

Efficient and Secured Wireless Monitoring Systems for  
Detection of Cardiovascular Diseases

A thesis submitted for the degree of  
Doctor of Philosophy

Fahim Sufi, B Comp Sc, M Eng,  
School of Computer Science and Information Technology,  
College of Science, Engineering and Health (SEH),  
RMIT University,  
Melbourne, Victoria, Australia.

31 March, 2011

## **Declaration**

I certify that except where due acknowledgement has been made, the work is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program; any editorial work, paid or unpaid, carried out by a third party is acknowledged; and, ethics procedures and guidelines have been followed.

Fahim Kamal Sufi

School of Computer Science and Information Technology

RMIT University

31 March, 2011

## Acknowledgments

I would like to thank my parents for encouraging me towards the doctoral thesis from my very childhood and providing me with the best education. My previous as well as present educational marvel is the generous contribution of my mother's countless efforts in arranging quality education for me.

Being a full time Analyst for the Office of Health Information System, Department of Health, Victorian Government and being a part time Computer Science & Information Technology, RMIT University PhD candidate, I did not have the minimal time for my family. Therefore, I want to thank my wonderful wife, daughter and parent in laws for allowing me to dedicate my family time towards my research work.

I would like to offer my ample gratitude to my supervisors Dr. Ibrahim Khalil and Prof. Zahir Tari for their valuable guidance through-out this research work. Dr. Ibrahim spent several nights at RMIT University (sparing his family time) assisting me with my research work. I would also like to extend my appreciation to Dr. John Fang and Prof Irena Cosic for supporting this research at the initial phase.

Moreover, I would like to thank Dr. S. S. Mahmood (Future Fibre Technologies) for his generous guidance on different signal processing techniques. In addition, Dr. A. Mahmood of School (of CS & IT, RMIT University) extended his expertise in data mining techniques for this research work and therefore deserves my sincere appreciation.

Furthermore, I would like thank Associate Prof. Jiankun Hu, for sharing his broad expertises in biometrics and security. Lastly, Prof. Ibrahim Habib offered his assistance in editorial and review works on different publications.

This work was supported by an Australian Post Graduate Award (APA), a Victorian Government Information & Communication Technology (ICT) Post Graduate Research Scholarship (Top up), an ECR Grant, School of Electrical & Computer Engineering and School of Computer Science & Information Technology.

## Credits

Portions of the material in this thesis have previously appeared in the following publications:

1. F. Sufi, Q. Fang, I. Khalil, and S. S. Mahmoud, Novel Methods of Faster Cardiovascular Diagnosis in Wireless Telecardiology, *IEEE Journal on Selected Areas in Communications*, Vol. 27, No. 4, pp. 537-552, May. 2009
2. F. Sufi and I. Khalil, Diagnosis of cardiovascular abnormalities from Compressed ECG: A Data Mining based Approach, *IEEE Transaction in Information Technology in Biomedicine*, Vol. 15, No. 1, pp. 33 - 39, Jan. 2011
3. F. Sufi and I. Khalil, Enforcing Secured ECG Transmission for realtime Telemonitoring: A Joint Encoding, Compression, Encryption Mechanism, *Security and Communication Networks*, Wiley InterScience Vol. 1, No. 5, pp. 389-405, 2008
4. F. Sufi and I. Khalil, A New Feature Detection Mechanism and Its Application in Secured ECG Transmission with Noise Masking, *Journal of Medical Systems (Springer)*, Vol. 33, No. 2, Page 121-132, Apr. 2009
5. F. Sufi, S. Mahmoud and I. Khalil, A Novel Wavelet Packet based Anti Spoofing Technique to Secure ECG Data, *International Journal of Biometrics*, Vol. 1, No.2, pp. 191 - 208, 2008
6. F. Sufi, I. Khalil and I. Habib, Polynomial Distance Measurement for ECG based Biometric Authentication, *Security and Communication Networks*, Wiley InterScience, Vol. 3, No. 4, pp. 303-319, Jul. 2010

7. F. Sufi, I. Khalil, A. Mahmood, Compressed ECG Biometric: A Fast, Secured and Efficient Method for Identification of CVD Patient, *Journal of Medical Systems*, DOI <http://dx.doi.org/10.1007/s10916-009-9412-4>, 2010 (In Press)
8. F. Sufi, I. Cosic and Q. Fang, A mobile phone based remote patient assessment system, *International Journal of Cardiovascular Medicine*, Vol. 9 (Supplement), pp 8-9, 2008
9. F. Sufi, I. Khalil and J. Hu, ECG based biometric: the next generation in Human Identification, *Handbook on Information & Communication Security*, Book Edited by: P. Stavroulakis, Springer, DOI 10.1007/978-3-642-04117-4, 2010, pp. 309-331
10. F. Sufi and I. Khalil, Faster person identification using compressed ECG in time critical wireless telecardiology applications, *Journal of Network and Computer Applications* (Elsevier), Vol. 34, No. 1, pp. 282-293, Jan. 2010
11. F. Sufi and A. Mahmood and I. Khalil, A clustering based system for instant detection of cardiac abnormalities from compressed ECG, *Expert Systems with Applications* (Elsevier), Vol. 38, No. 5, pp. 4705-4713, 2010
12. F. Sufi, F. Han, I. Khalil, J. Hu, A chaos-based encryption technique to protect ECG packets for time critical telecardiology applications, *Security and Communication Networks*, DOI: 10.1002/sec.226, 2010 (Published Online and In Press)
13. F. Sufi, I. Khalil and Ibrahim Habib, Cardioids-based Faster Authentication and Diagnosis of Remote Cardiovascular Patients, *Security and Communication Networks* (Wiley Interscience), 2010 (in Press)

14. F. Sufi and I. Khalil, Efficient Transmission in Telecardiology, Mobile Web 2.0: Developing and Delivering Services to Mobile Phones (CRC Press), Editor: S. Ahson and M. Ilyas, December, 2010
15. F. Sufi and I. Khalil, Secured Transmission & Authentication, Mobile Web 2.0: Developing and Delivering Services to Mobile Phones (CRC Press), Editor: S. Ahson and M. Ilyas, December, 2010
16. F. Sufi and I. Khalil, Efficient Cardiovascular Diagnosis, Mobile Web 2.0: Developing and Delivering Services to Mobile Phones (CRC Press), Editor: S. Ahson and M. Ilyas, December, 2010
17. Q. Fang, F. Sufi and I. Cosic, A Mobile Device Based ECG Analysis System, Data Mining in Medical and Biological Research, Book edited by: E. G. Giannopoulou, ISBN 978-953-7619-30-5, pp. 320, I-Tech, Vienna, Austria, Dec. 2008

# Contents

<b>Abstract</b>	<b>1</b>
<b>1 Introduction</b>	<b>2</b>
1.1 Motivation . . . . .	2
1.2 Objectives and Approach . . . . .	4
1.3 Summary of Contributions . . . . .	9
1.4 Structure of the Thesis . . . . .	10
<b>2 Compression of ECG</b>	<b>15</b>
2.1 Why ECG Compression is Necessary in Wireless Telecardiology? . . . . .	16
2.2 Background on ECG Features . . . . .	17
2.3 Background and Related Works on ECG Compression . . . . .	19
2.4 Why a New ECG Compression is Required? . . . . .	23
2.5 The Proposed Compression Method . . . . .	26
2.5.1 Generic Framework of the Proposed Compression Mechanism . . . . .	28
2.5.2 ECG Compression using ASCII Character Set . . . . .	33



2.5.3	Decompression in Doctor's Mobile . . . . .	38
2.5.4	Compression using a User Defined Character Set . . . . .	41
	Message Format . . . . .	42
2.6	Experimental Results . . . . .	44
2.6.1	Number of Operations per Second (NOp/s) Comparison . . . . .	44
	ZOP Method . . . . .	46
	SAPA Method . . . . .	46
	Peak Method . . . . .	46
	Proposed Method . . . . .	47
2.6.2	Compression and Decompression Time Comparison . . . . .	47
2.6.3	Compression Ratio Comparison . . . . .	49
2.6.4	Realtime performance measurement . . . . .	50
2.7	Discussion: Further Enhancement of the Compression Ratio . . . . .	51
2.8	Conclusion . . . . .	53
<b>3</b>	<b>ECG based Biometric Authentication</b>	<b>64</b>
3.1	Related Works on ECG based Biometric . . . . .	66
3.2	Challenges Faced by Existing ECG based Biometric . . . . .	68
3.3	Stages of Biometric Systems . . . . .	72
3.4	Types of ECG Biometric . . . . .	73
3.5	Weighted Signal Processing (WSP) Approach . . . . .	74
3.6	Polynomial Distance Measurement (PDM) . . . . .	78
3.6.1	System & Method for PDM Biometric . . . . .	81

ECG Feature Extraction . . . . .	82
Coefficient Generation for PDM . . . . .	84
Polynomial Distance Measurement (PDM) Process . . . . .	86
3.6.2 Experimentation & Results for PDM . . . . .	88
3.6.3 An Implementation Scenario . . . . .	98
3.7 Direct Approach on Compressed ECG . . . . .	100
3.7.1 System Design for Direct Approach on Compressed ECG . . . . .	102
3.7.2 An Algorithm for Biometric Feature Creation . . . . .	109
3.7.3 An Algorithm for Biometric Feature Matching . . . . .	111
3.7.4 Discussion . . . . .	113
3.8 Data Mining Methods on Compressed ECG . . . . .	117
3.8.1 Architecture of the Proposed Patient Identification System . . . . .	121
3.8.2 Training of the Proposed Model . . . . .	122
Testing the Identification Model with Compressed Recognition ECG .	126
3.8.3 Experimentation and Results . . . . .	129
Data Collection . . . . .	129
ECG Compression . . . . .	132
Frequency Calculation . . . . .	132
Attribute Selection . . . . .	136
Clustering . . . . .	138
3.9 Performance Comparison . . . . .	138
3.9.1 Misclassification Rate . . . . .	140

3.9.2	Template Size . . . . .	140
3.9.3	Computational Cost . . . . .	144
3.9.4	Conclusion . . . . .	145
<b>4</b>	<b>Securing the ECG</b>	<b>147</b>
4.1	Why Do We Need Secured ECG Transmission? . . . . .	149
4.2	Securing the ECG: Encryption, Obfuscation/ Anonymization . . . . .	152
4.3	Joint Encoding, Compression and Encryption . . . . .	153
4.3.1	2 Phase Encryption-Compression . . . . .	155
4.3.2	2 Phase Compression-Encryption . . . . .	157
4.3.3	3 Phase Encoding-Compression-Encryption . . . . .	159
4.3.4	Analysis of Performance . . . . .	160
4.3.5	Deployment of 3 Phase Encoding-Compression-Encryption Mechanism on the Mobile Platform . . . . .	162
	Deployment with .Net Compact Framework . . . . .	162
	Deployment with Java 2 Micro Edition . . . . .	163
4.3.6	System Architecture for Joint Encoding, Compression & Encryption .	163
	Secured Acquisition Device . . . . .	164
	Secured Mobile Phone . . . . .	166
	Central Sever (CS) . . . . .	167
4.3.7	Discussion-Security Strength for Joint Encoding, Compression & En- ryption . . . . .	169
4.4	Wavelet based Anonymization Technique . . . . .	171

4.4.1	Introduction - Discrete Wavelet based Anonymization . . . . .	171
4.4.2	System & Methodology for Discrete Wavelet based Anonymization . .	172
	Method 1: Discrete Wavelet based Anonymization . . . . .	173
	Method 2: Discrete Wavelet based Anonymization . . . . .	174
4.4.3	Results and Discussion for Discrete Wavelet based Anonymization . .	175
4.4.4	Wavelet Packet based Anonymization . . . . .	176
	System Overview for Wavelet Packet based Anonymization . . . . .	178
	Implementation of Wavelet Packet based Anonymization . . . . .	183
	Results for Wavelet Packet based Anonymization . . . . .	184
4.5	ECG Obfuscation with Noise . . . . .	186
4.5.1	System & Method of ECG Obfuscation with Noise . . . . .	190
	Selection of Optimal Feature Detection Algorithm . . . . .	191
4.5.2	Key used in ECG Obfuscation & Reconstruction . . . . .	199
4.5.3	ECG Obfuscation Process . . . . .	200
4.5.4	ECG Reconstruction Process . . . . .	203
4.5.5	Experimental Results for ECG Obfuscation . . . . .	207
4.6	Conclusion . . . . .	211
<b>5</b>	<b>Efficient Cardiovascular Diagnosis</b>	<b>219</b>
5.1	ECG Diagnosis from plain ECG . . . . .	221
5.1.1	Direct Approach . . . . .	221
5.1.2	Transformational Approach . . . . .	223
5.1.3	Intelligent Approach . . . . .	224

5.2	ECG Diagnosis from compressed ECG . . . . .	224
5.2.1	Instant Detection Approach . . . . .	227
5.2.2	Direct Approach . . . . .	234
	Method Description . . . . .	234
	Cardiovascular Abnormality Detection . . . . .	238
	Comparison Result . . . . .	243
5.2.3	Intelligent Approach . . . . .	246
	Architecture of the Proposed Disease Identification System . . . . .	250
5.2.4	Training of the Proposed Model . . . . .	254
	Character Frequency Calculation . . . . .	254
	Attribute subset selection . . . . .	255
	Automatic learning of normal and abnormal patterns using clustering of compressed ECG features . . . . .	257
5.2.5	Instant Abnormality Detection from Compressed ECG . . . . .	260
5.3	Results and Discussion . . . . .	260
5.4	Conclusion . . . . .	272
<b>6</b>	<b>Cardiod based Diagnosis and Person Identification</b>	<b>273</b>
6.1	Motivation . . . . .	275
6.2	Architecture & System Design . . . . .	279
6.3	Cardioid based Authentication Mechanism . . . . .	282
6.3.1	Method 1: ECG based Person Identification with Centroid, Four Ex- tremas, Area and Perimeter as template . . . . .	286

6.3.2	Method 2: ECG Biometric based on Centroid and Extreme Points . . .	289
6.3.3	Implementation & Experimentation Results . . . . .	292
	Misclassification Rate . . . . .	295
	Template Size . . . . .	296
	Authentication Time . . . . .	297
6.4	Cardioid based Diagnosis . . . . .	299
6.5	Discussion . . . . .	310
6.6	Conclusion . . . . .	313
<b>7</b>	<b>Conclusion</b>	<b>315</b>
7.1	Summary of Research Progress . . . . .	315
7.2	Limitations and Suggested Future Work . . . . .	319
7.3	Summary . . . . .	321
<b>A</b>	<b>Definitions of Selected Abbreviations</b>	<b>323</b>
	<b>Bibliography</b>	<b>328</b>

# List of Figures

1.1	Mobile phone based ECG telemonitoring and diagnosis. ECG can be compressed and encrypted before transmission to reduce data size and ensure secured-delivery. Authentication at the hospital server makes sure that the right person is provided with the service. . . . .	5
1.2	Overview of this thesis . . . . .	10
2.1	PQRST Signature of an ECG Signal . . . . .	18
2.2	Mobile Phone based ECG Compression . . . . .	28
2.3	Preprocessing Stages of ECG Compression . . . . .	31
2.4	Beats Hidden Within Compressed ECG . . . . .	32
2.5	ECG Samples Compression with the Proposed Method (Example) . . . . .	33
2.6	Step By Step Process Of Encoding (For an Example Case) . . . . .	34
2.7	Our Selection of MMS Character Set for Compressed ECG transmission . . . . .	41
2.8	A Health Message Frame (for SMS) . . . . .	42
2.9	Our Implementation of Mobile Phone based Wireless Telecardiology Application . . . . .	43

2.10	Compression Time Comparison with LZW and Wavelet based Compression Algorithm. 12 MIT-BIH Entries were Randomly Chosen . . . . .	48
2.11	Decompression Time Comparison with LZW and Wavelet based Compression Algorithm. 12 MIT-BIH Entries were Randomly Chosen . . . . .	49
2.12	Compression Time Comparison for LZW Based Compression, Wavelet based Compression and Proposed method for Different File Sizes . . . . .	50
2.13	Decompression Time Comparison for LZW Based Compression, Wavelet Based Compression and Proposed method for Different File Sizes . . . . .	51
2.14	Raising the Compression Ratio with the Proposed Compression Scheme and LZW based Compression Scheme . . . . .	52
3.1	ECG Required for Biometric Recognition . . . . .	65
3.2	The ECG Template (Enrolment ECG) for the First Five Subjects . . . . .	77
3.3	Recognition ECG (for Verification or Identification) for the First Five Subjects	79
3.4	Front End of the Implemented (Using .Net) ECG Biometric System . . . . .	80
3.5	Coefficient Generation Process with Polynomial . . . . .	84
3.6	Polynomial Distance Measurement . . . . .	87
3.7	Polynomial Creation for Subject 5 (for P Wave, T Wave and QRS Complex)	90
3.8	Polynomial Creation for Subject 10 (for P Wave, T Wave and QRS Complex).	91
3.9	Polynomial Creation for Subject 15 (for P Wave, T Wave and QRS Complex).	92
3.10	Polynomial Creation for Subject 20 (for P Wave, T Wave and QRS Complex).	93
3.11	Occurrence of Ectopic Beat in Healthy Subject . . . . .	96
3.12	Misclassification Resulting from not Prioritizing the Distance Measurement .	97



