition, Fourier transformation, and discrete cosine
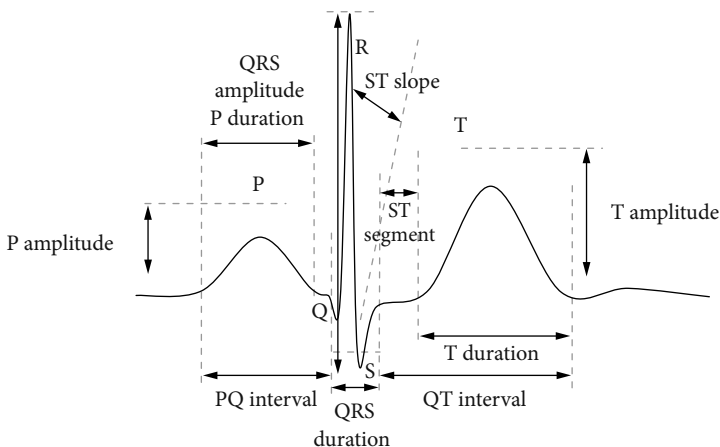

Fig. 17.4 Fiducial detection based ECG features using ECG based biometric

transform are some of frequency domain feature extraction techniques.

Wavelet Decomposition

Reference [17.3] has used wavelet decomposition techniques to measure the distance of the enrolment coefficients and recognition coefficients. They found this technique to be more applicable in minimizing misclassification rates when compared to other techniques like Percentage Root-Mean-Square Deviation (PRD), Cross-correlation (CC), etc. [17.26].

Wavelets offer a means of representing a signal in a way that simultaneously provides both time and frequency knowledge; therefore, it would provide an appropriate representation of the ECG waveform. Detail coefficients of the discrete wavelet transform (or DCT) ($\gamma^{q,v}$; detail coefficient v from the qth level of decomposition) are calculated for each signal. Using these coefficients, a distance is measured as Wavelet Distance Measurement (WDM).

The numerator of Eq. (17.6) is the absolute difference of the wavelet coefficients from the unknown signal and the enrolled data. The denominator is used to weigh the contribution of this difference based upon the relative amplitude of the wavelet coefficient from the signal not known. The denominator also includes a threshold (ξ) to avoid relatively small wavelet coefficients from overemphasizing deviations. For the WDIST measure, the person associated with the enrolled data with the lowest WDIST is selected as a match for human identification. In this paper, the mother wavelet, sym5 was chosen with a five decomposition level, which was empirically found to be the optimal value for ECG compression utilizing wavelets [17.3].

$$\text{WDIST} = \sum_{q=1}^{Q} \sum_{v=1}^{V} \frac{\left| \gamma_0^{q,v} - \gamma_z^{q,v} \right|}{\max(\left| \gamma_0^{q,v} \right|, \xi)} \qquad (17.6)$$

Fourier Transform

Researchers have also used Fourier Transformation based techniques, while extracting features from heart sounds [17.24]. The interesting fact about this research is that, instead of obtaining an ECG signal using the ECG acquisition device, they have used a stethoscope to obtain the Lubb–Dubb sound of the human heart. They have demonstrated their success in human identification from unique heart sounds.

Discrete Cosine Transform (DCT)

Reference [17.6] has used DCT based transformations to extract ECG feature templates. Using DCT based signal processing, they have depicted a way for obtaining a successful ECG based biometric.

17.3.3 Other Approaches

Other approaches for human identification include neural network based techniques, polynomial based techniques and different other statistical approaches.

Neural Network

Neural Networks was also been adopted for ECG based biometric research [17.12]. Researchers in [17.12] have used both template matching algorithms (based on a correlation coefficient) and Decision Based Neural Networks (DBNN) to obtain 100% accuracy in identifying person (when experimented on 20 subjects).

Polynomial Based

In [17.17, 18] a polynomial was used to extract polynomial coefficients from the ECG signal (both enrolment and recognition). These coefficients were then used as biometric templates for matching purposes. Using a distance measurement technique, similar to [17.3], [17.17, 18] has shown a superior mechanism of human identification using their ECG. Instead of a regular polynomial [17.17, 18], [17.25] used a Legendre polynomial to obtain better result in terms of shorter template size (more details).

Statistical Approaches

Percentage Root-Mean-Square Difference (PRD) is pervasively used to measure the quality of reconstructed ECG after lossy ECG compression [17.27]. PRD provides a measurement of distance between two signals as in Eq. (17.7).

$$\text{PRD} = \sqrt{\frac{\sum_{i=1}^{N} [x(i) - f(i)]^2}{\sum_{i=1}^{N} [x(i)]^2}} \times 100 \qquad (17.7)$$

Cross correlation (CC) is a technique used in statistics to match the similarity of signals as represented in Eq. (17.8). CCORR quantifies a linear least squares
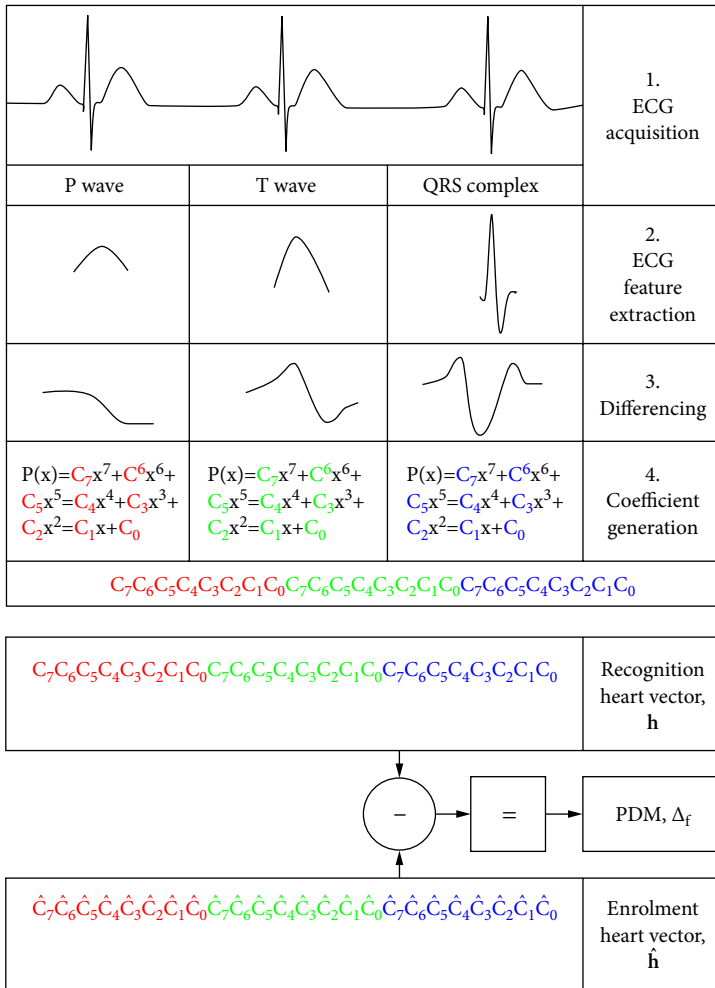
P wave	T wave	QRS complex	
			1. ECG acquisition
			2. ECG feature extraction
			3. Differencing
$P(x)=C_7x^7+C_6x^6+$ $C_5x^5=C_4x^4+C_3x^3+$ $C_2x^2=C_1x+C_0$	$P(x)=C_7x^7+C_6x^6+$ $C_5x^5=C_4x^4+C_3x^3+$ $C_2x^2=C_1x+C_0$	$P(x)=C_7x^7+C_6x^6+$ $C_5x^5=C_4x^4+C_3x^3+$ $C_2x^2=C_1x+C_0$	4. Coefficient generation
$C_7C_6C_5C_4C_3C_2C_1C_0C_7C_6C_5C_4C_3C_2C_1C_0C_7C_6C_5C_4C_3C_2C_1C_0$			

$C_7C_6C_5C_4C_3C_2C_1C_0C_7C_6C_5C_4C_3C_2C_1C_0C_7C_6C_5C_4C_3C_2C_1C_0$	Recognition heart vector, **h**

$-$ $=$ $\rightarrow$ PDM, Δ_f

$\hat{C}_7\hat{C}_6\hat{C}_5\hat{C}_4\hat{C}_3\hat{C}_2\hat{C}_1\hat{C}_0\hat{C}_7\hat{C}_6\hat{C}_5\hat{C}_4\hat{C}_3\hat{C}_2\hat{C}_1\hat{C}_0\hat{C}_7\hat{C}_6\hat{C}_5\hat{C}_4\hat{C}_3\hat{C}_2\hat{C}_1\hat{C}_0$	Enrolment heart vector, **ĥ**

Fig. 17.5 Polynomial based ECG biometric

(LS) fitting between two data sets. Different varieties of CC approaches have been employed for template matching of the ECG signal as reported in previous research [17.7, 28]. Some previous work utilized both P and QRS templates for locating successive P waves and QRS complexes for all cardiac cycles during their experimentation (detailed in [17.28]). More recently, [17.28] utilized all ECG signature templates (P wave, QRS complex and T wave) to perform multi-component CC approach to identify all three components from 3,000 cardiac cycles or beats

$$r_{cc} = \frac{1}{M}\sum_{i=1}^{N} x(i) \times f(i) \,. \qquad (17.8)$$

Apart from these, researchers have used Least Discriminant Analysis (LDA) [17.7], Autocorrelation [17.6] and Mean–Variance of RR interval [17.8] for ECG based biometric research.

17.4 Comparison of Existing ECG Based Biometric Systems

Within this section, basic comparisons among a few of the existing ECG based biometric methods are presented. Misclassification and accuracy is the most important criteria for assessing any of the biometric algorithms. Other parameters for judging

a particular identification method are template size, computational requirements etc.

17.4.1 Misclassifications and Accuracy

When PRD, CC and WDM were applied to a recognized person, they resulted in higher misclassification rates [17.3]. However, the PDM measurement technique resulted in a substantially lower rate of misclassifications. These misclassifications occurred because of not prioritizing the ECG features and occurrence of abnormal beats. However, [17.17] adopted a specialized algorithm, which assigned priority for distance measurements with QRS complexes being the highest priority and P waves being the lowest priority. To deal with the problem of ectopic beat, another algorithm [17.17] was utilized during the acquisition phase. Therefore, all the misclassifications were avoided. Table 17.1 compares the misclassification rate of the PDM method with recent ECG biometric matching algorithms. Table 17.2 compares the PDM of [17.17] method with other biometric modalities.

In Table 17.2, FMR and FNMR are abbreviations for False Match Rate and False Non Match Rate respectively [17.1]. FMR shows the chances of a wrong person's (different) enrolment data being matched against the recognition data provided. On the other hand, FNMR reflects the occurrences of the same person's enrolment data and recognition data not being similar. Both FMR and FNMR assist in generation of misclassification rate. As seen from Table 17.2, both FMR and FNMR have been previously used for performance comparisons of different biometric system [17.29–33].

Table 17.1 Misclassification rate for PRD, CC, WDM and proposed PDM [17.17]

Method	Misclassification rate (%)
PRD [17.3]	25
CC [17.3]	21
WDM [17.3]	11
PDM (without Alg. 1, without Alg. 2) [17.17]	13.33
PDM (with Alg. 1, without Alg. 2) [17.17]	6.66
PDM (with Alg. 1, with Alg. 2) [17.17]	0

Table 17.2 FRM and FNRR across different modalities [17.17]

Modality	FMR (%)	FNMR (%)	Reference
Face	1	10	[17.29]
Fingerprint	0.01	2.54	[17.30]
Iris	0.00129	0.583	[17.31]
On-line signature	2.89	2.89	[17.32]
Speech	6	6	[17.33]
ECG	6.66	6.66	PDM (without Alg. 1, without Alg. 2) [17.17]
ECG	3.33	3.33	PMD (with Alg. 1, without Alg. 2) [17.17]
ECG	0	0	PDM (with Alg. 1 + with Alg. 2) [17.17]

17.4.2 Template Size

As mentioned earlier, the size of the templates for data has a huge impact on the overall performance of the biometric system. A system that requires a larger vector of enrolment data can encompass processing delays while performing identification tasks on a reasonable population size. Moreover, longer transmission time is mandated during enrolment data transport. The storage problem of the template data is another issue for larger biometric data. Therefore, for faster performance, faster transmission and minimal storage of biometric data, the size of the template data should be minimal. As seen in [17.17], the biometric data required for a typical subject is only 318 B in uncompressed format. The active range for this template (enrolment/recognition data) was 228–402 B, during their experimentation in [17.17], with an average of 340 B. A recent work based on ECG based human identification requires at least 600 B (100 ms data of 11 bit resolution for 2 vectors on 500 Hz sampling frequency) of data for the creation of heart vector to be used as template [17.16]. For ECG biometric presented in [17.3], experimentation with PRD, CC and WDM was performed with variable length of ECG from 32 to 512 ms. For 32 ms ECG segment, with a 360 Hz sampling frequency results in 12 ECG samples ($0.36 \cdot 32 \approx 12$) or 126 B of data. Similarly, with longer ECG segment of 512 ms with the same sampling frequency, 185 ECG samples are required with an average size of 1,846 B. However, with only 12 sample (for the case of 32 ms ECG segment),

Table 17.3 Comparison of template sizes

Biometric data type	Size in B
Iris [17.34]	512
Face [17.34]	153,600-307,200
Voice [17.34]	2,048-10,240
ECG [17.16]	600
ECG (WDM) [17.3]	1,371
ECG (PRD / CC) [17.3]	2,210
ECG [17.17]	340

the misclassification rate is higher, since it can only represent one third of QRS complex while experimenting on 360 Hz sampling frequency (in case of MIT BIH ECG entries). Hence, not even a single feature can be represented by 126 B ECG segment. According to Table 17.3, the PDM technique shows the highest level of accuracy with minimal biometric template length [17.17].

17.4.3 Computational Cost

Computational cost is one of the major factors that determines the acceptability of a biometric system, since many of the biometric systems are integrated within a embedded box with less computational power. For this evaluation, we performed the comparison of computational power based on the number of operations needed to compute similarity matching between the enrolled data and recognition data. Table 17.4 shows the computational cost for PRD, CC, WDM and the proposed PDM method while performing template matching. Matching is thought to be the core computational cost involved for biometric, since this matching is required to be

Table 17.4 Comparison of number of operations (NOP) for PRD, CC, WDM and PDM [17.17]

Operation	PRD	CC	WDM	PDM
Addition	462	231	136	24
Subtraction	231	0	136	24
Multiplication	1	231	0	0
Division	1	1	136	24
Absolute value	0	0	136	24
Square root	1	0	0	0
Square	462	0	0	0
Conditional	0	0	256	0
Total	**1,158**	**463**	**800**	**96**

performed across all the entries (templates) within database wide identification. If the database contains 100 biometric entries, 100 matchings are needed to ascertain the lowest distance. On the other hand, wavelet decomposition to calculate the wavelet coefficients for WDM [17.3], or polynomial creation to calculate the values of polynomial coefficients for PDM are only a one-time cost. Therefore, the cost for polynomial computation is only a minute fraction of the cost associated with database wide matching, required for identification [17.17].

The ECG segments to measure PRD, CC and WDM (both for Table 17.3 and Table 17.4) were 231 samples, which contained a single heart beat with all the ECG feature waves. For WDM calculation of Table 17.4, 256 coefficients were generated for 231 ECG sample points. Out of these 256 coefficients, only 136 coefficients were utilized after taking the threshold (ξ) into consideration [17.3]. Therefore, conditional operations were also evaluated, considering the denominator of Eq. (17.6).

It is apparent from Table 17.4, PDM is computationally less expensive and viable than many of the existing algorithms.

17.5 Implementation of an ECG Biometric

The ECG biometric system stores the ECG enrolment data (template), x_u; where the number of the sample is denoted by u and u = 1, 2, 3, ... , U and U = Length (ECG template). Here, U is the total number of ECG samples needed to contain 5 full heart beats, where each beat contains a QRS complex, a T wave and a P wave. Therefore, when P_m is the P wave feature set, $(QRS)_m$ is the QRS complex feature set and T_m wave is the T wave feature set, we can write equations that were previously shown in Eqs. (17.1–17.3).

Hence, the complete ECG feature set containing all P waves, QRS complexes and T waves for enrolment data (x_u) is referred as F = $P_m \cup (QRS)_m \cup T_m$ and $\overline{F}$ is the featureless portion of x_u.