- 3.13 Successful Identification of Subject 12, using PDM + Algorithm 1 + Algorithm 2 97
- 3.14 PDM method for ECG based biometric authentication on a mobile phone  
based cardiovascular condition monitoring scenario (the picture within the  
User Authenticated screen has been intentionally obfuscated for privacy reasons) 100
- 3.15 An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry  
no. 16420. X Axis Shows the Number of Samples and Y Axis Shows the  
Corresponding ECG Amplitude in mV (millivolt) Range . . . . . 103
- 3.16 An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry  
no. 16773. X Axis Shows the Number of Samples and Y Axis Shows the  
Corresponding ECG Amplitude in mV (millivolt) Range . . . . . 103
- 3.17 An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry  
no. 16786. X Axis Shows the Number of Samples and Y Axis Shows the  
Corresponding ECG Amplitude in mV (millivolt) Range . . . . . 103
- 3.18 An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry  
no. 16795. X Axis Shows the Number of Samples and Y Axis Shows the  
Corresponding ECG Amplitude in mV (millivolt) Range . . . . . 104
- 3.19 An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry  
no. 17052. X Axis Shows the Number of Samples and Y Axis Shows the  
Corresponding ECG Amplitude in mV (millivolt) Range . . . . . 104
- 3.20 An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry  
no. 17453. X Axis Shows the Number of Samples and Y Axis Shows the  
Corresponding ECG Amplitude in mV (millivolt) Range . . . . . 104

3.21 An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry no. 16265 (used as Enrolment Data). X Axis Shows the Number of Samples and Y Axis Shows the Corresponding ECG Amplitude in mV (millivolt) Range105

3.22 An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry no. 16265 (used as Recognition Data). X Axis Shows the Number of Samples and Y Axis Shows the Corresponding ECG Amplitude in mV (millivolt) Range105

3.23 Two Overlapped ECG Segments of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry No. 16265. X Axis Shows the Number of Samples and Y Axis Shows the Corresponding ECG Amplitude in mV (millivolt) Range . . . . . 105

3.24 Compressed ECG Segment of nsrdb Entry 16420 (of Figure 3.15) . . . . . 106

3.25 Compressed ECG Segment of nsrdb Entry 16773 (of Figure 3.16) . . . . . 106

3.26 Character Frequency of Compressed ECG Segment in Figure 3.15. X Axis Shows the Number of Encoding Characters (157 Characters in Total), Y Axis Shows the Corresponding Frequency (or the Number of Occurrence for that Character within a Compressed ECG Packet). . . . . 107

3.27 Character Frequency of Compressed ECG Segment in Figure 3.16. X Axis Shows the Number of Encoding Characters (157 Characters in Total), Y Axis Shows the Corresponding Frequency (or the Number of Occurrence for that Character within a Compressed ECG Packet). . . . . 108

3.28 Overlap of Character Frequency of Compressed ECG Segments in Figure 3.21 and 3.22. X Axis Shows the Number of Encoding Characters (157 Characters in Total), Y Axis Shows the Corresponding Frequency (or the Number of Occurrence for that Character within a Compressed ECG Packet). . . . . 108

3.29 Matching Enrolment Data of 16265, 17453, 17052, 16795, 16786, 16773, 16420 with Recognition Data of 16265. X Axis Represents Different Individual and Y Axis Represents  $\psi$  Value of Equation 3.25. Matching Occurs with the Minimum Value of  $\psi$ . . . . . 114

3.30 Matching Enrolment Data of 16265, 17453, 17052, 16795, 16786, 16773, 16420 with Recognition Data of 16795. X Axis Represents Different Individual and Y Axis Represents  $\psi$  Value of Equation 3.25. Matching Occurs with the Minimum Value of  $\psi$ . . . . . 114

3.31 ECG based Biometric (from Compressed ECG) being used by the Multihop Network Node as well as The Hospital . . . . . 116

3.32 Architecture of the Data Mining based Patient Identification from Compressed ECG . . . . . 119

3.33 A Normal ECG Segment of a Monitored Patient at Instance A (ECG Obtained from CU1 Entry MIT BiH CU Ventricular Tachyarrythmia Database) [Phy, Accessed 2009] . . . . . 120

3.34 Compressed ECG for Figure 3.33 (using Algorithms Presented Earlier in Chapter 2) . . . . . 120

3.35	An Abnormal ECG Segment of the Monitored Patient at Instance A+1 (ECG Obtained from CU1 Entry of MIT BiH CU Ventricular Tachyarrhythmia Database) [Phy, Accessed 2009] . . . . .	121
3.36	Training with Enrolment Data and Testing with Recognition Data . . . . .	123
3.37	157 Character and Numeric Sub Groups (Attributes) used for Generating Compressed ECG (from Plain ECG Signal). Details of this Character Substitution based Compression Techniques have been Described in Chapter 2 . . .	123
3.38	Step by Step Procedure of the Proposed Patient Identification System . . . .	124
3.39	Eight Different ECG Segments for nsrdb Entry 16265 (4 Segments - in First Column) and 16272 (4 Segments - in Second Column)[Phy, Accessed 2009] . .	131
3.40	Eight Different ECG Segments for nsrdb Entry 16265 (4 Segments - in First Column) and 16272 (4 Segments - in Second Column) are Compressed using Compression Algorithm Described in Chapter 2 . . . . .	133
3.41	Frequencies of 157 Characters on the Eight Different ECG Segments for nsrdb Entry 16265 (4 Segments - in First Column) and 16272 (4 Segments - in Second Column)[Phy, Accessed 2009] . . . . .	135
3.42	Frequencies of 16 Selected Characters (or Attributes) for Entry no 16265 . .	137
3.43	Eight Different ECG Segments for nsrdb Entry 16265 (4 Segments - in First Column) and 16272 (4 Segments - in Second Column)[Phy, Accessed 2009] . .	137
4.1	Typical Realtime Telemonitoring Scenario . . . . .	150
4.2	Possible Attack points to Acquire Recognition ECG for Replay Attack . . . .	151
4.3	Transformation of the ECG with Proposed Encoding Method . . . . .	155

4.4	Arrangements of Encoding, Compression and Encryption (a) 2 Phase Encryption-Compression using existing encryption and compression techniques (b) 2 Phase Compression-Encryption using existing compression and encryption techniques (c) 3 Phase Encoding-Encryption-Compression using the proposed encoding and existing compression-encryption techniques. . . . .	156
4.5	Time Requirement for 3 Phase Encoding-Compression-Encryption Mechanism on .Net Based Smart Device Platform (Pocket PC 2003 Device) . . . . .	162
4.6	Time Requirement for 3 Phase Encode-Compress-Encrypt Mechanism on J2ME based MIDP (on CLDC) Platform . . . . .	163
4.7	Time Distribution of 3 Phase Encoding-Compression-Encryption on HP iPAQ 6365 . . . . .	164
4.8	System Architecture of 3 Phase Encoding-Compression-Encryption Mechanism	165
4.9	Communication Protocol Among Acquisition Device, Mobile Phone and Central Server . . . . .	168
4.10	Securing ECG with Wavelet Decomposition and Partial Encryption . . . . .	173
4.11	Original ECG Signal and Newly Constructed Trimmed ECG Signal with Node (3, 0) & (3, 1) Removed . . . . .	174
4.12	Removed (Selected for Encryption) Coefficients for Method 1 . . . . .	175
4.13	Original ECG Signal and Reconstructed ECG Signal with Node (3,0), (3,1) & (2,1) Removed . . . . .	176
4.14	Removed (Selected for Encryption) Coefficients for Method 2 . . . . .	177
4.15	Anti Spoofing to Resist Illegal Capture of the Recognition ECG . . . . .	178

4.16	The Proposed Wavelet Packet based ECG Anonymization Mechanism . . . .	184
4.17	The Wavelet Packet Based ECG Reconstruction Mechanism Performed by Authorized Personnel . . . . .	185
4.18	Wavelet Coefficients for Subject 1 . . . . .	186
4.19	Anonymized ECG for the First Subjects . . . . .	187
4.20	Key and Obfuscated ECG Distribution . . . . .	190
4.21	Block Diagram of ECG Obfuscation & Reconstruction Process . . . . .	191
4.22	Original ECG Signal . . . . .	193
4.23	Feature Template to be used for Feature Extraction . . . . .	194
4.24	Measurement of Cross Correlation ( $r_{cc}$ ) for Detection of P wave, QRS Complex and T Wave using CC Method 1 . . . . .	195
4.25	Measurement of Cross Correlation ( $r_{cc}$ ) for Detection of P wave, QRS Complex and T Wave using CC Method2 . . . . .	196
4.26	Detection of P wave, QRS Complex and T wave with Percentage of Similarity	197
4.27	Key Composition for ECG obfuscation & Reconstruction . . . . .	201
4.28	Details of Obfuscating ECG . . . . .	204
4.29	Details of Reconstructing ECG . . . . .	205
4.30	Noise for P wave, QRS complex and T wave . . . . .	209
4.31	Noised ECG signal . . . . .	210
4.32	Implementation of detection and obfuscation on mobile phone . . . . .	211
5.1	Cardiovascular Diagnosis on Mobile Phone . . . . .	220

5.2	Implementation of Direct Methods for Diagnosing ECG on J2ME Supported Mobile Phones . . . . .	223
5.3	Implementation of Direct Methods for Diagnosing ECG on .Net Supported PDAs / Smart Phones . . . . .	224
5.4	The Proposed Cardiac Diagnosis System . . . . .	227
5.5	Compressed ECG Packet . . . . .	231
5.6	The Relationship between Heart Rate and Compression Ratio . . . . .	231
5.7	The Distance between the Estimated HR and Original HR . . . . .	231
5.8	Heart Beat Detection from Compressed ECG . . . . .	235
5.9	Initiation of Stall after Successful Beat Detection . . . . .	236
5.10	Beats Hidden within Compressed ECG. The Shaded Segments Represented by $V$ Character Set, Where Each Segment Indicates Width of a Whole QRS Complex. . . . .	237
5.11	RR Interval for an MITBIH Entry. The RR Intervals Values Calculated by both the Methods are Almost Similar. However, the Proposed Method is a Bit Time Shifted from the RRs Calculated by ABT. Most Importantly, in Terms of Accuracy, this Lagging does not have any Adverse Affect, since the Time Shifted Delay (almost constant) is Added to Each of the RR Intervals. . . . .	240
5.12	Wide QRS Detected with Wider Buffer Size (Higher Values of $N_v$ as per Fact 2)	242
5.13	Two Different Scenarios of a Mobile Phone based Wireless Telecardiology System	245
5.14	Architecture of the Data Mining based Compressed ECG Diagnosis System .	251

5.15	A normal ECG Segment of a Patient (a Random CU1 Entry of MIT BiH CU Ventricular Tachyarrythmia Database) . . . . .	251
5.16	Initiation of Abnormality (Ventricular Tachyarrythmia) with the ECG Segment for CU1) . . . . .	251
5.17	An Abnormal (Ventricular Tachyarrythmia) ECG Segment of a Patient (CU1)	252
5.18	Compressed ECG for Fig. 5.15 (Normal ECG), Fig. 5.16 (Normal and Abnormal) and 5.17 (Abnormal ECG) . . . . .	252
5.19	157 Characters and Numeric Sub Groups (Attributes) used for Generating Compressed ECG (from Plian ECG Signal). Details of this Character Substitution based Compression Techniques have been Described in Chapter 2 . . .	254
5.20	Step by step procedure of the proposed cardiac abnormality detection technique	255
5.21	20 Randomly Selected ECG Segments for CU1 Entry (from CU Ventricular Tachyarrythmia - MIT BIH) . . . . .	262
5.22	Frequency Distribution of the 20 Randomly Selected ECG Segments for CU1 Entry (of Fig. 5.21). Boxed Region Shows high Frequencies of Attribute 115 to 131 Denoting Abnormality from the Compressed ECG. . . . .	263
5.23	Normal and abnormal cluster means . . . . .	265
5.24	Segregation of normal and abnormal ECG (in two different clusters) . . . . .	271
5.25	Suitability of different algorithms in mobile platform . . . . .	271
6.1	Architecture of Mission Critical Cardiovascular Abnormality Alerting System	280
6.2	Two Types of Authentication Mechanism for Cardiovascular Patient . . . . .	281
6.3	A typical Cardioid . . . . .	281



6.4	Matching Process (Method 1 as an Example) in ECG Cardioid based Biometric	283
6.5	3 Steps in Biometric Template Creation for Patient Authentication . . . . .	286
6.6	Cardioid based Patient Authentication and Diagnosis System (Desktop Im- plementation) . . . . .	286
6.7	Block Diagram of ECG based Person Identification with Centroid, Area and Perimeter as Template (Method 1) . . . . .	287
6.8	Block Diagram of ECG based Person Identification with Centroid and Four Extremas . . . . .	290
6.9	Calculation of Centroid and Four Extremas for QRS Complex, T Wave and P Wave . . . . .	290
6.10	Mobile Phone Implementation of Cardioid (for ECG Abnormality Diagnosis within Doctor's Mobile Phone) Running in Pocket PC Emulator under MS Visual Studio 2005. . . . .	298
6.11	Deployment of Cardioid based Patient Authorization and Diagnosis on HP 912 Business Messenger Mobile Smartphone . . . . .	300
6.12	Occurrence of Ventricular Beat from MIT-BIH Supraventricular Arrhythmia Database (svdb) Entry No. 803 . . . . .	300
6.13	Cardioid Drawn from the Entire ECG Strip Presented in Figure 6.12 (from MIT-BIH Supraventricular Arrhythmia Database (svdb) Entry No. 803) . . .	301
6.14	Occurrence of Ventricular Fibrillation from CU Ventricular Tachyarrhythmia Database (cudb) Entry No. 01 . . . . .	301
6.15	Drawing of ECG Curve in Multiple Screens of a Mobile Phone . . . . .	301

6.16 Centroid using the Normal Beats of Figure 6.12 . . . . .	302
6.17 Centroid using the Abnormal Beats (i.e. During the Onset of the Ventricular Beat) of Figure 6.12 . . . . .	303
6.18 Centroid using the Normal Beats of Figure 6.14 . . . . .	303
6.19 Centroid using the Abnormal Beats of Figure 6.14 (during Occurrence of Ven- tricular Fibrillation) . . . . .	304
6.20 Cardioid Drawn from the Four Normal Beats of Figure 6.14 . . . . .	306
6.21 Cardioid Drawn After the Occurrence of VF in Figure 6.14 . . . . .	306
6.22 Cardioid Drawn from the Entire ECG Trace Presented in Figure 10 . . . . .	307
6.23 Occurrences of Ectopic beats / premature beats (ectopic beats marked with red boxes and a suspected beat marked with blue box) from AHA Database entry no. 01 . . . . .	308
6.24 Cardioid Drawn from the Entire ECG Strip Presented in Figure 6.23 . . . . .	309
6.25 Beat Alignment in time Series Domain . . . . .	311

# List of Tables

2.1	ECG Features Related to P Wave, QRS Complex and T Wave . . . . .	18
2.2	Comparison of RAM and CPU Speed Among Mobile Phone, Implantable De- vices and PC . . . . .	24
2.3	Unsuitable Criteria for Mobile Phone based Realtime ECG Compression . . .	55
2.4	Experimentation with Different Entries of MIT-BIH . . . . .	57
2.5	Comparison of the Proposed Method with Other Direct ECG Compression Algorithms . . . . .	57
2.6	NOp/s Counting of ZOP Method . . . . .	58
2.7	Number of Operations per Second Counting of SAPA Method . . . . .	59
2.8	NOp per Sec. Counting of Peak Method . . . . .	60
2.9	NOp per Sec. Counting of the Proposed Method . . . . .	61
2.10	Comparison of the Proposed Method with Other Lossless ECG Compression Algorithm . . . . .	62
2.11	Realtime Compression / Decompression Factor for Pocket PC and Smart Phone	62
2.12	Further Compression with LZW based Compression Schemes . . . . .	63