During the recognition stage (verification or identification), the recognition data y_n is compared against the enrolment data with a functions set S_j bounded by a threshold Γ_j. The threshold is introduced because of the fact that the recognition data can never be exactly same as the enrolment data.

$$S_j = \{S_1, S_2, S_3\} . \tag{17.9}$$

The three functions (S_1, S_2, S_3) used for determination of similarity between the recognition data y_n and enrolment data x_u are Percentage Root-Mean-Square Deviation, Cross Correlation (CC) and Wavelet Distance Measurement (WDM). These functions will be further discussed in details later in this section.

S_j decides whether y_u and x_u are similar based on a set of threshold Γ_j, where,

$$\Gamma_j = \{\Gamma_1, \Gamma_2, \Gamma_3\} . \qquad (17.10)$$

Γ_1 is the threshold for PRD, which was empirically calculated as < 14 for person recognition. Similarly Γ_2 (calculated to be > 0.03 for similarity) and Γ_3 (< 6 identifying similarity between two signals) are the thresholds for CC and WDM respectively. Based on the values returned by S_j, a weighted measurement is calculated, which is termed as the confidence level (CL). During the verification stage (when matching is performed on a one-to-one basis), a person claims that he or she is the person with identity, I. Therefore, this claim is evaluated by $S_j(y_u, x_u)$ considering the threshold Γ_j. A_1 denotes the claim is true and A_2 refers that the claim is false (for the case of spoofer). The decision logic (DL) uses verification function $\Lambda(I, y_u)$ to provide its decision $\{A_1, A_2\}$ during verification stage, whether the claim is true or false. Hence, the verification stage of ECG biometric can be shown as Eq. (17.11).

$$\Lambda(\mathbf{I}, \mathbf{y}_u) \in \begin{cases} A_1, & if\,((\mathbf{S}_1(\mathbf{y}_u, \mathbf{x}_{qu}) < \Gamma_1) \\ & \vee(\mathbf{S}_2(\mathbf{y}_u, \mathbf{x}_{qu}) < \Gamma_2) \\ & \vee(\mathbf{S}_2(\mathbf{y}_u, \mathbf{x}_{qu}) < \Gamma_3)) = true \\ A_2 & Otherwise \end{cases}$$
$$(17.11)$$

Again, for the identification stage, the recognition data is collected by the biometric sensor and then the data is compared to the enrolment data of all the identities enrolled within the system (one-to-many matching). The number of identities is denoted by q. Therefore, $q = 1, 2, 3, \ldots, Q$ and Q is the total number of people (identities) enrolled within the ECG biometric system. The identity set $\mathbf{I}_q$ contains all the individual identities identifying a specific person (enrolled within the system). Hence,

$$\mathbf{I}_q = \{I_1, I_2, I_3, I_4, \ldots, I_Q\} . \qquad (17.12)$$

During identification stage the DL uses function $\Theta(\mathbf{y}_u)$ to ascertain identity I_q. In case the DL fails

to identify the person, the unidentified status ($\mathbf{I}_{Q+1}$) is generated by function $\Theta(\mathbf{y}_u)$. The identification function $\Theta(\mathbf{y}_u)$ evaluates S_j and obtains a maximum value of CL, during the identification process. The whole process of identification can be mathematically defined as follows:

$$\Theta(\mathbf{y}_u) \in \begin{cases} \mathbf{I}_q, & if\,\mathbf{S}_j(\mathbf{y}_u, \mathbf{x}_{qu})\,within\,\Gamma_j \\ & AND\,\max(CL) \\ \mathbf{I}_{Q+1} & Otherwise \end{cases} . \qquad (17.13)$$

17.5.1 System Design of ECG Biometric

As mentioned earlier, the ECG biometric requires the following three stages or scenarios:

1. An individual enrolls into the ECG biometric system, providing his/her ECG template $\mathbf{x}_u$. The enrolment data contains five heart beats.
2. After the ECG enrolment, the system asks to verify the enrolment data. Therefore, the individual provides his ECG again. This verification ECG, $\mathbf{y}_u$ is matched against his enrolment data, $\mathbf{x}_u$ (using $\mathbf{S}_j$) and if the results of the function set, $\mathbf{S}_j$ is within the threshold, Γ_j then verification function, $\Lambda(I, y_u)$ returns A_1, denoting successful verification. Otherwise, A_2 is returned and the person might need to go through the enrolment process again. For this particular scenario, when the system asks (system is initiated) for verification of the enrolled data, the system already knows who the person is (since the person just enrolled).

   However, verification can be user initiated as well, when the user needs to identify himself/herself by providing their name or PIN or smart card apart from the verification data, $\mathbf{y}_u$. As seen in Fig. 17.6 the template fetcher module takes identity information (e.g., smart card, PIN, etc.) for identifying the person first and then pulls corresponding enrolled data ($\mathbf{x}_u$) for that person. Then, $\mathbf{S}_j(\mathbf{y}_u, \mathbf{x}_u)$ performs PRD, CC, WDM and CL calculation for the decision.
3. During the identification scenario, any person provides his/her ECG to the system. This identification ECG data, $\mathbf{y}_u$ is served as the sole parameter for identification function, $\Theta(\mathbf{y}_u)$. This function verifies the identity of the person, $\mathbf{I}_q$ and, in case of failure to identify, $\mathbf{I}_{Q+1}$ is returned by the function. Unlike the verification stage (where the person is already known),
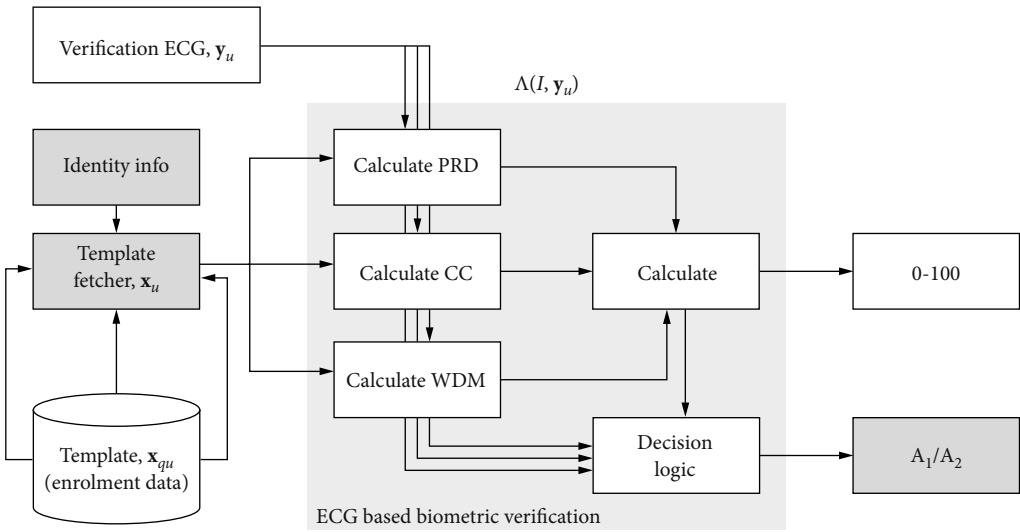
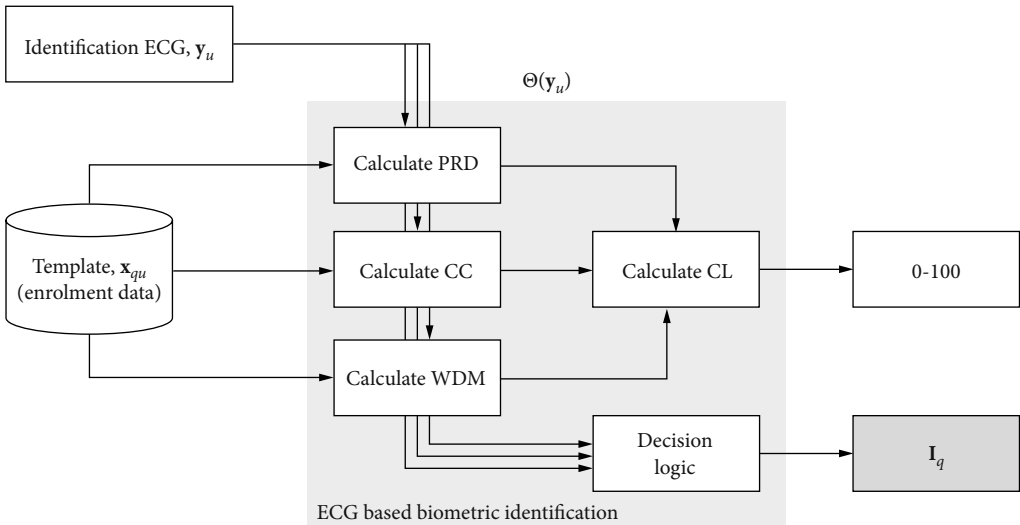**Fig. 17.6** Verification process for the ECG based biometric implementation

Fig. 17.7 Identification process of ECG biometric

the identification scenario executed an extensive database search across all the enrolled identities to retrieve the best match with maximum value of confidence level.