3.1	Variance of Values for PRD, CC and WDM on Different Subjects. <sup>1</sup> = Enrolment ECG and <sup>2</sup> = Recognition ECG. The Enrolment and Recognition ECGs are in Bytes. . . . .	78
3.2	Dissimilarity of Coefficients for P Wave Across 5 Subjects . . . . .	89
3.3	Dissimilarity of Coefficients for T Wave Across 5 Subjects . . . . .	89
3.4	Dissimilarity of Coefficients FOR QRS Complex Across 5 Subjects . . . . .	94
3.5	Similarity of P Wave Coefficients for an Individual Across all the ECG Features	94
3.6	Similarity of T Wave Coefficients for an Individual Across all the ECG Features	94
3.7	Similarity of QRS Complex Coefficients for an Individual Across all the ECG Features . . . . .	95
3.8	Standard Deviations of the ECG Biometric Template Values (Templates for $\Lambda_{16265E}$ ) . . . . .	112
3.9	ECG Segments Collection from NSRDB, Entry No. and Segments Obtained. Four ECG Segments were Obtained for Each of the Entries (i.e. 36 ECG Segments Obtained for our Experimentation) . . . . .	130
3.10	Average Frequencies of the 16 Selected Attributes for the Nine Entries (or Patient). ECG Segments Collected from Public Database [Phy, Accessed 2009]	136
3.11	Cluster Means (Denoted by M) and Deviations (Denoted by S) for all the 9 Clusters, Against Each of the 16 Selected Attributes) . . . . .	139
3.12	Misclassification Rate for PRD, CC, WDM and the Proposed ECG Biometric from Compressed ECG (Applying Data Mining Agent (DMA) . . . . .	141
3.13	FRM and FNRR Across Different Modalities . . . . .	141

3.14	Comparison of Template Sizes . . . . .	143
3.15	Comparison of Number of Operations (NOP) for PRD, CC, WDM and PDM	144
4.1	Results for Securing ECG with 2 Phase Compression-Encryption Technique .	157
4.2	Results for Securing ECG with 2 Phase Encryption-Compression Technique .	158
4.3	Results for Securing ECG with 3 Phase Encoding-Compression-Encryption Mechanism . . . . .	214
4.4	Results of Performance Comparison among Three Joint Compression Encryp- tion Mechanisms . . . . .	215
4.5	Notations for Security Strength of the Scheme . . . . .	215
4.6	Reduction of ECG File Size for Method 1 & 2. M1 and M2 Denotes Method 1 and Method 2. . . . .	216
4.7	Performance Metrics for the Proposed ECG Anonymization Mechanism. Cf. Size, Comp. Cf. Size and Encr. Cf. Size are in Bytes. . . . .	216
4.8	Definition of Mathematical Symbols for ECG Obfuscation . . . . .	217
4.9	Definition of Mathematical Symbols for ECG Reconstruction . . . . .	218
5.1	The Relationship between CR and Encoding Types . . . . .	228
5.2	Disease Detection with Algorithms . . . . .	239
5.3	Comparison of the proposed HR detection method with ABT, SDBT and FDBT.	244
5.4	Delay Involved in Different Telecardiology Scenarios. All the values of times are in seconds. The ECG Segments collected are for the duration of 1 minute (21600 samples/ECG segment). . . . .	247

5.5	Selected Characters (First Half Attributes) and their Respective Frequencies in Compressed ECGs (Normal) for 13 Different Instances . . . . .	266
5.6	Selected Characters (Last Half Attributes) and their Respective Frequencies in Compressed ECGs (Normal) for 13 Different Instances . . . . .	267
5.7	Selected Characters (First Half Attributes) and their Respective Frequencies in Compressed ECGs (abnormal) for 7 Different Instances . . . . .	268
5.8	Selected Characters (Last Half Attributes) and their Respective Frequencies in Compressed ECGs (abnormal) for 7 Different Instances . . . . .	269
5.9	$A_j$ , $B_j$ and $S_j$ values for the 20 ECG segments . . . . .	270
6.1	The Difference in ECG Feature Waves between Two Different Individuals . .	293
6.2	Uniqueness of Cardioids of Various MIT_BIH Entries . . . . .	295
6.3	Misclassification Rate for PRD, CC, WDM and PDM . . . . .	295
6.4	FRM and FNMR Accross Different Modalities . . . . .	296
6.5	Comparison of Template Sizes . . . . .	297
6.6	Comparison of Cardioid based Automated Authentication Technique Against Username / Password based Authentication (Times are in Seconds. Cardioid Biometric were Performed on Randomly Selected MIT BIH Entries) . . . . .	298
6.7	Execution Time (in seconds) on HP iPAQ 912 Business Messenger for Car- dioid, First Derivative based Technique, Second Derivative based Technique and Threshold based Technique . . . . .	309
7.1	Summary of research progress . . . . .	316

# Abstract

Cardiovascular Disease (CVD) is the number one killer for modern era. Majority of the deaths associated with CVD can entirely be prevented if the CVD struck person is treated with urgency. This thesis is our effort in minimizing the delay associated with existing tele-cardiology application. We harnessed the computational power of modern day mobile phones to detect abnormality in Electrocardiogram (ECG) and if abnormality is detected, our innovative ECG compression algorithm running on the patient's mobile phone compresses and encrypts the ECG signal and performs efficient transmission towards the doctors or hospital services. After receiving the compressed ECG packets the doctor's mobile phone or the hospital server authenticates the patient using our proposed set of ECG biometric based authentication mechanisms. Once authenticated, the patients are diagnosed with our faster ECG diagnosis algorithms. In a nutshell, this thesis contains a set of algorithms, that can save a CVD affected patient's life by harnessing the power of mobile computation and wireless communication.

# Chapter 1

## Introduction

### 1.1 Motivation

Coronary Heart Disease (CHD) and stroke being the top most killer diseases in Australia [Acc, Accessed 2008], more people are diagnosed with Cardiovascular (CVD) related disorders. Among Australians about 25 % would be dead within an hour of their first symptom of heart attack and 40 % will be dead within a year [Acc, Accessed 2008]. However, medical research suggests that if the CVD attacked patient is provided with faster treatment, he or she may survive longer [Luca et al., 2004]. According to [Luca et al., 2004], every second counts towards longevity of the CVD attacked patient, since cardiac cell damage is a completely irrecoverable process. Cardiologists state 'time is muscle' regarding cardiac cell damage. Therefore, to reduce the risk of patient death, hospitals arrange all the necessary facilities in providing early detection and faster care to the CVD patients [Bradley et al., 2006; Otsuka et al., 2009; Sillesen et al., 2008; Ortolani et al., 2007].

Today we are living in the era of mobile phone and faster communication. Modern mobile



phone has limited computational power, on which we execute miniature programs, audio / video applications, games etc [Yuan, c2004]. Harnessing the computational intelligence of mobile phone's processor (computational resource), we may run intelligent life saving programs for CVD patients or even for normal people (having a chance possible CVD anomaly) for wellness monitoring. Providing realtime health monitoring services has recently been addressed by several research groups [Lee et al., 2007; Hung and Zhang, 2003; Zhou et al., 2005; Gao et al., 2005; Jasemian and Arendt-Nielsen, 2005; Kim et al., 2006]. However, none of these presents a comprehensive version of tele-health (or wireless health) platform that can be readily adopted and commercialized.

The existing tele-health platforms have not been accepted well because of inefficient transmission, primitive authentication mechanism, security vulnerabilities, and above all slower diagnosis. Since for cardiac health monitoring, faster action is required for saving a patient's life [Luca et al., 2004; Bradley et al., 2006; Otsuka et al., 2009; Sillesen et al., 2008; Ortolani et al., 2007], slower communication and diagnosis are completely undesirable. In addition to faster communication and diagnosis, the medical service providers require establishment of proper authentication mechanism to identify their subscribers (i.e. CVD affected patients / monitored patients). Moreover, security threats must be conquered for protection of patient's privacy.

Thus, providing faster cardiac healthcare toward a CVD affected patient, who is being monitored by mobile computation platform, spurred the initiation of this research work. The entire objective is to save valuable life, with the help of portable computational platforms, like mobile phones and portable Electrocardiogram (ECG) monitoring devices [Ali, Accessed

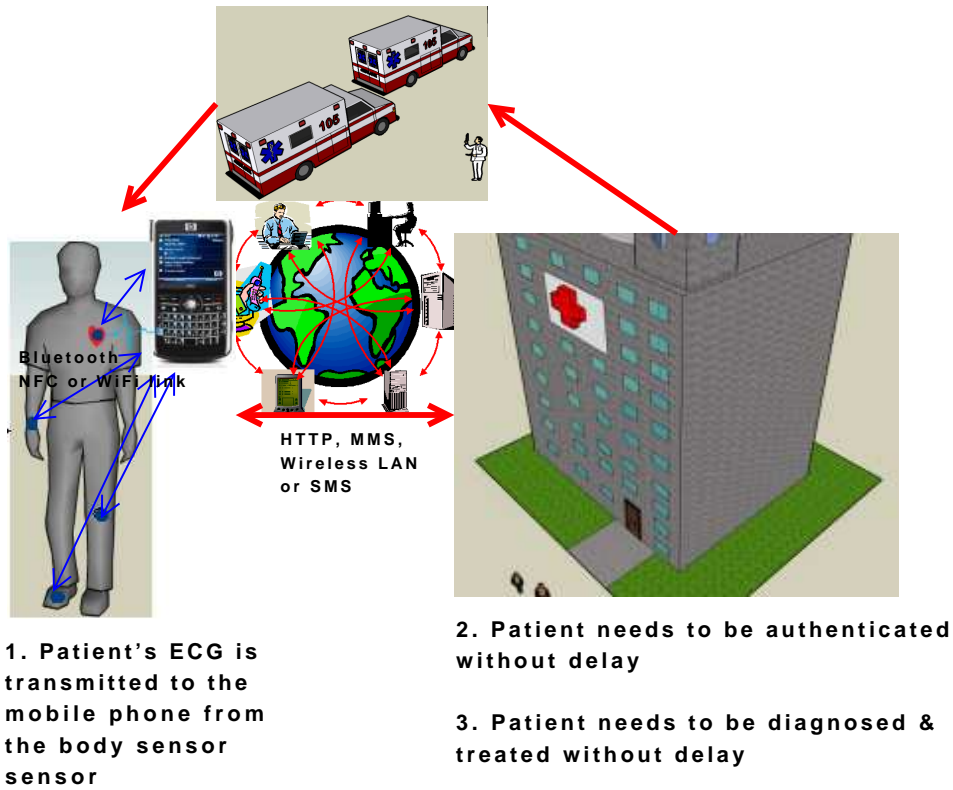
2009].

After the initial literature review, we came up with our own proposed platform that we believe, has the potential of addressing most of the obstacles faced by the existing tele-health applications. As seen from Figure 1.1, the patient is attached with an ECG acquisition device that collects the ECG signal from the patient's body. The collected ECG is continuously transmitted from the body sensor to the patient's mobile phone using Bluetooth protocol. The patient's mobile phone then compresses and encrypts the ECG packets for fast and secured transmission to the hospital or medical servers.

Once the ECG packets are received by the hospital, the hospital may use the ECG packets to authenticate the patient using ECG based biometric techniques. Once the hospital recognizes the patient as a subscriber, the hospital can perform a preliminary detection of CVD with our proposed set of CVD detection techniques. This faster preliminary detection of CVD can determine the serious patients requiring cardiologist's attention.

## 1.2 Objectives and Approach

After the initial literature review within the area of mobile phone based telecardiology application, we found that the existing telemonitoring platforms are more focused towards Cardiovascular (CVD) diagnosis [Lee et al., 2007; Hung and Zhang, 2003; Zhou et al., 2005; Gao et al., 2005] or underlying transmission mechanism [Jasemian and Arendt-Nielsen, 2005; Kim et al., 2006]. Even though there have been a lot of research performed in remote telecardiology diagnosis, hardly any of the previous literatures addressed the necessity of delay minimization within the telecardiology framework. After a person has a heart abnormality,



**ECG packet transmission needs to be fast, secured and efficient**

*Figure 1.1: Mobile phone based ECG telemonitoring and diagnosis. ECG can be compressed and encrypted before transmission to reduce data size and ensure secured-delivery. Authentication at the hospital server makes sure that the right person is provided with the service.*

if that person is not taken to the cardiologist immediately, then his life may be in jeopardy [Luca et al., 2004]. According to literature [Luca et al., 2004], the delay of every second may even shorten the lifespan of a patient having heart attack. The contributions of the existing research [Bradley et al., 2006; Otsuka et al., 2009; Sillesen et al., 2008; Ortolani et al., 2007] were mainly focused on the overall process of mobilizing the patient to the hospital considering ambulance to hospital communication, ECG diagnosis performed within ambulance, electronic transfer of ECG from the ambulance to the hospital etc.

However, to the best of our knowledge, none of these previous researches made any effort in minimizing delay in diagnosis process (i.e. faster algorithms to diagnose cardiovascular diseases) or faster transmission of ECG data. Twelve lead ECG data with 500 Hz sampling frequency along with some other vital signal can easily reach 13 GB per day [Sufi et al., 2006b]. Without efficient transmission mechanism in place, this massive amount of ECG packets can create enormous delay in realtime CVD patient monitoring.

CVD patients are generally subscribed to a hospital, from where they might receive one or more medical services (e.g. on-site cardiologist's visit, ambulance service for critical condition etc.). However, for CVD patients monitored remotely via the mobile phone, the patients must be authenticated before providing them with any services. Unfortunately, very few research articles [Blount et. al., 2007] have addressed this mobile phone based authentication mechanism. The research presented in [Blount et. al., 2007], basically provide manual user name and password based authentication system and at an event of cardiac failure, the CVD patients may be unable to move their fingers for these manual authentication system. This is because, the cardiac arrest may result in the anomaly of Autonomous Nervous System

(ANS) [Kumar et al., 2007], making them unable to move their finger. Therefore, efficient mechanisms for automated authentication of patients need to be thoroughly researched.

Health Insurance Portability and Accountability Act (HIPAA) of United States in 1996 mandates that patient's privacy being protected at all times [Cen, Accessed 2008; Pub, 1996]. Other countries like Taiwan and Australia have similar regulations regarding protection of information [Lee and Lee, 2008; Off, Accessed 2009]. However, none of the existing telecardiology platforms [Lee et al., 2007; Hung and Zhang, 2003; Zhou et al., 2005; Gao et al., 2005; Jasemian and Arendt-Nielsen, 2005; Kim et al., 2006] addressed the issues of secured and efficient ECG transmission mechanism. Without secured ECG transmission the ECG packets can be spoofed by the malicious user. Once the hackers attain the patients ECG signal, they may run detection algorithms [Hamilton and Tompkins, 1986; Friesen et al., 1990; Kumar et al., 2007; Bartolo et al., 2001; Akselrod et al., 2007; Kusumoto, 2009; Clifford et al., 2006] to obtain a patient's private health information. Moreover, using ECG based biometric techniques [Biel et al., 2001; Chan et al., 2008; Wubbeler et al., 2007; Poon et al., 2006; Israel et al., 2005; Irvine et al., 2001; Bui and Hatzinakos, 2008; Kyoso and Uchiyama, 2001; Kyoso, 2003; Shen et al., 2002; Shen, 2005; Shen and Tompkins, 2005; Wang et al., 2008; Hou and Andrews, 1978; Plataniotis et al., 2006; Kanade and Jain, 2005], the hacker can gain access to secured ECG biometric facility. Therefore, serious research requires to be in place, to ensure secured ECG transmission for protecting patient's privacy, as well as for protecting ECG biometric template. These issues that have been neglected by the existing research have motivated us to derive four research questions:

- How to ensure faster and more efficient ECG transmission (with the objective of mini-

## CHAPTER 1. INTRODUCTION

mizing transmission delay)?

- How to perform automated authentication mechanism (with the objective of minimizing the authentication delay)?
- How to establish end to end secured ECG transmission (with the objective of protecting patient's privacy and upholding HIPAA regulations)?
- How to perform faster Cardiovascular Disease (CVD) diagnosis (with the objective of saving patient's life and increasing life span)?

### 1.3 Summary of Contributions

In summary, this thesis contributes the followings:

- *A new wireless telecardiology platform* : We established a new mobile phone based realtime telecardiology application supporting fast and secured ECG transmission along with fast and accurate patient authentication and diagnosis. Our proposed telecardiology application can significantly reduce the threats posed by CVD, which is the number one killer of modern era.
- *An innovative ECG compression algorithm* : We proposed a new lossless ECG compression mechanism that has higher compression ratio, faster execution speed and realtime processing capabilities (detailed in Chapter 2).
- *Novel authentication mechanisms with ECG based Biometric* : We have proposed new techniques of highly accurate ECG based biometric that works on plain ECG. These techniques present the capability of automated CVD patient authentication using patient's ECG signal. Moreover, we have presented new mechanisms of patient identification directly from the compressed ECG. Person identification directly from the compressed ECG has never been reported in earlier literature (detailed in Chapter 3).
- *Innovative algorithms for securing ECG signal and protecting patient's privacy* : We have presented new techniques (ECG encryption with permutation cipher, noise based ECG obfuscation/ anonymization, discrete wavelet based ECG anonymization and wavelet packet based ECG anonymization) for securing ECG signals (detailed in Chapter 4).