For both Figs. 17.6 and 17.7 (verification and identification), $\mathbf{S}_j$ or the template matching function were same. However, the decision logics were

slightly different for verification and identification.

During the calculation of the confidence level (CL), weight is given to the individual matching functions S_1, S_2 and S_3. 25% weight is given to PRD and 25% weight is provided to CC and a higher weight of 50% is allocated for WDM. WDM is given the highest weight because it was proven by the most recent

research in ECG biometrics, that WDM provides the most accurate identification rate (a rate of 89%).

$$CL = 0.25X(100\text{-}PRD) + 25XCC \\ + 0.5X(100\text{-}WDM) \tag{17.14}$$

Decision logic is slightly different in verification and identification stages. Accurate enrolment data (template) ensures reliable system behavior. Therefore, to ensure accuracy of the enrolment data, verification logic (system initiated – after enrolment) is more rigid than identification logic. Verification logic can be formulated as follows:

$B: PRD \leq 14$

$C: CC \geq 0.03$

$D: WDM \leq 6$

$E: WDM \geq 69.25$

$G:$ Person Recognized (Verified/Identified) .

The decision logic can be formulated as follows:

$$G \rightarrow B \wedge C \wedge D \wedge E \ .$$

Decision in Identification Mode: The identification logic can be formulated as follows:

$$G \rightarrow (D \wedge E) \wedge (B \vee C) \ .$$

17.5.2 Finding the Threshold with Experimentation

The ideal values for $\varGamma_j$ were required to be measured to program the proposed ECG biometric system. For this, 15 MIT-BIH people were employed and their ECGs were acquired. After a duration (one week to one month), their ECGs were acquired. For each person, the two ECG signals were measured for PRD, CC and WDM. Matlab scripts were used to automate the task for 15 MIT-BIH subjects. For all the cases, PRD were < 13.3, CC > 0.0351 and WDM

were < 5.4. Accounting calculation and experimentation errors PRD, CC and WDM values for identification was determined to be < 14, > 0.03 and < 6.

Paired ECGs of the five subjects are provided in Fig. 17.8–17.9 [17.26]. Table 17.5 shows the values for pre-identified cases of subject 1–5. Obviously, for all the cases the empirical values of the thresholds were within range.

The ECG samples for all the subjects were also randomly cross checked in [17.26] to ensure effectiveness of the threshold decided for PRD, CC and WDM. During this procedure, none of the cross checking entries resulted in violation of the set thresholds.

17.5.3 Software Implementation of the Biometric System

After the successful discerning of the thresholds for the identification task, the condition was coded to develop a rule based ECG biometric system. The whole system was implemented under a .net environment with MS Visual Studio 2005 environment. Enrolment data were maintained in SQL Server database. Publicly available ECG data were used for testing purposes (enrolment, verification and identification). The software system needs the location of the ECG file containing recognition data (captured with biopac system). On location of the ECG file, "Identify Person" option performs template matching (PRD, CC, WDM, CL) across the SQL Server database. The highest match (defined by the highest CL value) is pulled up from the database and presented by the system. Recognition data is also shown on the software screen. Since the ECG data (recognition) contains vital cardiovascular details, only selected persons with authority will be able to view this ECG signal. Otherwise, only a noised ECG is displayed. This noise obfuscation procedure

Table 17.5 Performance comparison of CL with PRD, CC and WDM [17.26]

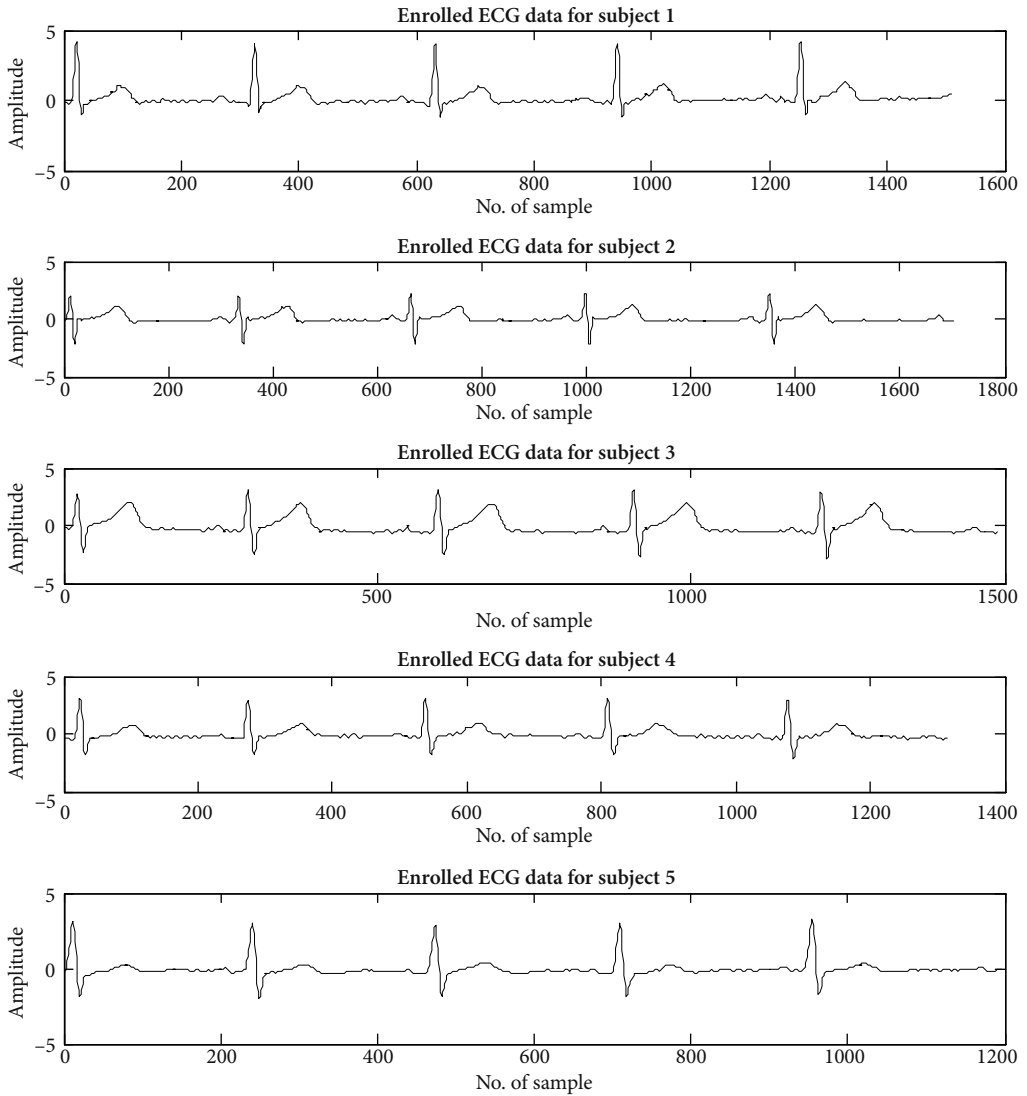| Subject	PRD	CC	WDM	CL	Length	EECG	RECG
1	11.3	0.16449	5.576	73.49925	1,511	16,273	14,611
2	13.116	0.032614	4.2031	70.4348	1,701	16,554	16,555
3	12.387	0.1375	3.7496	73.46595	1,488	14,153	14,090
4	13.194	0.049062	4.0596	70.89825	1,314	12,783	12,838
5	13.109	0.038704	3.141	71.11985	1,195	11,749	11,663

Fig. 17.8 Enrolment ECG of the subjects [17.26]

has been explained in earlier research [17.28, 35]. Figure 17.10 shows the software implementation of the ECG based recognition system.