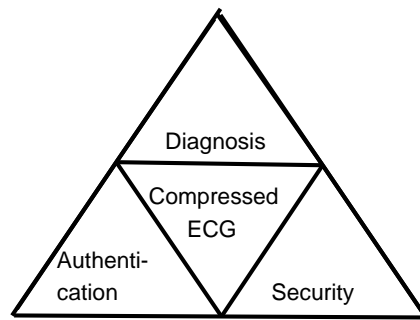


Figure 1.2: Overview of this thesis

- *Novel algorithms for faster CVD diagnosis* : We invented a new set of algorithms that can diagnose CVD directly from the compressed ECG. According to the literature this has never been investigated by previous researchers (detailed in Chapter 5).
- *Cardiod based CVD detection and patient authentication* : Finally, we have designed and developed a completely new cardiod based approach for patient identification and CVD diagnosis. Cardiod is our proposed technique that provides a graphical representation of cardiovascular abnormalities (detailed in Chapter 6).

#### 1.4 Structure of the Thesis

To achieve and document the aim of this research, this thesis is organized in four major sections: compression, automated authentication (with ECG Biometric), secured transmission and faster diagnosis. Figure 1.2 structures the content of the thesis, based on our research objectives.

Chapter 1 establishes the foundations of this research work, by providing a brief description of the problems and challenges incurred in existing wireless telecardiology applications. These problems or challenges provided us the motivation for this research work. Based on the



major challenges, four research questions are raised within this chapter. Lastly, this chapter organizes the thesis, relating each chapter with the objectives and research questions.

Chapter 2 answers the first research question, which is how to achieve faster and more efficient ECG data transmission. Using a completely new ECG compression algorithm, we were able to produce significantly higher level of compression ratio. Unlike the existing ECG compression algorithms [Zhang et al., 2005; Duda et al., 2001; Miaou and Chao, 2005; Rossi et al., 2002; Jalaeddine et al., 1990; Kim et al., 2006; Goudarzi et al., 2004; Uzar and Ider, 2001; Blanchett and Kember, 1998; Zigel et al., 2000a; Hao et al., 2005; Rezazadeh et al., 2005; Miaou and Lin, 2002; Wei et al., 2001; Barlas et al., 1993; Horspool and Windels, 1994; Hamilton and Tompkins, 1991; Moody et al., 1998; Cox and Ripley, 1973; Yuan, 2004; Alesanco et al., 2006; Velasco et al., 2004], our novel ECG compression algorithm is of lower complexity. Therefore, it is highly suitable for mobile phone based remote telecardiology applications, which is the objective of this thesis. According to our experimentations with several existing compression algorithms (both generic compression algorithms as well as specialised ECG compression algorithms), the compression and decompression times of this algorithm is faster than most of the existing methods. Being a faster algorithm with its capacity for achieving higher compression ratio, our proposed compression algorithm entails faster cardiovascular (CVD) patient care. As we had stated earlier, faster patient care is highly desirable for CVD patients, since every second counts towards the mortality [Luca et al., 2004; Otsuka et al., 2009; Sillesen et al., 2008; Ortolani et al., 2007; Bradley et al., 2006].

Chapter 3 presents the answers to the second research question, which is how to perform

faster authentication of the CVD patient. Since each patient receives a set of services (e.g. realtime CVD abnormality detection, on-site cardiologist support, faster ambulance service etc.), the patient must be authenticated by the hospital server before providing any service. We present four different authentication mechanisms, based on ECG based biometric. Among these authentication mechanisms weighted Signal Processing (WSP) Approach and Polynomial Distance Measurement (PDM) Approach are specifically designed for telecardiology applications not utilizing our ECG compression technique [Hung and Zhang, 2003; Blount et al., 2007; Zhou et al., 2005; Jasemian and Arendt-Nielsen, 2005; Lee et al., 2007; Gao et al., 2005; Kim et al., 2006]. On the other hand, for telecardiology applications using our compression algorithm, this chapter presents two different ECG based biometric methodology. Both these methodologies named as Direct Approach and Data Mining based Approach are faster than existing ECG based authentication mechanisms [Biel et al., 2001; Chan et al., 2008; Wubbeler et al., 2007; Poon et al., 2006; Israel et al., 2005; Irvine et al., 2001; Bui and Hatzinakos, 2008; Kyoso and Uchiyama, 2001; Kyoso, 2003; Shen et al., 2002; Shen, 2005; Shen and Tompkins, 2005; Wang et al., 2008; Hou and Andrews, 1978; Plataniotis et al., 2006; Kanade and Jain, 2005]. Apart from being faster, which is directly related to faster CVD patient care (i.e. saving the lives of more CVD patients), our algorithms provide more accurate form of person identification (i.e. lower misclassification, lower False Match Rate, lower False Non-Match Rate) compared to the existing ECG based biometrics.

Chapter 4 describes different methodologies for securing the ECG signal, answering our third research question. The first one is Joint encoding-compression-encryption mechanism. This method is so secured that approximately  $4 \times 18 \times 9.333 \times 10^{970}$  years is required to

compute the full search space with a super computer that can compare a trillion trillion trillion ( $10^{36}$ ) combinations of one ECG segment (comprising 500 ECG samples) per second for ECG morphology matching. The security strength of this mechanism is substantially higher than that of the existing encryption mechanism like, AES or DES. While providing the highest level of security, this algorithm shrinks the file size up to 95% (i.e. 20.06 Compression Ratio), which is highly desirable for realtime telecardiology applications with massive data transmission. Secondly, this chapter illustrates an ECG obfuscation mechanism that can hide the ECG features required for both person identification and CVD disease recognition. Therefore, patient's privacy is protected which is mandated by HIPAA regulations [Cen, Accessed 2008; Off, Accessed 2009; Pub, 1996; Lee and Lee, 2008]. The obfuscated ECG appears as regular ECG, misguiding the Hackers and making conventional hacking utilities useless (since the text is not encrypted; it is rather unencrypted). Lastly, Discrete Wavelet based ECG anonymization technique and Wavelet Packet based ECG anonymization technique are presented. For obfuscation and anonymization techniques, only authorized person with the shared secret key can decrypt the anonymized ECG without any loss of information.

Chapter 5 illustrates innovative algorithms directed towards answering the last research question of faster cardiovascular diagnosis. In this chapter, we segregated the main stream ECG diagnosis algorithms in two types: plain ECG based diagnosis and compressed ECG based diagnosis. For the first category (plain ECG based diagnosis), we implemented a rule based system for identifying heart beats of the CVD patients. We also developed several algorithms that works directly on compressed ECG providing faster patient care.

Chapter 6 presents cardioid based technique for both CVD patient authentication and di-

agnosis. Cardiod based technique is a completely new technique that is specifically designed for mobile phones with limited computational resources. Since the biometric template size is substantially smaller than other existing ECG biometrics, the patient authentication mechanism is more efficient. The CVD disease identification is also very fast since only 5 points (or sample) are used for diagnosis (rather than several hundred samples, used by the existing ECG diagnosis system). Therefore, cardiod based technique answers two of the research questions, namely authentication and diagnosis.

Finally, chapter 7 concludes this thesis with summary of research progress, our core research contributions and suggested future research.

## Chapter 2

# Compression of ECG

This chapter answers our first research question regarding achievement of faster and more efficient ECG transmission. By harnessing the power of a new compression mechanism that can raise the compression ratio to a higher level with minimal computation, we can achieve faster and efficient transmission. The idea is to compress the ECG at patient's side (i.e. on patient's mobile phone), before sending it to the doctor or to the hospital server. The receiver (doctor or the hospital server), on the other hand, needs to quickly decompress the ECG, when necessary. Since both compression and decompression may execute within mobile phone platform (patient's and doctor's) with limited computational resources, the design of the compression algorithm needs special consideration with the objective to minimize the number of operations.

This chapter, therefore, presents a new compression algorithm to compress ECG files in realtime for faster transmission on mobile platform. The proposed compression algorithm, lays the foundation of latter chapters that describe other algorithms (for ECG biometric

based authentication, encryption mechanism, CVD diagnosis etc.), which are based on the compressed ECG signals. At first, the background of the existing compression algorithms is provided. Then, the motivations of compression and the reasons for choosing a new compression algorithm are outlined. Next, the proposed compression algorithm is described in details, with examples for ASCII and MMS character sets. In the results section, performance comparisons were carried out with respect to existing compression methods. Lastly, the discussion section shows how to raise the compression ratio further with Lempel-Ziv-Welch (LZW) based compression before this chapter is concluded.

## 2.1 Why ECG Compression is Necessary in Wireless Telecardiology?

First of all, in a wireless telecardiology application, huge ECG data is transmitted from the patient to the medical server or to the doctors. Transmission and storage of enormous amount of physiological signal impose huge challenges to the research community. To help us understand precisely about how large data we are dealing with, examples from [Sufi et al., 2008c] is necessary. Data volume from a single patient with only few biosignal acquisition devices (ECG, EEG, EMG, SpO2, Accelerometer), can easily reach several GB in 24 hours [Sufi et al., 2008c], in case of continuous monitoring. If a patient with heart abnormality is remotely monitored, then with 12 lead ECG, 10 bit Resolution and 360 Hz Sampling Frequency the data can easily reach up to 2.77 GB in one day. And if we intend to transmit this enormous amount of data using available telecommunication technologies (like, PSTN, GSM, GPRS, 3G etc.), then a dedicated minimum speed of 269 kbps is required

(*Required Transmission Speed* =  $\frac{\text{Size of Data}}{\text{Transmission Time}} = \frac{2.77 \text{ GB}}{24 \text{ Hours}} = 269 \text{ kbps}$ ). Unfortunately,

this type of transmission speed is guaranteed by a very limited number of telecommunication service providers. During this transmission of enormous ECG data, compression technology can be applied for faster transmission on limited bandwidth wireless link. At the end, faster transmission means faster treatment for the patient.

Secondly, some of the messaging protocols like SMS can only allow a limited set of characters or message sizes. For example, SMS can only accommodate a message size of 140 bytes or 160 ( $140 \times \frac{8}{7}$ ) characters. Since each SMS involves cost for the patient, it is imperative to transmit compressed data for economic reasons.

Lastly, compression algorithm also adds value to a realtime telemonitoring scenario by allowing more storage of physiological signals.

## 2.2 Background on ECG Features

The human heart contains four chambers: 2 Atria and 2 Ventricles. The de-oxygenated blood from the body is collected in the right atrium, from where it is pumped to the right ventricle. The right ventricle then pumps the de-oxygenated blood (carbon dioxide saturated) blood to the lungs for gas exchange via diffusion. Within the lungs the blood becomes oxygen rich and from the lungs the oxygenated blood reaches the left atrium. The left atrium forwards the oxygenated blood to the left ventricle, from where the fresh blood is forced to the rest of the body. This whole work flow of circulatory management is controlled by the nervous system. During this process, both the atria contract and relax together followed by the joint ventricular contraction and relaxation.

These mechanical activities of the heart can be efficiently traced by ECG recordings,

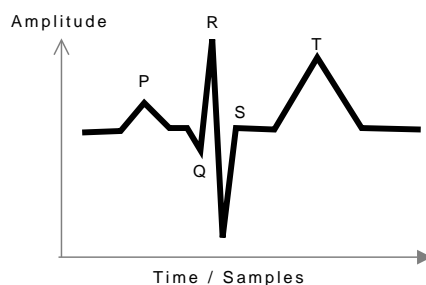


Figure 2.1: PQRST Signature of an ECG Signal

Table 2.1: ECG Features Related to P Wave, QRS Complex and T Wave

P wave duration	QRS complex duration	T wave duration
P wave amplitude	QRS complex amplitude	T wave amplitude
P wave onset slope	Q onset slope	T wave onset slope
P wave offset slope	Q offset slope	T wave offset slope
	R onset slope	
	R offset slope	
	S onset slope	
	S offset slope	

where the electrical activities of heart are depicted. ECG tracing has 3 major waves or complexes that signify atrial and ventricular activities (as seen from Figure 2.1): P wave, QRS complex and T wave. P wave signifies atrial depolarization (equivalence of mechanical atrial contraction), QRS complex represents more vigorous ventricular depolarization (equivalence of mechanical ventricular contraction) and T wave identifies repolarization of the arteries (equivalence of mechanical ventricular relaxation). The electrical activity occurs from atrial repolarization is lost (or superimposed) by the more vigorous (high amplitude) QRS complex, which represents ventricular contraction (mechanical event). Cardiologists have used different features of these feature waves (i.e. P wave, T wave and QRS complex) to assess the condition of heart. Table 2.1 lists some of these features.



### 2.3 Background and Related Works on ECG Compression

Considering the loss of information, the existing compression algorithms can be divided into two main categories: lossless [Zhang et al., 2005; Duda et al., 2001; Miaou and Chao, 2005] and lossy [Rossi et al., 2002], [Jalaleddine et al., 1990; Kim et al., 2006; Goudarzi et al., 2004; Urar and Ider, 2001; Blanchett and Kember, 1998; Zigel et al., 2000a; Hao et al., 2005; Rezazadeh et al., 2005; Miaou and Lin, 2002; Wei et al., 2001; Barlas et al., 1993; Horspool and Windels, 1994; Hamilton and Tompkins, 1991; Moody et al., 1998; Cox and Ripley, 1973; Yuan, c2004; Alesanco et al., 2006; Velasco et al., 2004]. Lossless compression algorithms are based on techniques such as null suppression, run-length encoding, diatomic encoding, pattern substitution, inter-beat differencing, intra-beat differencing techniques and statistical encoding [Gilbert., 1987]. In null suppression method repeated null values or zero values are replaced with shorter code word followed by the length of the null occurrence. Run-length encoding is similar to null suppression, except for its application for all the repeated symbols. In diatomic encoding method, occurrence of two consecutive symbols is coded with a single code symbol. Pattern substitution method looks for specific patterns and encodes them with short code symbols. All the above mentioned lossless compression methods can be implemented in single pass. But in two pass statistical encoding methods, the complexity level is higher, where symbol probability or frequency is calculated before encoding. The knowledge of symbol probability or frequency is used to encode the information optimally, where more frequent symbols are encoded with shortest code word and less frequent symbols are encoded with larger code word. Many forms of entropy coding are used in the literature [Duda et al., 2001] for ECG compression. Huffman encoding [Huffman, 1952] is also used frequently as the

final step for many ECG compression algorithms [Urar and Ider, 2001; Hamilton and Tompkins, 1991; Alesanco et al., 2006], since it compresses the information further without any loss. In Huffman encoding most frequently occurring values are represented by simple and shortened binary code. LZW [Ziv and Lempel, 1978] based algorithms pioneers Huffman and Arithmetic encoders by searching for the repeated patterns in the input stream and encoding them with shorter codes. Since all the two pass encoding schemes scan the whole document in the first pass, these methods cannot be utilised for the purpose of realtime compression as the whole ECG session is required to be completed before applying compression.

Transformational techniques like wavelet transform also have been used for ECG compression [Duda et al., 2001; Miaou and Chao, 2005; Goudarzi et al., 2004; Miaou and Lin, 2002]. After wavelet decomposition, Set Partitioning in Hierarchical Trees (SPIHT) encoding is often adopted to exploit the inherent similarities across sub bands in a wavelet decomposition and perform uniform quantization and bit allocation. SPIHT codes the most important wavelet transform coefficients in priority, and transmits them according to that order. Even though SPIHT encoding is generally used for lossy compressions [Goudarzi et al., 2004; Miaou and Lin, 2002], recent research demonstrates its applicability in lossless ECG compressions [Miaou and Chao, 2005].

Research on lossy ECG compression has out numbered the research in lossless ECG compression. There are mainly three types of lossy ECG compressions: direct time domain methods [Jalaleddine et al., 1990; Rossi et al., 2002; Hamilton and Tompkins, 1991], feature extraction methods [Kim et al., 2006; Goudarzi et al., 2004; Urar and Ider, 2001; Zigel et al., 2000a; Hao et al., 2005; Wei et al., 2001; Hamilton and Tompkins, 1991; Alesanco

et al., 2006] and transformational methods which generally exploit Wavelet transformation, Discrete Cosine transformation, KLT, and Fourier transformation etc. [Kim et al., 2006; Goudarzi et al., 2004; Hao et al., 2005; Miaou and Lin, 2002; Alesanco et al., 2006; Velasco et al., 2004].