17.5.4 Testing on Subject

After the system was developed, it was tested on the same 15 MIT-BIH subjects (fromwww.ecgwave. info). ECGs for all the subjects were acquired after two months of collection of the Enrolment data. These ECG files were fed to the biometric software, to measure the effectiveness of the system. Hitting the "Identify Person" button results in extensive database wide search to ascertain the highest value for CL. Name and picture of the person with highest CL value is displayed by the software.
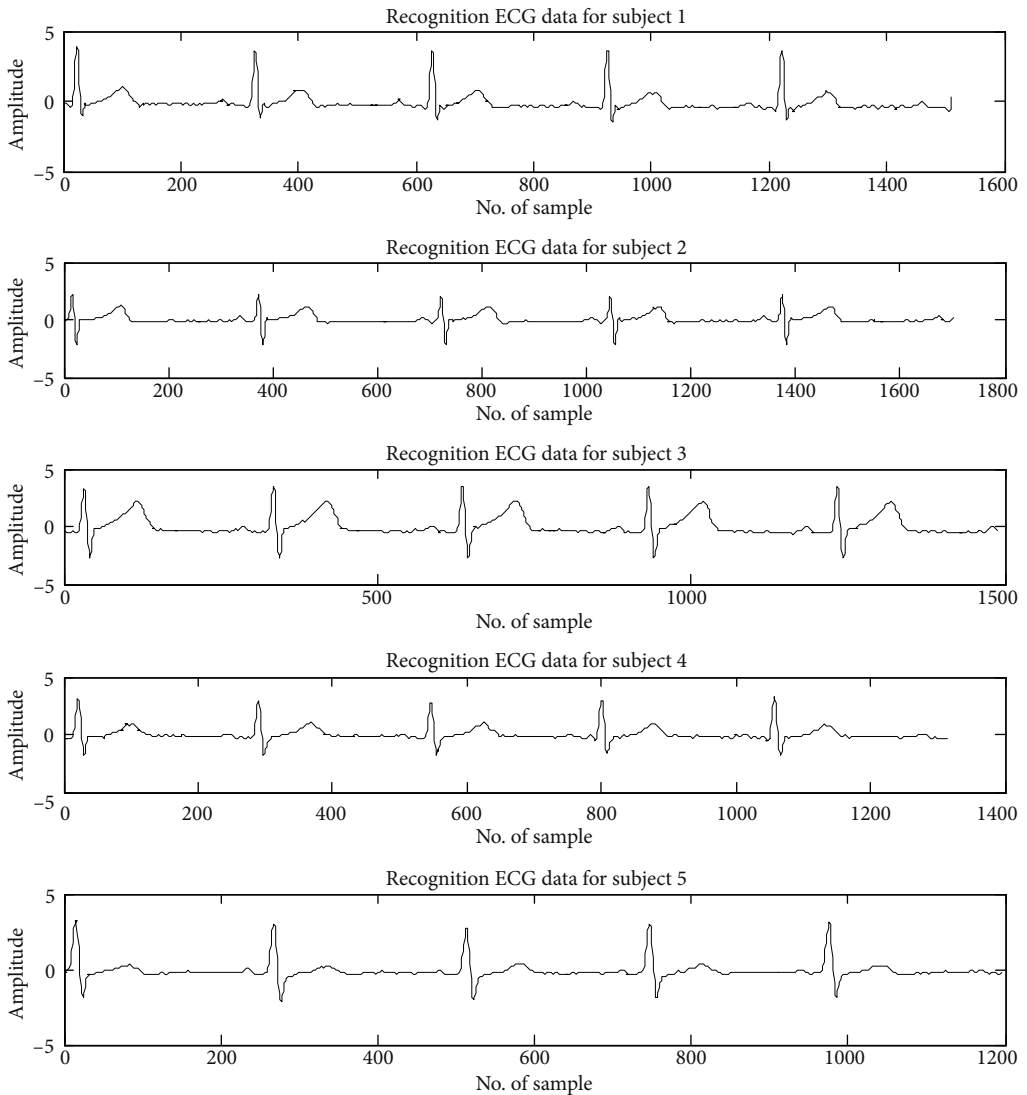
Fig. 17.9 Recognition ECGs of the subjects [17.26]

17.6 Open Issues of ECG Based Biometrics Applications

The existing ECG based biometric authentication systems suffer from several pitfalls [17.2–16, 24]. However, many of these short comings were addressed by more recent researches [17.17, 18, 25]. The results obtained in [17.17, 18, 25] needs to be validated by a larger population size.

17.6.1 Lack of Standardization of ECG Fiducial Points

Most of existing works related ECG biometric, including the earliest method shown in [17.2], rely heavily on the detection of ECG PQRST signature [17.17]. Recent papers describe the ECG biometric performed in two possible ways; by detecting the fiducial point or without fiducial point
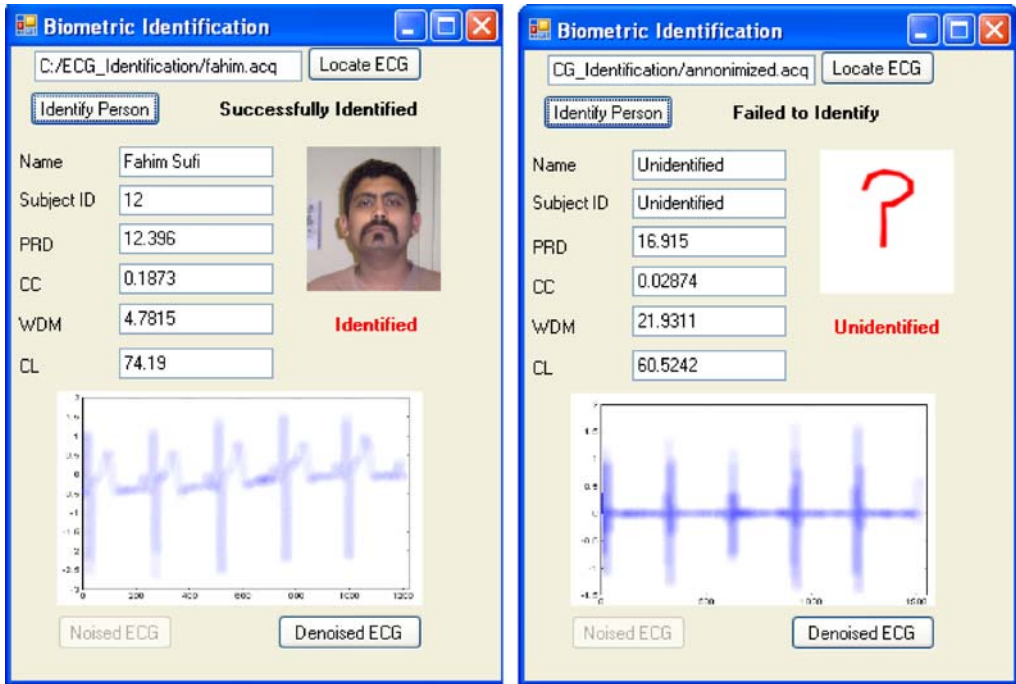
Fig. 17.10 ECG Biometric software performing identification

detection. ECG biometric based with fiducial point detection is inherently flawed as reported by recent research [17.6], since there is no standard definitions as to where the ECG feature wave boundaries lie [17.36]. Most of the medical grade ECG devices approximate these fiducial points since approximate locations are sufficient for medical diagnosis as reported by [17.6]. However, for the purpose of ECG being a biometric entity, the points need to be exact since the slightest variation of fiducial point locations will result in misclassifications within the enormous domain of human population (approximately 6.5 billion). The misclassification will be even severe when different ECG acquisition devices are used, since each of the device vendors follows its own definition of ECG wavelength boundaries [17.6, 17].

17.6.2 Time Variant Nature of ECG

The second challenge poisoning the domain of the ECG based biometric is the time varying nature of ECG waves [17.17]. Unlike other biometric entities, like fingerprint, iris, etc., the morphology

of the ECG signal acquired even for a fraction of a second varies from time to time even for the same person [17.7], With the change of heart rates, different patterns, like RR interval, QT interval, and T duration of the ECG signal, vary for the same person [17.37]. Therefore, if the acquired ECGs for the same person during both the enrolment stage and recognition stages are collected when the person is under different physiological conditions (exhausted, stressed, after exercise, relaxed, anxious), most of the existing systems on ECG based biometric will likely fail, since these time varying physiological variations were considered using very few algorithms [17.7]. Based on this time varying nature, which is one of the crucial challenges for ECG based biometric recognition, researchers have shown the possibility of ensuring security on a body sensor network with multiple sensors communicating amongst themselves [17.4, 5]. Researchers in [17.4, 5] have proposed a practical case where all the sensors placed within a body have their own heart monitoring sensors just for ensuring secured communication among the sensors placed within a body area network (BSN). Therefore, as long as these sensors

sense the synchronized (subject to minute delay) heart beats for a particular person, they are allowed to communicate with each other, since it is ensured that they are within the same BSN. For these cases, both randomness and biometric nature of the human heart is used to substitute the requirement of session key for a secured communication [17.17].

17.6.3 Pertinence of Random Abnormality in ECG

Few random traces of ECG abnormality can exist in a normal person, ruining the ECG PQRST signature, which may result in misclassification for biometric recognition [17.17]. One of these abnormalities is ectopic beat or premature beat which often goes unnoticed for a normal person. Hardly any of the existing biometric recognition techniques deployed any algorithms to deal with automated detection of nonstandard ectopic beats. Application of only simple beat averaging techniques implemented by earlier researches [17.12–14] results in the storage of faulty template, giving misclassifications when applied to a few seconds of ECG acquisition with an abnormal beat present [17.17].

17.6.4 Longer Duration for ECG Wave Acquisition

For a biometric system to be pervasively accepted, the time required to acquire the biometric data should be as minimal as possible [17.17]. Present biometric solutions based on fingerprints take less than a second of acquisition time, which is one of the reasons why fingerprint being widely accepted where urgency is crucial (military operations, medical service providers, etc.). Many of the previous research adopted beat averaging for 20 beats, which might take up to 20 s of time (for acquisition) [17.17]. Therefore, these ECG based biometric systems are not feasible for time critical operations and mission critical health services [17.17].

17.6.5 Lack of Portability and Higher Computational Cost for ECG File Processing

One of the major obstacles in the world of biometrics is reduction of the number of features for biometric recognition [17.17]. Therefore, principal component analysis and similar measurements have been implemented by earlier works on ECG biometrics [17.2, 7]. The sizes of the templates for iris, face and voice are 512 B, 150–300 kB and 2–10 kB respectively as reported in [17.17, 34]. Even the most recent work demonstrated on ECG based human identification needs at least 600 B (100 ms data of 11 bit resolution for 2 vectors on 500 Hz sampling frequency) of data for the generation of heart vector to be used as a biometric template (enrolment/verification data) [17.16]. Even though the size of the template appears to be insignificant, when this information is matched by $O(N^2)$ algorithms, across a recognition database of only 100 people, the computational latency/cost is notable for many of the existing ECG biometric systems [17.3, 6, 15]. Therefore, for organizations comprising of thousands of staff, many of the existing biometric algorithms are unsuitable for commercialization, even though their research value is of significant importance. Therefore, an algorithm, where one-to-many matching is performed only for limited number of entries (vectors with minimal elements), will be optimal choice for future ECG based biometric system seeking commercial impact [17.17].

17.6.6 Lack of Experimental Data for Verification

Unlike fingerprinting or some other fingerprint based techniques, ECG based biometrics is lagging behind in validating the level of uniqueness. The main reason is simply because of lack of data. As data must be obtained using acquisition devices from the human being, the entire process may go through rigorous ethical guidelines. Therefore, obtaining ethics approval is required in most cases prior to collection of ECG data to be used for biometrics.

Even after proper ethics approval, existing researchers are only able to acquire a limited set of data. As an example [17.2–4, 7, 9, 12, 14, 16–18] validated their research only on 7, 15, 15, 20, 29, 35, 50, 74, 99, 168 subjects respectively. To uphold ECG as a powerful entity for human identification, validation of results on a larger group comprising of different ethnicity, age and sex is required. PTB and MIT BIH databases (available in http://www.physionet.org) are very popular ECG databases available for cardiovascular researchers.
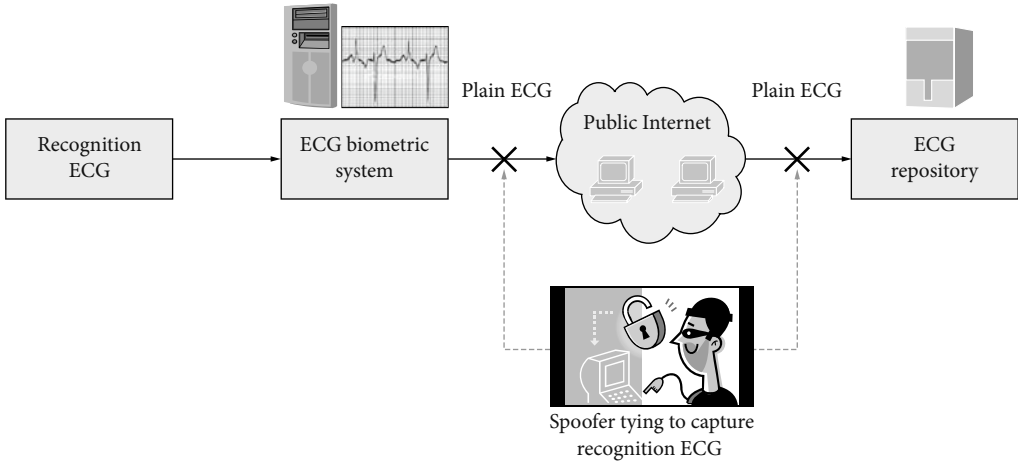
Fig. 17.11 Security threats for plain text ECG transmission via public Internet
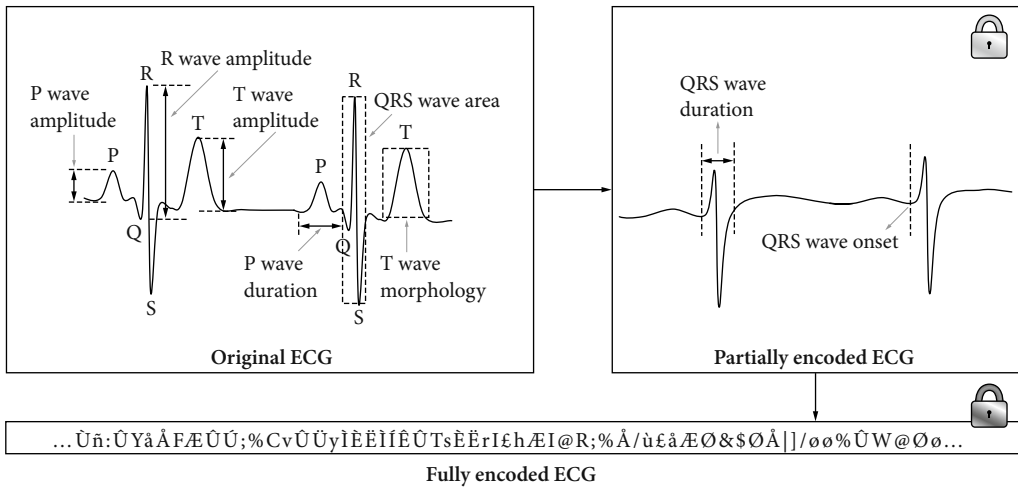

Fig. 17.12 Encoding ECG with specialized ECG encryption algorithm [17.27]

However, both of these databases are primarily suitable for disease diagnosis purposes and contain abnormal ECG (with cardiovascular disease traits). However, for ECG based biometrics, at least two sets of data (for enrolment and recognition), which has been obtained over a moderate interval, is necessary.

As a result, ECG biometric researchers can only use a limited number of datasets for ECG based biometrics. For example, [17.6] only used ECG data from 13 selected individuals present within these databases. Very recently, ECG Wave Information

(ECGWI) (available at http://www.ecgwave.info) provides ECG data collected from a larger population. As ECGWI's data includes multiple recorded sessions (from the same person), it is highly suitable for ECG based biometric research.