Direct time domain methods are of lower complexity than the feature extraction methods or transformational methods. Therefore, techniques presented in direct time domain methods can be easily implemented in small devices [Rossi et al., 2002]. Generally these methods employ the knowledge of previous samples, often referred to as the prediction algorithm or utilise the knowledge of both previous and future sample, referred to as interpolation algorithm [Jalaleddine et al., 1990]. Differential Pulse Code Modulation (DPCM) has been one of the most popular direct transformational ECG compression methods. The simplest form of DPCM, applies Zero Order Prediction (ZOP), where the previous sample is thought to be the predicted sample, and only the difference between the current sample and the previous sample is transmitted [Jalaleddine et al., 1990]. This technique is commonly termed as first difference or intra-beat difference.

In feature extraction methods of lossy ECG compression, different sections of ECG curve is recognized by the algorithm. Many of the ECG compression techniques that start with QRS detection, before performing the actual compression, fall into this category [Kim et al., 2006; Goudarzi et al., 2004; Urar and Ider, 2001; Zigel et al., 2000a; Hao et al., 2005; Wei et al., 2001; Hamilton and Tompkins, 1991; Alesanco et al., 2006]. QRS detection is needed for detecting each of the beats. Many of the methods perform inter-beat difference where current beat is subtracted from the previous beat or an average beat [Zhang et al., 2005; Hamilton and

Tompkins, 1991; Alesanco et al., 2006]. The residue from inter-beat subtraction is generally less than intra-beat difference. This is mainly because in inter-beat difference complex areas, like QRS and T, is also normalized, leaving minimal residue. But, for patients, having irregular beats, inter-beat difference does not offer much reduction of information. To deal with this varying period (TT interval) issue, beats are averaged [Kim et al., 2006; Goudarzi et al., 2004; Urar and Ider, 2001; Wei et al., 2001; Hamilton and Tompkins, 1991] before any other operations. Some techniques [Alesanco et al., 2006] engage beat template databases, which are modified and updated with every ECG sample. Beat templates from the database are used for inter-beat difference calculations resulting in complex PC based telecardiology applications [Alesanco et al., 2006]. Moreover, since the baseline is not always straight or even, some methods adjust or remove the baseline [Zigel et al., 2000a; Alesanco et al., 2006]. Beat alignment/period alignment, amplitude normalization [Goudarzi et al., 2004] or baseline adjustment [Zigel et al., 2000a; Alesanco et al., 2006] requires execution of further operations. All these additional operations make the compression procedure more complex.

Recently, transformational methods, especially wavelet transform based compression algorithms are becoming popular. Almost all of the transformational methods are targeted for PC based solutions. Unlike the PC based programming environment, the small device environment, e.g. Connected Limited Device Configuration (CLDC) of Java 2 Micro Edition (J2ME), has hardly any supporting libraries which make the development extremely difficult [Sufi, 2007; Sufi et al., 2006b; 2008c]. Moreover, the limitations of the hardware such as the lower memory size, the number of I/O ports etc, challenge the implementation of transformational methods on the mobile phone.

## 2.4 Why a New ECG Compression is Required?

Based on the techniques used, compression algorithms for ECG can be broadly classified into three major groups, namely direct domain method [Rossi et al., 2002; Jalaeddine et al., 1990], feature extraction method [Kim et al., 2006; Zigel et al., 2000a] and transformational method [Miaou and Lin, 2002; Velasco et al., 2004]. The existing ECG compression techniques are somewhat unsuitable for mobile phone based wireless telecardiology applications for the following reasons:

- *Computationally expensive:* Most of the existing ECG compression algorithms were designed and tested on PC [Kim et al., 2006; Jalaeddine et al., 1990; Rossi et al., 2002; Zigel et al., 2000a; Miaou and Lin, 2002; Velasco et al., 2004]. However, a regular mobile phone (not high end) is capable of running only 10,000 operations per second, while executing Java MIDlets on Java Kilobyte Virtual Machine (KVM) [Sufi, 2007]. CLDC 1.1 restricts the usage of floating point operations, which means all the floating point must be removed before performing any operations on the mobile devices. Multi dimensional arrays are not supported as well, hence, any algorithm performing matrix based calculation can not be implemented on Java<sup>TM</sup> based mobile devices directly. Complex functions comprising a large number of basic operations like QRS detection, Beat/Period alignment, and transformations will provide unexpected delay or even deadlock in small devices. Furthermore, due to the memory restriction, algorithms requiring large memory for maintaining lookup table [Duda et al., 2001], codebook [Zigel et al., 2000a] and frequency table [Kim et al., 2006; Utrar and Ider, 2001; Horspool and

Table 2.2: Comparison of RAM and CPU Speed Among Mobile Phone, Implantable Devices and PC

Device Type	RAM (KB)	CPU Speed (kHz)
Pacemaker	About 10	30 to 100
Implantable Loop Recorder	About 100	30 to 100
Implantable Cardioverter Defibrillator	About 250	30 to 100
Mobile Phone	About 250	50 to 100
Personal Computer	128000	1200000

Windels, 1994; Hamilton and Tompkins, 1991; Alesanco et al., 2006] are not feasible for mobile phone platforms. Frequency tables were widely used by some 2-pass encoding techniques like Huffman [Urar and Ider, 2001; Hamilton and Tompkins, 1991; Alesanco et al., 2006; Velasco et al., 2004], LZW [Horspool and Windels, 1994], Significant bit encoding [Kim et al., 2006], SPIHT [Miaou and Chao, 2005; Goudarzi et al., 2004; Miaou and Lin, 2002] etc. Therefore, algorithms for ECG compression, analysis, display, secured transmission etc. must be shared by limited computational power offered by the mobile devices. Under these limitations, existing PC based ECG compression algorithms are ineffective for mobile phone based wireless telecardiology applications.

- *Unsuitable for MMS/SMS transmission:* Mobile phone based wireless telecardiology application often requires transmission of ECG signals over existing MMS and SMS protocols [Lee et al., 2007; Sufi et al., 2006b]. These MMS and SMS protocols only support limited character sets (e.g. GSM 03.38) during transmission. However, most of the existing ECG compression algorithms use Huffman-encoded and optimally arranged binary representation of the compressed ECG as the final output. Therefore, if existing

ECG compression algorithms are adopted for transmission of compressed ECG over existing text messaging (SMS/MMS) communication, many of the characters will be lost, since they are not supported by the underlying transmission infrastructure. This will result in lossy and mutilated transmission of ECG, which is not at all suitable for diagnostic purposes.

- *Need for Realtime Performance:* Realtime processing in telemonitoring simply means the time required to process (compute) the physiological signal must be less than the time required to receive that signal, during a continuous acceptance of physiological signal from the acquisition device. If the mobile phone, which receives physiological signal, consumes less than one second to process one second worth of ECG data, then realtime operation is executed [Sufi et al., 2007]. This realtime factor [Sufi et al., 2007], often determines the efficiency and effectiveness of a remote telemonitoring platform. Therefore, any algorithm pertaining to realtime telemonitoring should be evaluated for realtime performance.
- *Requirement of decompression for further analysis on compressed ECG:* Finally, the main objective of existing ECG compression techniques is to achieve high compressibility by having redundancy free output. This means that to perform analysis from the compressed ECG one must decompress the compressed ECG signals, which results in unwanted delays. This is specially true in case of resource constraint mobile devices, where decompression time could be long.

Moreover, the vast majority of the literatures related to existing ECG compression algorithms are lossy, which make them unsuitable for medical diagnosis as mandated by the law requirement in many countries including U.S. Therefore, lossless compression is mandatory and the main focus of this section. The unsuitability of existing compression algorithms for mobile phone based telemonitoring is briefed in Table 2.3.

## 2.5 The Proposed Compression Method

The proposed ECG compression algorithm is based on symbol substitution technique [Lei et al., 2004; Sufi et al., 2005; 2006a], which has been successfully applied in our previous genome sequence compression algorithm. The algorithm was proven to be faster than many other existing algorithms for compression of genome sequences [Sufi et al., 2006a; 2005]. Encouraged by the result, we intended to apply similar technique in the present case as well, although there is subtle difference between the two. Genome sequences are represented by only four types of ASCII characters: A, T, G and C. For each of these characters 8 bits are used. However, with binary encoding only 2 bits ( $2^2 = 4$ ) are sufficient to represent each these four characters, establishing a basic compression ratio of 4 ( $\log_4 4^4$ ). Previous symbol substitution algorithms [Lei et al., 2004; Sufi et al., 2005; 2006a] achieved the same level of compression by symbol substitution of 4 consecutive characters from genome sequence with a single ASCII character. According to [Lei et al., 2004; Sufi et al., 2006a; 2005], the basic compression achieved with symbol substitution is faster and computationally inexpensive compared to other types of compression algorithm. Therefore, it is reasonable to adopt a symbol substitution based ECG compression technique for inexpensive processing on mobile



phones. By efficiently substituting ECG samples with a character, which is supported by MMS and SMS architecture, we will be able to transmit compressed ECG without any loss or distortion. However, this task is not as straight forward as it were for genome sequences for the following three reasons:

1. Unlike genome sequences, where there is a single character (any character from A, T, G, C group) representing a single nucleotide, each of the ECG sample has multiple digits (1-6 digits for MIT BIH Database ECG entries). The number of digits depends on the acquisition device settings (resolutions).
2. Unlike genome sequences, where the four characters can be represented with 4 digits (1, 2, 3 and 4), a single ECG sample is a non-integer floating point value. Therefore, before the start of symbol substitution process, ECG samples should be transformed into integer values.
3. Unlike genome sequences, where the sequences do not have any negative values, a single ECG sample can be either positive or negative. Therefore, the signs and the values require separate encodings.

For obtaining proper understanding of the proposed compression framework, at first the generic compression model will be presented. Next, based on the proposed generic compression framework, ASCII encoding and a user defined character set will be applied to compress ECG respectively. Within the result section, detailed performance comparison will be performed. Finally, the discussion section illustrates how further compression ratio can be obtained using LZW based compression along with the proposed compression technique.

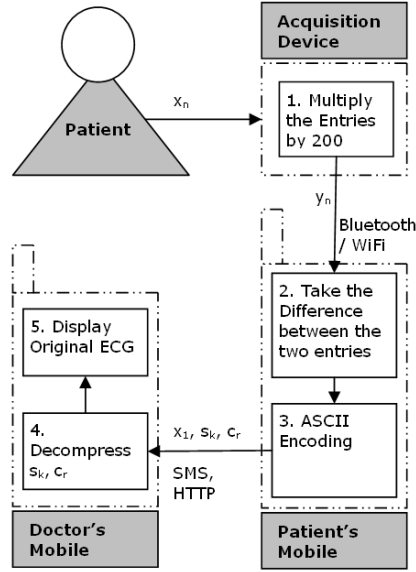


Figure 2.2: Mobile Phone based ECG Compression

### 2.5.1 Generic Framework of the Proposed Compression Mechanism

The proposed symbol substitution based ECG compression deals with the above challenges while performing compression. As depicted in Figure 2.3, original ECG is first normalized. During this normalization, the original ECG is multiplied with an acquisition device dependent constant,  $C$  as in Eq. 2.1.

$$y(n) = x(n) \times C \quad (2.1)$$

The purpose of this normalization is to reduce the character size (number of digits) of each of the samples and transform the floating point values to integer values. As an example, two consecutive samples of 0.205 and 0.210 (of MIT BIH Arrhythmia database) become 41 and

42, when  $C$  is 200 for that whole duration of ECG acquisition. Therefore, for this example, the character size is reduced from 10 to 4. Then, the difference between two consecutive samples is calculated using Eq. 2.2.

$$z(n) = y(n) - y(n - 1) \quad (2.2)$$

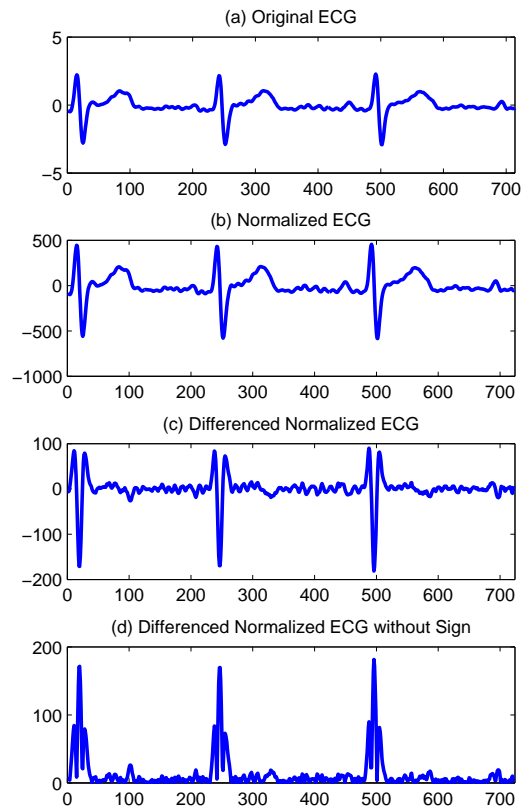
This operation, as depicted in Figure 2.3 (c), performs amplitude reduction. This intrabeat subtraction for the reduction of amplitude was previously used by [Hamilton and Tompkins, 1991] during ECG compression. Therefore, for the previous example, 41 and 42 results in 1. This task further reduces the number of digits for the ECG samples. Most of the ECG samples are transformed to single digit signed integer values by Eq. 2.1 and 2.2. As it is evident from Figure 2.3(a) - 2.3(c), sample values can be negative or positive. Next, the signs and the values are segregated and character encoded separately using the same character set,  $S = \{S_1, S_2, S_3, S_4, \dots, S_M\}$ , where  $M$  is the highest number of character for that particular character encoding. Compression ratio ( $CR$ ) of a symbol substitution based compression depends on the range of input and output characters, for a particular character encoding. When  $M_i$  and  $M_o$  are the number of different characters supported by the input and output texts, then  $CR$  can be expressed as Eq. 2.3. As an example, when  $M_i$  is 4 for genome sequence data and  $M_o$  is 256 (since 256 ASCII characters were used for symbol substitution), a  $CR$  value of 4 is obtained ( $\log_4 256$ ) [Lei et al., 2004; Sufi et al., 2005; 2006a].

$$CR = \log_{M_i} M_o \quad (2.3)$$

However, unlike genome data, where ATGC can be represented by unsigned 1234 (base 4 numbering), ECG data is signed. Therefore, sign and value encodings should be done separately. During the sign encoding process,  $M_i$  is 2 (0 for positive value and 1 for negative value), since sign (+/-) can be encoded in binary numbering system. For ASCII, the value of  $CR$  is 8 ( $\log_2 2^8$ ) as was performed in our previous research [Sufi et al., 2006b; Sufi and Khalil, 2008b]. However, the full set of 256 ASCII characters are not supported by existing text messaging (SMS/MMS) systems. Therefore, a reduced character set is required for ECG transmission via SMS and MMS. Algorithm 1 shows both sign encoding and value encoding process. In this algorithm the value of  $q$ , which is the number of Differenced Normalised ECG to be read by the algorithm at a time, depends on the particular character encoding. For ASCII, it is 8, since 8 consecutive sign bits (0 or 1) from 8 ECG samples are represented by a single character from 256 ASCII set. For SMS and MMS transmission, the supported character set is often 7 bits, resulting in  $q = 7$ .

After successful sign encoding, absolute values (values without sign information) are left as seen in Figure 2.3 (d). Within these values, there are both single double digit numbers. The encoding of single digit and double digit numbers are done with different character subset  $U$  and  $V$  respectively, where  $S = U \cup V$ .

To increase the compressibility, 2 consecutive single digit values are encoded with one



*Figure 2.3: Preprocessing Stages of ECG Compression*

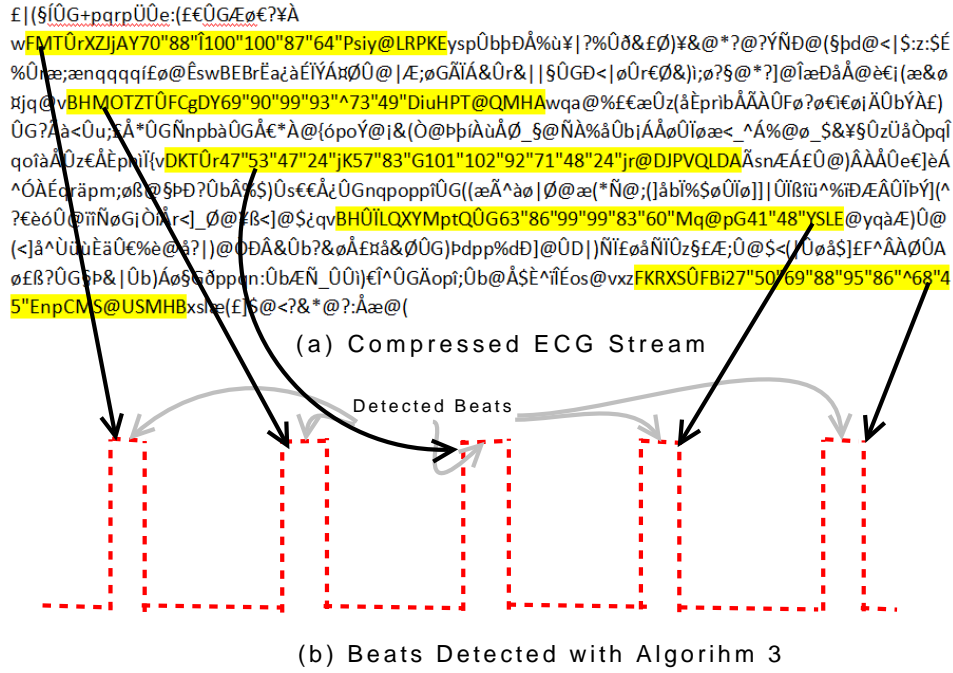


Figure 2.4: Beats Hidden Within Compressed ECG

element of  $U$ . However, for double digit values, one to one mapping is performed with elements of  $V$ . Theoretically,  $CR$  achieved for encoding single digit values is  $2 \times \log_{10} M_o$  for a particular character set. But for double digit values it is only  $\log_{10} M_o$ .