Apart from all these challenges, research communality is continuously endeavoring for more accurate biometric solutions. All the previous research related to ECG based biometric system [17.2–16] show moderate level of accuracy in identifying person by template matching or feature comparison techniques.
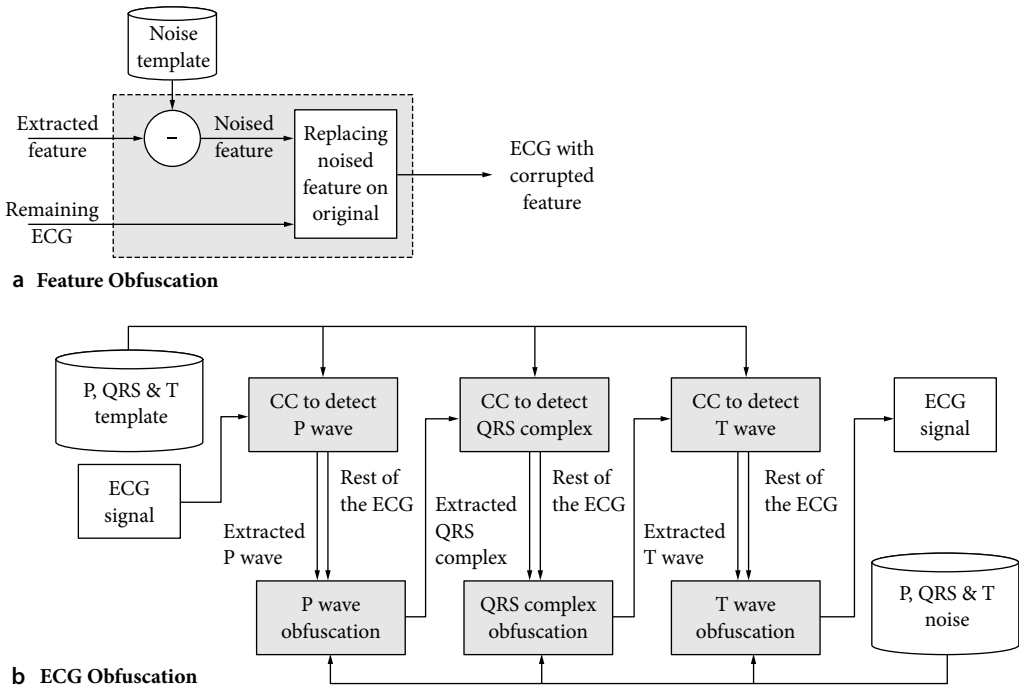
a Feature Obfuscation

b ECG Obfuscation

Fig. 17.13a,b ECG obfuscation with noise smearing [17.35]

17.7 Security Issues for ECG Based Biometric

Since ECGs can be successfully utilized to perform human identification, proper security mechanisms should be in place during data transmission. Especially during the transmission of ECGs via internet, ECGs should be encrypted, obfuscated or anonymized. Apart from providing standard information security, securing ECG resists spoof attacks on biometric data. This is highly desirable as biometric entity disclosure means unauthorized persons access to restricted facilities [17.18]. With the absence of proper encryption mechanism, plain ECG can be spoofed by a malicious hacker to be used for replay attack (as seen in Fig. 17.11). Recent research shows three major types of techniques for securing ECG files.

17.7.1 ECG Encryption

A specialized permutation cipher (character shuffling) based ECG encryption technique has been

reported by recent researches [17.27]. Permutation key is only known to the authorized personnel, who can decrypt the ECG encrypted ECG. As seen in Fig. 17.12, following some mathematical transformations [17.27], the original ECG can be transformed into fully encoded ECG (in a form of scrambled ASCII letters). This technique has shown better results in terms of security strength when compared with AES and DES. When combined with existing encryption schemes, the strength can be further raised providing unmatched protection against spoof attacks [17.27].

17.7.2 ECG Obfuscation

These types of mechanisms, basically work in a two step process [17.28, 35]. At first the location of the feature waves are detected with an efficient detection algorithm. Once the feature waves are detected, random noise or predefined noise is added on top the feature wave, so that the feature wave gets corrupted. Fig. 17.13 shows the block diagrams of ECG obfuscation technique. Fig. 17.13a, shows the noise addi-
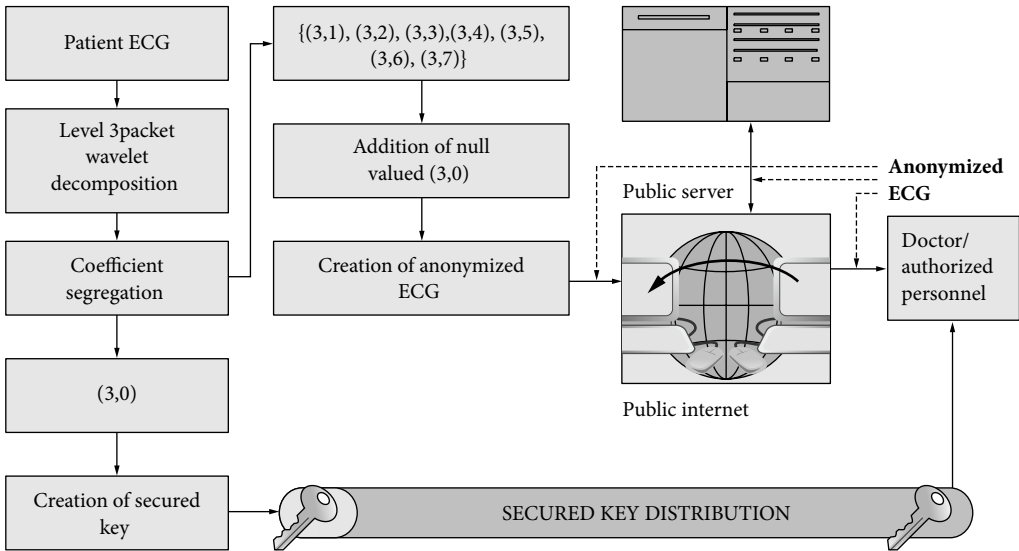
Fig. 17.14 Wavelet based ECG anonymization techniques [17.26]

tion process to each of the detected ECG features. In Fig. 17.13b the researchers used Cross Correlation based techniques to detect the individual ECG features [17.35]. However in [17.28], a different feature detection method was utilized to find the original location of the features.

Doctors, on the other hand, know the exact noises that were added to corrupt the ECG signal. These noises, along with the feature template, create the key for reconstruction of the original ECG signal.

17.7.3 ECG Anonymization

These techniques utilize the knowledge of both frequency and time domain information through wavelet decomposition [17.26, 38]. After obtaining the wavelet coefficients, the first coefficient (that represents the lowest frequency) is corrupted with known or random values. Then, including the corrupted coefficients, all the wavelet coefficients (unchanged ones) are used to recreate the ECG. However, because of the impact of the corrupted coefficient, the reconstructed ECG becomes anonymized. Fig. 17.14 shows the entire process of wavelet based ECG anonymized procedures in block diagram [17.26].

This anonymized can then be distributed freely over the public infrastructure. To retrieve the original ECG, the authorized personnel must know the original value of the corrupted coefficient.

17.8 Conclusions

Within this chapter, we have introduced the physiology and different features of the ECG wave and how these ECG features can be used for identifying a person. Then we discussed the existing ECG based biometric research under three different classifications. We compared those existing ECG based biometric techniques in terms of computational requirements, template size and misclassification rate. We have also implemented a simple ECG based biometric system based on three different techniques (CC, PRD and WDM). Next, we discussed some of the open issues and challenges prevailing in ECG biometric domain. Before concluding the chapter, we also talked about the existing techniques for securing ECG signals.

References

17.1. A.K. Jain, A. Ross, S. Prabhakar: An introduction to biometric recognition, IEEE Trans. Circuits. Syst. Video **14**(0), 4–20 (2004)

17.2. L. Biel, O. Petersson, L.P. Philipson Wide: ECG Analysis: a new approach in human identification, IEEE Trans. Instrum. Meas. **50**(3), 808–812 (2001)

17.3. A.D.C. Chan, M.M. Hamdy, A. Badre, V. Badee: Wavelet distance measure for person identification using electrocardiograms, IEEE Trans. Instrum. Meas. **57**(2), 248–253 (2008)

17.4. C.C.Y. Poon, Y.T. Zhang, S.D. Bao: A novel biometric method to secure wireless body area sensor networks for telemedicine and m-Health, IEEE Commun. Mag. **44**, 73–81 (2006)

17.5. F.M. Bui, D. Hatzinakos: Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling, EURASIP J. Adv. Signal Process. **2008**, 529879 (2008)

17.6. Y. Wang, F. Agrafioti, D. Hatzinakos, K. N. Plataniotis: Analysis of human electrocardiogram for biometric recognition, EURASIP J. Adv. Signal Process., **2008**, 148658 (2008)

17.7. S.A. Israel, J.M. Irvine, A. Cheng, M.D. Wiederhold, B.K. Wiederhold: ECG to identify individuals, Pattern Recognit. **38**(1), 133–142 (2005)

17.8. J.M. Irvine, B.K. Wiederhold, L.W. Gavshon, S.A. Israel, S.B. McGehee, R. Meyer, M.D. Wiederhold: Heart rate variability: a new biometric for human identification, Int. Conf. on Artif. Intell., Las Vegas (2001) pp. 1106–1111