Therefore, all double digit high pitched values are represented with  $V = \{v1, v2, v3, v4, \dots\}$ . Among these high pitched values, QRS complexes are the most obvious ones. For a person, who knows the character set  $V$ , it is possible to ascertain the possible locations of the QRS complexes from the compressed ECG as depicted in Figure 2.4. This is how, the proposed compression algorithm exposes the crucial ECG feature waves (QRS Complex) within the compressed ECG, from where it is possible to perform ECG analysis without requiring to decompress the compressed ECG. Details of ECG analysis from the compressed ECG will be presented in chapter 5.

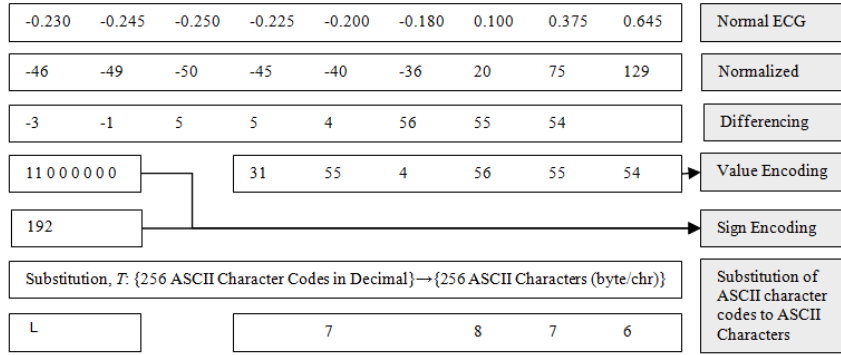


Figure 2.5: ECG Samples Compression with the Proposed Method (Example)

The generic biosignal compression algorithm presented in Algorithm 1 can be successfully applied to any of the character sets  $S$  like, ASCII, UTF-7, GSM 03.38, Unicode-16, Unicode-32 to compress signals like ECG, Blood Pressure or Pulse.

### 2.5.2 ECG Compression using ASCII Character Set

The signs and the values from all the normalised differences with sign are separated using Eq. 2.4. For each element of the normalised difference with sign, vector  $d(i)$ :

$$d(i) = m(i) \times p(i) \tag{2.4}$$

where  $m(i) = \text{Sign}[d(i)]$  and  $p(i)$  is the absolute value of  $d(i)$ . Then the signs and the values are ASCII encoded using Eqs. 2.5 -2.8 and Eqs. 2.9-2.11 respectively. During the sign encoding process, the proposed algorithm reads 8 consecutive entries of Step 2 (Figure 2.6) and represents their signs by a single ASCII character. Since each of the 8 entries can be either positive or negative, they can have  $2^8$  or 256 different values, just enough for using 256 ASCII characters to represent each of the combinations.

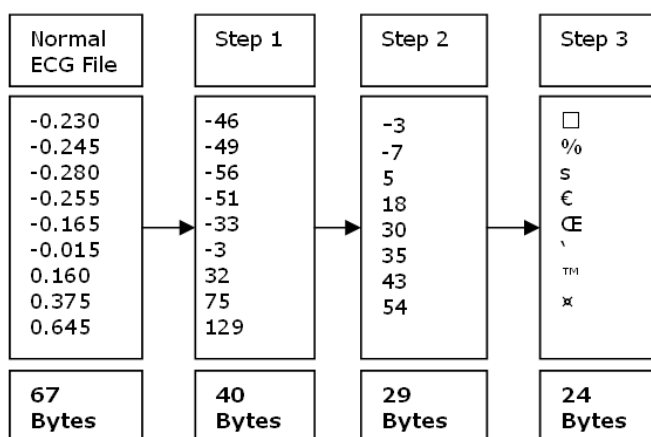


Figure 2.6: Step By Step Process Of Encoding (For an Example Case)

Sign information  $m(i)$  is rearranged as in Eq. 2.5.

$$L = \begin{bmatrix} m(1) & m(9) & \dots & m(K-7) \\ m(2) & m(10) & \dots & m(K-6) \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ m(8) & m(16) & \dots & m(K) \end{bmatrix} \quad (2.5)$$

where  $K = N - 1$  if  $(N - 1)$  is divisible by 8; otherwise, we add + (Positive Padding) such that  $K \geq N$ . The signs are replaced by 0 or 1 as in Eq. 2.6.

$$b(i) = \begin{cases} 0 & \text{if } m(i) = +ve \\ 1 & \text{if } m(i) = -ve \end{cases} \quad (2.6)$$



Therefore, a new matrix  $B$  can now be constructed as follows,

$$B = \begin{bmatrix} b_1(1) & b_1(2) & \dots & b_1(\frac{K}{8}) \\ b_2(1) & b_2(2) & \dots & b_2(\frac{K}{8}) \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ b_8(1) & b_8(2) & \dots & b_8(\frac{K}{8}) \end{bmatrix} \quad (2.7)$$

where  $b_j(k)$  is either zero or one according to Eq. 2.6 and  $j = 1, 2, \dots, 8$  and  $k = 1, 2, \dots, K/8$ . Then all columns in Eq. 2.7 are converted into corresponding decimal value (from binary) followed by ASCII conversion using Eq. 2.8. The first element is the least significant bit and the last element is the most significant bit.

$$s_k = ASCII\left(\sum_{i=0}^7 b_j(k) \times 2^i\right) \quad (2.8)$$

where  $k = 1, 2, \dots, K/8$  Once the signs are coded, the signs from the original normalised differences (with sign) are removed. Figure 2.3 (d) shows the sign removed values of differences. The normalised difference without sign values can be divided into simple blocks and complex blocks. In simple blocks, the normalised difference without sign values ranges from 0 to 9 and for complex block the values are equal to or higher than 10. Therefore, simple blocks have single digit and complex blocks have multiple digits for each of the values. Dif-

ferent functions are used for converting the simple block and complex blocks as presented in Eq. 2.11. In simple block, diatomic encoding was performed, where each pair of normalised differences without sign values was encoded with a single ASCII character and for complex region one to one mapping was performed. Thus for simple block bounded by 0-9 region, ASCII codes 0-47 and 58-110 were used and for complex block ASCII codes 110-255 were used. From Eq. 2.4, pair wise values were taken to construct pair set of the  $d(i)$  value, Therefore,

$$o_l = (p_{2i-1}(l), p_{2i}(l+1)) \quad (2.9)$$

where,  $i = 1, \dots, N-1$  and  $l = 1, \dots, \frac{(N-1)}{2}$  Every pair of  $o_l$  are evaluated as follows,

$$o_l = \begin{cases} ((p_{2i-1} \times 10) + p_{2i}) & \text{When } p_{2i} < 10 \\ ((p_{2i-1} \times 100) + p_{2i}) & \text{When } 9 < p_{2i} < 10 \end{cases} \quad (2.10)$$

where  $i = 1, \dots, N-1$  and  $l = 1, \dots, \frac{(N-1)}{2}$ . In Eq.2.10 string concatenations were performed.

If the consecutive 2 entries have a numerical value less then 100 (i.e. 2 digits number), then the two entries are encoded by a single ASCII character, using the 2 digit decimal number as the character code (from Eq. 2.11). As an example, if 2 consecutive numbers (Step 2 of Figure 2.6) are 3 and 7, then we get 37, and the ASCII character represented by

the character code of 37 is %.

Again, if the numerical value of concatenated 2 consecutive entries (step 2 of Figure 2.6) is more than 100 then we represent each of the 2 entries by a single ASCII character. As a result, there will be 2 different ASCII characters (Eq. 2.11). For an example if the 2 consecutive entries found in step 2 (Figure 2.6) are 5 and 18, then the numeric value of the concatenated string will be 518, which is greater than 100. So, in this case 5 will be represented by the ASCII character (s) with character code (5+110) or 115 and 18 will be represented by the ASCII character with character code (18+110) or 128. Eq. 2.11 shows the value encoding process.

$$\begin{aligned}
 & \text{When } o_l < 100, \\
 c_r = & \begin{cases} ASCII((p_{2i-1} \times 10) + p_{2i}) & \text{When } o_l < 48 \\ ASCII((p_{2i-1} \times 100) + p_{2i} + 10) & \text{When } 48 < o_l < 100 \end{cases} \\
 & \text{where } i = 1, 2, \dots, N - 1 \text{ and } r = 1, 2, \dots, R \\
 & \text{When } o_l > 100 \\
 & c_r = ASCII(p_{2i-1} + 110) \\
 & c_{r+1} = ASCII(p_{2i} + 110) \\
 & \text{where } i = 1, 2, \dots, N - 1 \text{ and } r = 1, 3, 5, \dots, R - 1
 \end{aligned} \tag{2.11}$$

$R \geq \frac{(N-1)}{2}$  when  $o_l < 100$  for all  $o_l$   $R = N - 1$  when  $o_l > 100$  for all  $o_l$  Compression is achieved when the number of sign coded ASCII characters and number of value coded ASCII

characters are less than the original length of the ECG signal or when,  $\frac{K}{8} + R < N$ . During this encoding process (Eq. 2.11), numbers were not utilised for ASCII encoding purpose. Hence, character code 48 to 57 (number 0 to 9) has been left outside this encoding scheme. As a result, any unnatural (more than 255) values of normalised difference without sign, for which limited ASCII characters are not enough, can be preserved using the numerical values (no ASCII conversion is performed).

### 2.5.3 Decompression in Doctor's Mobile

During the decompression process, each of the compressed character is read and translated to the character code. The very first character is the first ECG sample and the next one holds the sign information of eight consecutive entries.

$$x_1, s_k, c_r = x_1, s_1, c_1, c_2, c_3, c_4, c_5, s_2, c_6, c_7, \dots, \quad (2.12)$$

$$s_K, c_{R-5}, c_{R-4}, c_{R-3}, c_{R-2}, c_{R-1}, c_R$$

where  $k = 1, 2, \dots, \frac{K}{8}$  and  $r = 1, 2, \dots, R$

The decompression is processed in two parts: decompression of sign from  $s_k$  (Eq. 2.13-2.14) and decompression of value from  $cr$  (Eq. 2.15-2.19). First the sign values are decoded from the ACSII values using Eq. 2.13 and matrix  $B$  of Eq. 2.7 is recreated.

$$b_j(k) = Dec \rightarrow Bin[CharacterCode[s_k]] \quad (2.13)$$

where  $j = 1, 2, \dots, 8$  and  $k = 1, 2, \dots, \frac{K}{8}$ . After the creation of Matrix  $B$ , Matrix  $L$  of Eq. 2.5 can be recovered by

$$m(i) = ((-2) \times b_j(k) + 1) \quad (2.14)$$

where  $i = 1, 2, \dots, K$ . The occurrences of the next ASCII characters are translated to normalised difference values (Step 2 of Figure 2.6) until there are 8 consecutive digits, and then these 8 consecutive digits are appended to the sign information (Eq. 2.15-2.18).

If  $CharacterCode(c_r) < 48$  then,

$$d_i = m(i) \times ((CharacterCode(c_r)) \text{ Div } 10) \quad (2.15)$$

$$d_{i+1} = m(i+1) \times ((CharacterCode(c_r) \text{ Mod } 10))$$

If  $58 \leq CharacterCode(c_r) < 110$  then,

$$d_i = m(i) \times ((CharacterCode(c_r) - 10) \text{ Div } 10) \quad (2.16)$$

$$d_{i+1} = m(i+1) \times ((CharacterCode(c_r) - 10) \text{ Mod } 10) \quad (2.17)$$

If  $CharacterCode(c_r) > 110$  then,

$$d(i) = m(i) \times ((CharacterCode(c_r) - 110)) \quad (2.18)$$

where  $i = 1, 2, \dots, N - 1$  for all cases of Eq. 2.15 to 2.18. During this process of

decoding (Eq. 2.15-2.18), whenever  $i$  is divisible by 8, the next compressed character by the doctor's mobile will be an ASCII coded character holding sign information of the next 8 normalised difference value. Lastly, each of the decoded normalised differenced values with sign is multiplied with 0.005 and added with previous uncompressed digit to retrieve the next uncompressed digit (Eq. 2.19).

$$x(i + 1) = x(i) + (d(i) \times 0.005) \quad (2.19)$$

In case of Java<sup>TM</sup> based mobile phones, which can not operate with floating point numbers, ECG curves are drawn based on the reconstructed normalised ECG. Therefore, multiplication with 0.005 is not performed (Eq. 2.19). Table 2.4 contains the experimentation results obtained by the proposed method against different entries of MIT-BIH Database. Compression Ratio was calculated by Eq. 2.20.

$$CR = \frac{n1}{n2} \quad (2.20)$$

where  $n1$  and  $n2$  are the sizes of original ECG file and Compressed ECG file. Table 2.4 shows that the compression ratio is linearly dependant ( $\gamma=0.983$ ) on the number of Simple Block Encoding and inversely dependant ( $\gamma=-0.983$ ) on the number of Complex Block Encoding. This is due to the fact that during simple block encoding 2 entries of Normalised Difference without sign is represented by 1 ASCII Character, therefore higher compression

```

@£$¥èéùìòÇøÅå_{}[~]|€ÆæßÉ !#
□%&()*+,-./:;<?¡
ABCDEFGHIJKLMNOPQRSTUVWXYZ
YZ§;
abcdefghijklmnopqrstuvwxyzäöñüàÁ
ÃÄÅÈÉÊËÌÍÎÏÐÑÒÓÔÕÖÙÚÛÜÝÞþá
âãçêëíîïðóôõúý\

```

Figure 2.7: Our Selection of MMS Character Set for Compressed ECG transmission

is achieved. Whereas in complex block, single entry of Normalised Difference without sign is represented by a single ASCII character. Therefore, ECG samples containing larger area of complex blocks result in lesser compression.

#### 2.5.4 Compression using a User Defined Character Set

Character encodings significantly varies from platform to platform. Therefore, when we wanted to transport our previous implementation [Sufi and Khalil, 2008b] of ECG compression with ASCII encoding from Windows Mobile platform to Java 2 Micro Edition platform we faced challenges. One of the major challenges encountered was many of those ASCII encoded characters were lost after transmission via MMS. Regular mobile phone as well as the telephony network can only deal with a reduced number of character set (e.g. GSM 3.38). For the research involved in this work, we carefully selected a set of characters (Figure 2.7) supported by MMS transmission. Figure 2.7 shows the selected character sets for our implementation of mobile phone based telecardiology application.

These characters were kept in an array of 148 length called MMSCS for performing symbol substitution based compression of ECG signal.

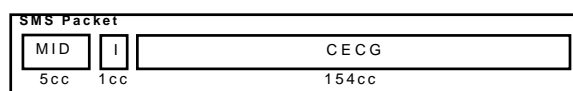


Figure 2.8: A Health Message Frame (for SMS)

### Message Format

For the proposed framework, the message frames for both SMS and MMS contain 3 main sections namely the Message ID (MID), Health Index (I) and the Compressed ECG (CECG).

Figure 2.8 shows the message format used during our implementation of patient to doctor communication via SMS. Unlike MMS and HTTP implementations, SMS can only accommodate a short message restricted by 160 characters. Therefore, ECG transmission via a single SMS can only accommodate a limited number of ECG samples (Approximately 173). This size is enough to transmit a single abnormal ECG feature (e.g. Abnormal QRS).

Size of MID is 5 characters. Since, each of the characters can have 148 different values from our MMSCS, the proposed MID can contain  $(148)^5$  or 71,008,211,968 different combinations. This enormous combination range is capable of uniquely identifying messages sent from different patients at different times. Indicator or I can contain 148 different characters from MMSCS. Hence, this one character position can provide indications of 148 cardiovascular abnormalities (RBBB, LBBB, Tachycardia, Bradycardia, Arrhythmia etc.). CECG contains the actual ECG in a compressed format.

Health Message is similarly constructed for MMS messages containing ECGs. But, the CECG is not limited to 154 cc, since MMS can accommodate longer messages. Hence, more ECG data can be sent at a time via MMS messages.



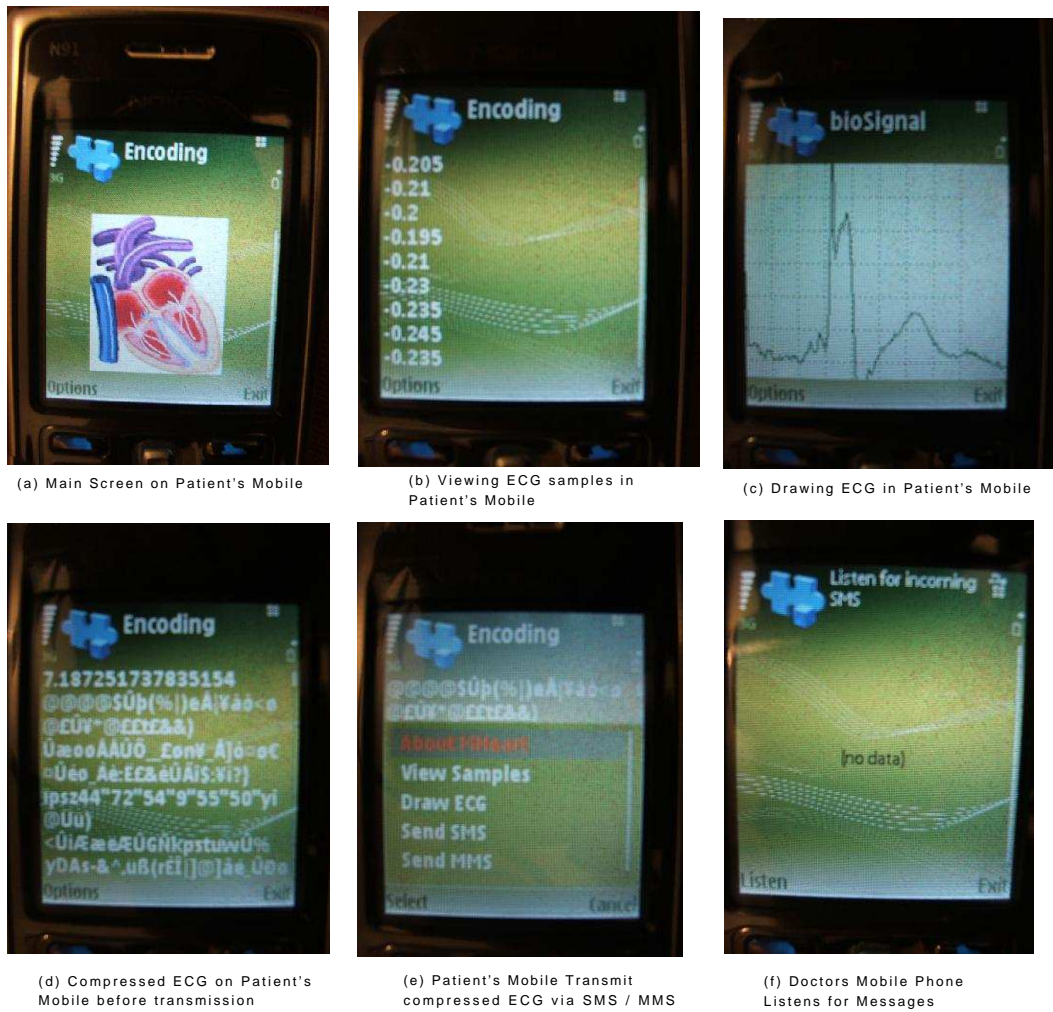


Figure 2.9: Our Implementation of Mobile Phone based Wireless Telecardiology Application

## 2.6 Experimental Results

Compression Ratio, Percentage Root Mean Square Difference (PRD), Number of Operations (NOp), compression time and decompression time were selected for performance comparison. Performance of the proposed method was measured based on 12 random entries of MIT-BIH Arrhythmia Database (<http://www.physionet.org/>). Each of the entries was 1 minute long and had 360 Hz sampling rate using a resolution of 11b/sample. The experimentation was performed on Intel Centrino 1.4 GHz Desktop PC with 512 MB RAM for performance measurement of the proposed method (in Table 2.4) and execution time comparison with LZW and Wavelet based methods (Figure 2.10, Figure 2.11, Figure 2.12 and Figure 2.13). HP iPAQ h2200 Pocket PC and HP iPAQ h6365 smart phone were used to deploy and implement ZOP, Peak, Scan Along Polynomial Approximation (SAPA) and the proposed method for Number of Operation per Second (NOp/s) wise comparison (Table 2.5). Details of ZOP, SAPA and Peak methods can be found in [Rossi et al., 2002; Miaou and Lin, 2002]. In addition, the calculations involving realtime factors and execution times for the proposed algorithm were performed in both handheld and smart phone platforms.

### 2.6.1 Number of Operations per Second (NOp/s) Comparison

An operation is termed as an expression that derives a new value from one or more other values. It is an action resulting from one or more instructions. Previous research [Rossi et al., 2002] calculated the complexity of three different ECG compression algorithms based on the average NOp needed to compress 1 second of ECG data (NOp/s) [Rossi et al., 2002]. NOp often determines the computational cost, complexity, total lines of codes (LOC) and

execution time of an algorithm.

ZOP, Peak, SAPA and the proposed method were programmed in .Net platform using Microsoft Visual Studio 2005, Pocket PC 2003 environment. These four compression algorithms were implemented on HP iPAQ h2200 Pocket PC and HP iPAQ h6365 smart phone for final deployment and testing purpose. At first, all the basic operations were identified within the source code environment. For each of the identified operations, counter variables were set up. Corresponding counter variables were incremented just after the execution of the basic operations. Thus, the total number of operations (NOp) during the compression of ECG file was obtained. Finally, the total NOp was normalised to calculate the number of operations required to compress one second of ECG data.

In [Rossi et al., 2002], the actual peak (QRS Complex) detection was supposed to be carried out by the microcontroller based pace maker. Therefore, NOp counting for QRS Complex detection was overlooked in the Peak method [Rossi et al., 2002]. To make the Peak method operable in mobile phone, a QRS detection algorithm was required be incorporated. One of the simplest forms of ECG complex region detection (QRS complex detection) can be performed by Eq. 2.21 that was applied by existing research in low-delay ECG compression algorithm for real-time situation [Jalaleddine et al., 1990].

$$Std = \sqrt{\frac{\sum_{w=1}^B (x_w - \bar{x})^2}{B}} \quad (2.21)$$

where  $B$  is the average length of the QRS complex and  $w = 1, 2, \dots, B$

If the standard deviation,  $Std$  is greater than a predetermined threshold then a QRS complex is detected. Therefore, by sliding the B block along the N length ECG samples and evaluating the standard deviation by eq. 2.21, the complex blocks can be detected and preserved for Peak algorithm. Equation 2.21 was finally utilised to program the Peak detection method, which was eventually compared with the proposed algorithm.

### **ZOP Method**

ZOP method [Rossi et al., 2002; Miaou and Lin, 2002] detects whether the next sample lies within a pre-defined range for all the ECG samples. Therefore, the major calculation involves addition and subtraction of a predefined error value from the previous sample to determine the permissible range of the next sample. Table 2.6 shows the average NOp performed by ZOP method every second.

### **SAPA Method**

SAPA method [Rossi et al., 2002; Miaou and Lin, 2002] is based on the calculation of gradients (slopes) from the point of origin to the error ranges of a next point, as well as the calculation of centre slopes. Therefore, most of the basic operations, depicted in Table 2.7, originated from the calculation of gradients.

### **Peak Method**

Equation 2.21 includes addition, subtraction, square, division and square root operations and it was frequently utilised by the Peak method. Moreover, for calculating the threshold, multiplication of a constant with the average normalised ECG value with sign was performed.

Array List functionality of .Net 2 was also utilised to maintain and update (sliding of the block) block B (Equation (2.21)). Table 2.8 exposes the fact that for all the cases, NOP count for the basic operations remained equal.

### Proposed Method

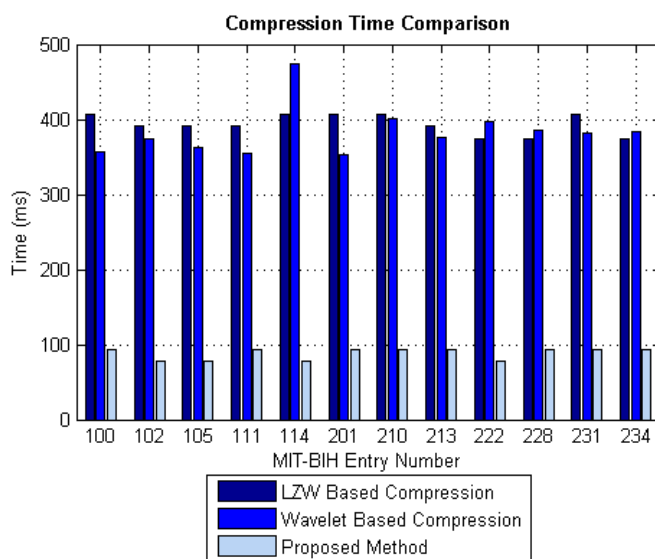
Finally, the proposed method was implemented on the same environment and the basic operations also included string join operation (for calculation of  $o_l$  using Eq. 2.10) and ASCII Conversion operation (for Eq. 2.8 and 2.11). Table 2.9 represents the basic operations performed while executing the proposed method for different MIT-BIH entries. Among all the operations, absolute operation was performed only after the signs (+ve/-ve ECG Sample) were coded. Therefore, performing the absolute operation was essential for obtaining the  $p(i)$  value of equation 2.4.

Table 2.5 shows the NOP/s comparison results, where only Zero Order Prediction (ZOP) [Jalaleddine et al., 1990] method has less NOP compared to the proposed method. But, ZOP suffers seriously from the high Percentage Root-Mean-Square Deviation (PRD) value indicating its unacceptability for diagnostic purposes [Rossi et al., 2002; Miaou and Lin, 2002]. Peak method removes the T wave completely and becomes unsuitable for diagnostic.

### 2.6.2 Compression and Decompression Time Comparison

Transformational method and LZW based methods frequently use library functions provided by the programming interface. Since library functions applies multiple numbers of basic operations and programmers are often kept distant from identifying these basic operations,

the NOP/s count for transformational methods, e.g., wavelet based methods, is not always viable. Therefore, for transformational methods and LZW based ECG compression methods, the compression and decompression times were selected as comparison parameters. Figure 2.10 and Figure 2.11 shows the lower time requirement for the proposed method to compress and decompress randomly selected ECG files, compared to Wavelet based and LZW based compression methods.



*Figure 2.10: Compression Time Comparison with LZW and Wavelet based Compression Algorithm. 12 MIT-BIH Entries were Randomly Chosen*

Unlike some recent research in realtime ECG compression [Alesanco et al., 2006], which needs 1200 ms for compression and 180 ms for decompression of 1 second ECG data, the proposed method only needs 88 ms for compression and 106.33 ms for decompression on an average. The proposed method outperforms existing methods with its faster execution time which can be ascribed to the simplicity and compact nature of the proposed algorithm. Moreover, it is important to compare the file size dependency of the proposed method.

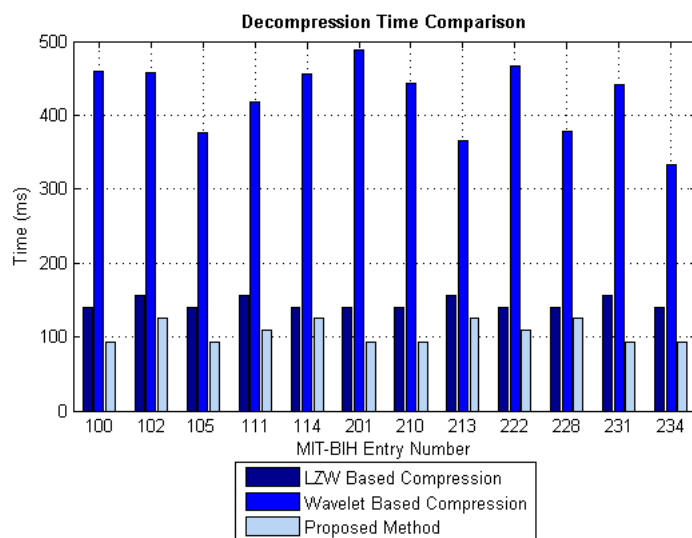


Figure 2.11: Decompression Time Comparison with LZW and Wavelet based Compression Algorithm. 12 MIT-BIH Entries were Randomly Chosen

Figure 2.12 and Figure 2.13 are the compression and decompression time comparison for LZW based compression, wavelet based compression and proposed method with five different file sizes (5.76 KB, 10.6 KB, 51.8 KB, 114 KB and 166 KB). These varying sized files were obtained by random selection of different sections of a randomly selected MIT-BIH entry. It is noticeable that our proposed method provides best performance for both compression and decompression while the file size increases.

### 2.6.3 Compression Ratio Comparison

The compression ratio of the proposed method was compared with other existing lossless compression methods. Table 2.10 shows the compression ratio wise comparison.

The proposed method pioneers most of the existing lossless ECG compression with higher compression ratio.

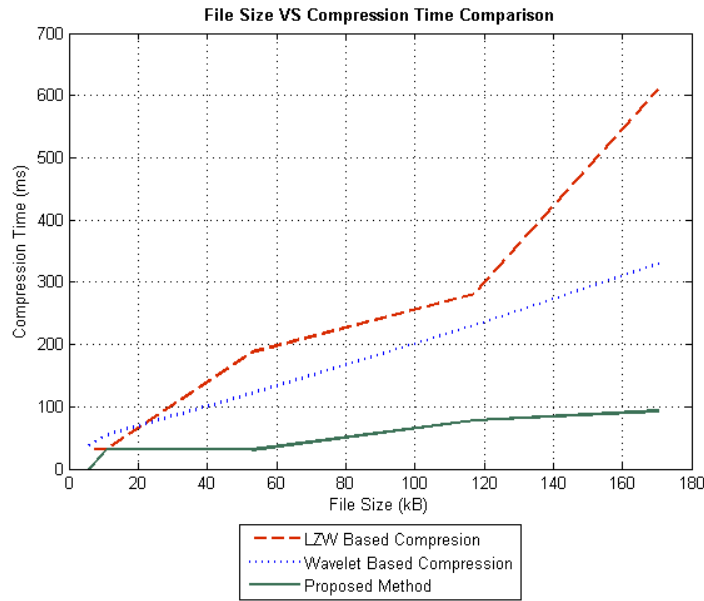


Figure 2.12: Compression Time Comparison for LZW Based Compression, Wavelet based Compression and Proposed method for Different File Sizes

#### 2.6.4 Realtime performance measurement

Realtime factor,  $T_r$ , which is defined as the time needed to compress / decompress 1 second of ECG data, was calculated on both HP iPAQ h2200 Pocket PC and HP iPAQ h6365 smart phone. The average total time ( $T_t$ ) needed to compress / decompress 12 randomly selected MIT-BIH Arrhythmia Database entries was measured on both devices and Eq. 2.22 was used to calculate the realtime factor  $T_r$  for compression and decompression.

$$T_r = \frac{T_t \times F}{N} \quad (2.22)$$

Where  $N$  is the length (total number of samples) of the ECG file and  $F$  is the sampling frequency. For our MIT-BIH Arrhythmia Database entries  $F$  was 360 and  $N$  was 21600.



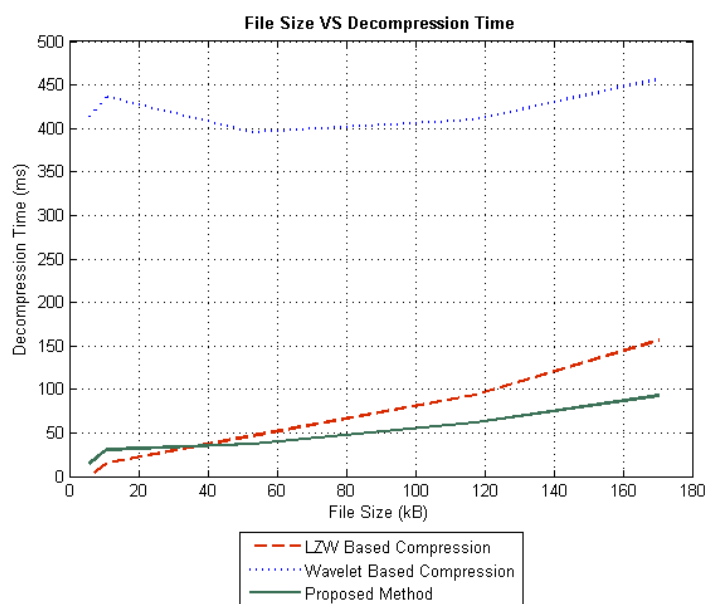


Figure 2.13: Decompression Time Comparison for LZW Based Compression, Wavelet Based Compression and Proposed method for Different File Sizes

Table 2.11 shows that for both devices it was less than 1 second, adhering to the minimum criteria for realtime operation [Sufi et al., 2007].