17.9. S.A. Israel, W.T. Scruggs, W.J. Worek, J.M. Irvine: Fusing face and ECG for personal identification, Proc. 32nd IEEE Appl. Imagery Pattern Recognit. Workshop (2003), 226–231

17.10. M. Kyoso, A. Uchiyama: Development of an ECG identification system, Proc. 23rd IEEE Eng. Med. Biol. Conf., Vol. 4 (2001) pp. 3721–3723

17.11. M. Kyoso: A technique for avoiding false acceptance in ECG identification, Proc. IEEE EMBS Asian-Pacific Conf. Biomed. Eng. (2003) pp. 190–191

17.12. T.W. Shen, W.J. Tompkins, Y.H. Hu: One-lead ECG for identity verification, Proc. 2nd Joint EMBS/BMES Conf. (2002) pp. 62–63

17.13. T.W. Shen: Biometric Identity Verification Based on Electrocardiogram (ECG). Ph.D. Thesis (University of Wisconsin, Madison 2005)

17.14. T.W. Shen, W.J. Tompkins: Biometric Statistical Study of One-Lead ECG Features and Body Mass Index (BMI), Proc. 2005 IEEE EMBS Conference, Shanghai (2005)

17.15. K.N. Plataniotis, D. Hatzinakos, J.K.M. Lee: ECG biometric recognition without fiducial detection, Proc. Biometrics Symposiums (BSYM), Baltimore (2006)

17.16. G. Wubbeler, M. Stavridis, D. Kreiseler, R.D.C. Bousseljot Elster: Verification of humans using the electrocardiogram, Pattern Recognit. Lett. **28**(0), 1172–2275 (2007)

17.17. F. Sufi, I. Khalil, I. Habib: Polynomial distance measurement for ECG based biometric authentication, Security and Communication Networks (Wiley Interscience), DOI 10.1002/sec.76 (Accepted and published online 3 Dec 2008)

17.18. F. Sufi, I. Khalil, An Automated Patient Authentication System for Remote Telecardiology, The fourth International Conference on Intelligent Sensors, Sensor Networks and Information Processing, ISSNIP 2008, Melbourne (2008)

17.19. M. Gabriel Khan: *Rapid ECG Interpretation*, 2nd edn. (Saunders, Philadelphia, PA 2003)

17.20. H.-W. Chiu, T. Kao: A mathematical model for autonomic control of heart rate variation, IEEE Eng. Med. Biol. Mag., **20**(2), 69–76 (2001)

17.21. M. Malik, T. Farrell, T. Cripps, A. Camm: Heart rate variability in relation to prognosis after myocardial infarction: selection of optimal processing techniques, Eur. Heart J. **10**(0), 1060–1074 (1989)

17.22. M. Kumar, M. Weippert, R. Vilbrandt, S. Kreuzfeld, R. Stoll: Fuzzy evaluation of heart rate signals for mental stress assessment, IEEE Trans. Fuzzy Syst. **15**(5), 791–808 (2007)

17.23. O. Meste, B. Khaddoumi, G. Blain, S. Bermon: Time-varying analysis methods and models for the respiratory and cardiac system coupling in graded exercise, IEEE Trans. Biomed. Eng. **52**(11) 1921–1930 (2005)

17.24. K. Phua, T.H. Dat, J. Chen, L. Shue: Human identification using heart sound, 2nd Int. Workshop on Multimodal User Athentication (2006)

17.25. I. Khalil, F. Sufi: Legendre Polynomials Based Biometric Authentication Using QRS Complex of ECG, 4th Int. Conference on Intelligent Sensors, Sensor Networks and Information Processing, ISSNIP 2008, Melbourne (2008)

17.26. F. Sufi, S.S. Mahmoud, I. Khalil: A novel wavelet packet-based anti-spoofing technique to secure ECG data, Int. J. Biom. **1**(2), 191–208 (2008)

17.27. F. Sufi, I. Khalil: Enforcing Secured ECG Transmission for realtime Telemonitoring: A joint encoding, compression, encryption mechanism, Secur. Comput. Netw. **1**(5), 389–405 (2008), doi: 10.1002/sec.44

17.28. F. Sufi, I. Khalil: A new feature detection mechanism and its application in secured ECG transmission with noise masking, J. Med. Syst. (2008), doi: 10.1007/s10916-008-9172-6

17.29. K. Nandakumar, A.K. Jain, S. Pankanti: Fingerprint-based fuzzy vault: implementation and performance, IEEE Trans. Inf. Forensics Secur. **2**(4), 744–757 (2007)

17.30. K.-A. Toh, X. Jiang, W.-Y. Yau: Exploiting global and local decisions for multimodal biometrics ver-

ification, IEEE Trans. Signal Process. **52**(10), 3059–3072 (2004)

17.31. J.P. Martinez, R. Almeida, S. Olmos, A.P. Rocha, P. Laguna: A wavelet-based ECG delineator: evaluation on standard databases, IEEE Trans. Biomed. Eng. **51**(4), 570–581 (2004)

17.32. L. Sörnmo, P. Laguna: *Bioelectrical Signal Processing in Cardiac and Neurological Applications* (Elsevier, Amsterdam 2005)

17.33. P. Phillips, P. Grother, R. Micheals, D. BoneBlackburn, E. Tabassi, M. Bone: Facial recognition vendor test 2002, Evaluation report, March 2003, available online at http://www.frvt.org/

17.34. D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, A.K. Jain: FVC2004: Third fingerprint verification competition, Proc. 1st Int. Conference on Biometric Aunthentication, Vol. 3072 (2004) pp. 1–7

17.35. F. Sufi, S. Mahmoud, I. Khalil: A New Obfuscation Method: A Joint Feature Extraction & Corruption Approach, 5th Int. Conference on Information Technology and Application in Biomedicine, Shenzhen, China, May (2008)

17.36. R. Poli, S. Cagnoni, G. Valli: Genetic Design of Optimum Linear and Nonlinear QRS Detectors, IEEE Trans. Biomed. Eng. **42**(11), 1137–1141 (1995)

17.37. T.H. Linh, S. Osowski, M. Stodolski: On-line heart beat recognition using hermite polynomials and neuro-fuzzy network, IEEE Trans. Instrum. Meas. **52**(4), 1224–1231 (2003)

17.38. F. Sufi, S. Mahmoud, I. Khalil: A Wavelet based Secured ECG Distribution Technique for Patient Centric Approach, 5th Int. Workshop on Wearable and Implantable Body Sensor Networks, Hong Kong, China (2008)

The Authors

Fahim Sufi is an analyst with Office of Health Information System, Department of Human Services. Apart from serving the Governmental agencies, he has actively worked with private health informatics sectors such as McPherson Scientific Pty Ltd., Australia. He is also pursuing his PhD degree from RMIT University, Melbourne. He has many publications in journals, at international conferences, and book chapters. He has 7 years of industry experience in software design and development and 5 years of research experience in biomedical/health informatics.

Fahim Sufi
School of Computer Science and IT
RMIT University, Melbourne 3001, Australia
fahim.sufi@student.rmit.edu.au

Ibrahim Khalil is a senior lecturer in the School of Computer Science & IT, RMIT University, Melbourne, Australia. Ibrahim completed his PhD in 2003 from University of Berne, Switzerland. He has several years of experience in Silicon Valley based companies working on large network provisioning and management software. He also worked as an academic in several research universities. Before joining RMIT, Ibrahim worked for EPFL and University of Berne in Switzerland and Osaka University in Japan. Ibrahim's research interests are quality of service, wireless sensor networks and remote health care.

Ibrahim Khalil
School of Computer Science and IT
RMIT University
Melbourne 3001, Australia
ibrahimk@cs.rmit.edu.au

Jiankun Hu obtained his Masters Degree from the Department of Computer Science and Software Engineering of Monash University, Australia; PhD degree from Control Engineering, Harbin Institute of Technology, China. He has been awarded the German Alexander von Humboldt Fellowship working at Ruhr University, Germany. He is currently an Associate Professor at the School of Computer Science and IT, RMIT University. He leads the Networking Cluster within the Discipline of Distributed Systems and Networks. Dr. Hu's current research interests are in network security with emphasis on biometric security, mobile template protection and anomaly intrusion detection. These research activities have been funded by three Australia Research Council (ARC) Grants. His research work has been published on top international journals.

Jiankun Hu
School of Computer Science and IT
RMIT University
Melbourne 3001, Australia
jiankun.hu@rmit.edu.au