## 2.7 Discussion: Further Enhancement of the Compression Ratio

From the design objectives, experimentation results and comparison details, it becomes apparent that the proposed compression algorithm is not only a simple algorithm capable of being executed on generic mobile phone platforms, but also it provides a significant amount of compression ratio. However, this compression ratio can be raised even further, when it is coupled with existing LZW based compression algorithms to obviate the repetition found within the encoded ECG text (by the proposed method). Up to 90.64% of compression ratio can be obtained from 2 phase encoding (proposed compression) and LZW based compres-

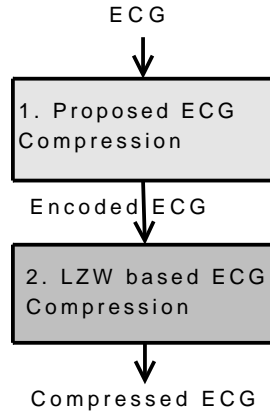


Figure 2.14: Raising the Compression Ratio with the Proposed Compression Scheme and LZW based Compression Scheme

sion algorithm with the specific sequence shown in Figure 2.14. It should be noted that performing LZW based compression before the proposed ECG will not produce any suitable result, because the proposed compression algorithm only expects ECG sample (not LZW based compressed ECG). The results of this higher compression ratio can be clearly seen from Table 2.12.

In Table 2.12,  $S_o$  refers to original ECG size for the first one minute data in kilobyte (KB). Then,  $S_e$  refers to the reduced data size with the proposed compression method. The compression ratio obtained by the proposed compression method is represented by  $CR_{oe}(CR_{oe} = \frac{S_o}{S_e})$ . Next,  $S_c$  refers to compressed ECG with LZW based compression algorithm.  $CR_{ec}(\frac{S_e}{S_c})$  and  $CR_t(CR_{oe} \times CR_{ec})$  denote compression achieved with LZW based compression and total compression ratio respectively. Lastly, compression time achieved by the proposed method, compression time achieved by the LZW based method and the total compression time is represented by  $T_e, T_c$  and  $T_t$  respectively.

As already stated, higher compression ratio benefits faster transmission of enormous

ECG at the expense of higher computational complexities for resource constraint mobile devices. It should be mentioned that we obtained algorithms of ICSsharpCode.SharpZipLib (<http://www.icsharpcode.net>) library to compress the data using LZW based algorithms. This library supports four types of compression (Zip, GZip, Tar, BZip2). Since this compression library was available in open source format, it can be easily programmed for J2ME platform.

## 2.8 Conclusion

Proposed here is a relatively simple but highly efficient lossless ECG compression method that can be implemented on mobile phones for realtime diagnosis. The output of the compressed file can easily be transmitted utilising HTTP/ SMS/ MMS and decompressed on a mobile phone handset at the receiver's end. The compression algorithm performs encoding while it receives new samples and transmits them with minimal delay, which makes the system suitable for realtime applications. Moreover, the proposed method outperforms most of the existing compression methods with less computational cost, faster execution time and better compression ratio without compromising the reconstruction quality. According to our experimentation, a maximum of 4.051 compression ratio was achieved with our proposed encoding scheme. This compression ratio could be raised even further to 90.64%, if LZW based compression is added after encoding is performed with our proposed method (as shown in Fig. 2.14).

Now that we have achieved efficient transmission and storage of ECG, we need to explore details of the CVD patient authentication mechanism. In our next chapter, we will delve into

## CHAPTER 2. COMPRESSION OF ECG

the details of our proposed ECG based biometric authentication systems. Few of our proposed authentication mechanisms can directly authenticate patients from their compressed ECG packets, which were compressed using the methods described in this chapter.

Table 2.3: Unsuitable Criteria for Mobile Phone based Realtime ECG Compression

Unsuitable criteria for mobile phone based realtime ECG compression	Listed References (Reviewed literatures)
Complex Calculation involving floating points	[Urar and Ider, 2001; Goudarzi et al., 2004; Jalaleddine et al., 1990; Moody et al., 1998; Hao et al., 2005; Barlas et al., 1993; Miaou and Chao, 2005; Rezazadeh et al., 2005; Blanchett and Kember, 1998; Gilbert., 1987]
Matrix based calculation (involves usage of multidimensional array)	[Urar and Ider, 2001; Barlas et al., 1993; Gilbert., 1987]
Reconstruction Error	[Urar and Ider, 2001; Goudarzi et al., 2004; Jalaleddine et al., 1990; Moody et al., 1998; Hao et al., 2005; Barlas et al., 1993; Miaou and Chao, 2005; Rezazadeh et al., 2005; Velasco et al., 2004; Gilbert., 1987]
QRS Detection	[Urar and Ider, 2001; Goudarzi et al., 2004; Moody et al., 1998; Velasco et al., 2004; Hao et al., 2005; Barlas et al., 1993; Rezazadeh et al., 2005; Blanchett and Kember, 1998]
Beat Alignment (Period Normalization/ Base Alignment/ Amplitude Normalization)	[Urar and Ider, 2001; Goudarzi et al., 2004; Moody et al., 1998; Hao et al., 2005; Barlas et al., 1993; Blanchett and Kember, 1998; Velasco et al., 2004]
2-Pass Encoding	[Urar and Ider, 2001; Goudarzi et al., 2004; Jalaleddine et al., 1990; Moody et al., 1998; Blanchett and Kember, 1998; Velasco et al., 2004; Gilbert., 1987]
Lookup Table based encoding	[Hao et al., 2005; Miaou and Chao, 2005]
Application of Transformational Methods	[Urar and Ider, 2001; Goudarzi et al., 2004; Jalaleddine et al., 1990; Miaou and Chao, 2005; Rezazadeh et al., 2005; Velasco et al., 2004; Gilbert., 1987]

---

 Algorithm 1: Compression of ECG Data
 

---

```

//Notation Description:
//cc holds the compressed character (output of this algorithm).
//char(index) returns to returns the V character for
//that index value ( $v_{index} \in V$ ).
//entry(index) returns the Differenced Normalised ECG
//of the index value.
Loop (Until the end of Differenced Normalized ECG entries)
  Read q number of Differenced Normalized ECG entries
  cc = " "
  signVal = 0
  // Following codes performs sign encoding
  Loop ( $i = 1; i ++; i \leq q$ )
    if (ith entry is negative)
      signVal = signVal +  $2^{(q-1)}$ 
    endif
    cc = char(signVal)
  End Loop
  //Following codes performs the value encoding
  Loop ( $i = 1; i = i + 2; i \leq q$ )
    if (two consecutive entries are both single digit)
      cc = cc+ char((entry(i)  $\times$  10) + entry(i + 1))
    else
      cc = cc+char(entry(i))
      cc = cc+char(entry(i + 1))
    endif
  End Loop
End Loop

```

---

Table 2.4: Experimentation with Different Entries of MIT-BIH

MIT-BIH Entry	CR	Number of Simple Block Encode			Number of Complex Block Encode ( $o_l > 100$ )
		$o_l < 48$	$48 < o_l < 99$	Total	
100	4.05	9598	533	10131	669
102	4.01	9341	740	10081	719
105	3.85	8665	840	9505	1295
111	3.86	8311	1384	9695	1105
114	4.03	9129	1026	10155	645
201	3.97	9486	427	9913	887
210	3.93	9084	752	9836	964
213	3.56	5728	2801	8529	2271
222	4.05	9204	1067	10271	529
228	3.86	8001	1780	9781	1019
231	3.87	8966	771	9737	1063
234	3.93	9196	674	9870	930

Table 2.5: Comparison of the Proposed Method with Other Direct ECG Compression Algorithms

Compression Algorithms	Number of Operations Second	CR	PRD
Peak	90750.73	6.6	2.1
ZOP	913.62	4.7	2.6
SAPA	2081.38	5.5	2.4
Proposed method	2038.67	3.9	0

*Table 2.6: NOP/s Counting of ZOP Method*

MIT-BIH Entry	Add/sec.	Sub/sec.	Total NOP/s
100	360	163.93	883.93
102	360	169.55	889.55
105	360	193.533	913.53
111	360	213.03	933.03
114	360	196.516	916.516
201	360	160.35	880.35
210	360	185.06	905.066
213	360	268.96	988.966
222	360	198.62	918.62
228	360	219.216	939.216
231	360	182.6	902.6
234	360	172.08	892.08
Average	360	193.62	913.621



Table 2.7: Number of Operations per Second Counting of SAPA Method

MIT-BIH No	SlopCount/sec.	MinSlop/sec.	MaxSlop/sec.	Add./Sec	Div./sec.	Sub./Sec.	Total NOp/s
100	565.7	17.116	17.116	377.13	565.7	754.266	2091.33
102	565.45	16.96	16.96	376.96	565.45	753.93	2090.28
105	563.3	15.516	15.516	375.53	563.3	751.06	2080.93
111	557.5	11.66	11.66	371.66	557.5	743.33	2055.83
114	558.15	12.1	12.1	372.1	558.15	744.2	2058.65
201	569.05	19.366	19.366	379.36	758.73	758.73	2105.88
210	562.9	15.25	15.25	375.26	562.9	750.53	2079.2
213	557.85	11.88	11.88	371.9	557.85	743.8	2057.316
222	560	13.33	13.33	373.33	560	746.66	2066.66
228	557.7	11.78	11.78	371.8	557.7	743.6	2056.66
231	571.3	20.85	20.85	380.86	571.3	761.73	2115.6
234	571.9	21.26	21.26	381.26	571.9	762.53	2118.23
Average	563.4	15.589	15.589	375.5958	579.2067	751.1972	2081.381

Table 2.8: *NOp per Sec. Counting of Peak Method*

MIT-BIH Entry	Add./Sec.	Sub./Sec.	Div./Sec.	Multipl./Sec	Root/Sec.	Square/Sec.	Array List Add/Sec.	Array List Re- move/Sec.	Total Nop/Sec.
100	29772	29053.33	1076.03	1077.35	358.68	28694.66	360	358.66	90750.73
102	29772	29053.33	1076.03	1077.35	358.68	28694.66	360	358.66	90750.73
105	29772	29053.33	1076.03	1077.35	358.68	28694.66	360	358.66	90750.73
111	29772	29053.33	1076.03	1077.35	358.68	28694.66	360	358.66	90750.73
114	29772	29053.33	1076.03	1077.35	358.68	28694.66	360	358.66	90750.73
201	29772	29053.33	1076.03	1077.35	358.68	28694.66	360	358.66	90750.73
210	29772	29053.33	1076.03	1077.35	358.68	28694.66	360	358.66	90750.73
213	29772	29053.33	1076.03	1077.35	358.68	28694.66	360	358.66	90750.73
222	29772	29053.33	1076.03	1077.35	358.68	28694.66	360	358.66	90750.73
228	29772	29053.33	1076.03	1077.35	358.68	28694.66	360	358.66	90750.73
231	29772	29053.33	1076.03	1077.35	358.68	28694.66	360	358.66	90750.73
234	29772	29053.33	1076.03	1077.35	358.68	28694.66	360	358.66	90750.73
Avg.	29772	29053.33	1076.03	1077.35	358.68	28694.66	360	358.66	90750.73

Table 2.9: *NOp per Sec. Counting of the Proposed Method*

MIT-BIH Entry	Add./Sec.	Sub./Sec.	Multi./Sec.	Absolute/Sec.	ASCII Conv./Sec.	String Join	Total Nop/Sec.
100	720.96	360	360	149.78	236.15	180	2006.9
102	726.33	360	360	150.03	236.98	180	2013.35
105	749.58	360	360	152.42	246.58	180	2048.58
111	753.92	360	360	154.02	243.42	180	2051.35
114	735.48	360	360	156.88	235.75	180	2028.11
201	722.82	360	360	146.13	239.78	180	2008.73
210	736.93	360	360	152.27	241.07	180	2030.27
213	825.25	360	360	162.87	262.85	180	2150.97
222	730.97	360	360	155.55	233.82	180	2020.33
228	763.5	360	360	159.87	241.98	180	2065.35
231	735.47	360	360	147.18	242.72	180	2025.37
234	728.25	360	360	146.02	240.5	180	2014.77
Avg.	744.12	360	360	152.75	241.8	180	2038.673

*Table 2.10: Comparison of the Proposed Method with Other Lossless ECG Compression Algorithm*

Lossless ECG Compression Method	Highest Possible Compression Ratio with MIT/BIH Arrhythmia Database
Direct SPIHT (Method 1 of [Jalaleddine et al., 1990])	2.443
Direct SPIHT +BPC (Method 2 of [Jalaleddine et al., 1990])	3.011
DCCR+SPIHT (Method 3 of [Jalaleddine et al., 1990])	2.569
DCCR + SPIHT +BPC (Suggested Method of [Jalaleddine et al., 1990])	3.281
Entropy Coding of second-difference ECG [Kim et al., 2006]	2.800
Proposed Method	4.051

*Table 2.11: Realtime Compression / Decompression Factor for Pocket PC and Smart Phone*

Device Type	Realtime factor for compression (ms)	Realtime factor for decompression (ms)
HP iPAQ h2200 Pocket PC	0.233	0.15
HP iPAQ h6365 Smart Phone	0.416	0.266

Table 2.12: Further Compression with LZW based Compression Schemes

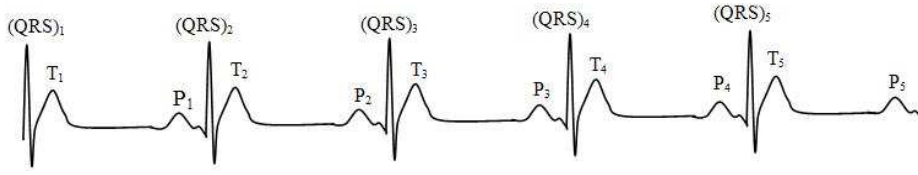
2*MIT BIH No.	2*S <sub>o</sub>	Encoding		Compression		2*CR <sub>t</sub>	2*T <sub>e</sub>	2*T <sub>c</sub>	2*T <sub>t</sub>
		S <sub>e</sub>	CR <sub>oe</sub>	S <sub>c</sub>	CR <sub>ec</sub>				
100	172197	45152	3.82	16355	2.76	10.5432	125	93	218
102	171033	44632	3.83	16341	2.73	10.4559	125	62	187
105	170912	47952	3.56	17306	2.77	9.8612	140	46	186
111	169280	46644	3.63	17330	2.69	9.7647	140	46	186
114	171214	44608	3.84	16526	2.70	10.368	140	62	202
201	171367	46163	3.71	16030	2.88	10.6848	140	93	233
210	170549	46454	3.67	16694	2.78	10.2026	156	78	234
213	168640	51573	3.27	19850	2.60	8.502	125	62	187
222	170355	44296	3.84	16581	2.67	10.2528	125	92	217
228	168208	46228	3.64	18075	2.56	9.3184	140	62	202
231	169048	46358	3.65	17004	2.73	9.9645	125	62	187
234	170184	46478	3.66	16799	2.77	10.1382	125	62	187

## Chapter 3

# ECG based Biometric Authentication

In the previous chapter, we have described a novel ECG compression algorithm that is fast in execution and can also provide high level of compression ratio. Patient's mobile phone executes the algorithm and sends the compressed ECG packets to the doctor/ hospital server. After receiving the compressed ECG packets the hospital server or the mobile phone requires to quickly authenticate the patient, before providing the patient with any services. Therefore, in this chapter, we present our innovative algorithms for ECG based biometric for remote authentication of CVD patients. Our second research question regarding faster authentication is answered in this chapter.

Since our telecardiology platform is based on compressed ECG for efficient transmission (as discussed earlier in Chapter 2), we focus our attention mainly on biometric authentication mechanisms that do not require decompression. On the other hand, telecardiology



*Figure 3.1: ECG Required for Biometric Recognition*

systems not harnessing the efficiency of compression algorithms [Hung and Zhang, 2003; Jasemian and Arendt-Nielsen, 2005; Gao et al., 2005; Zhou et al., 2005; Lee et al., 2007], need faster ECG biometric mechanisms based on plain ECG (not compressed). Therefore, in this chapter, we present four different algorithms to cater to the needs of all different forms of ECG transmission. Two of them are designed to work on plain ECG (Weighted Signal Processing (WSP) Approach and Polynomial Distance Measurement (PDM) Approach). It should be mentioned that WSP served as a preliminary assessment and feasibility study for our core contribution with PDM. On the other hand, the other two methods are suitable for compressed ECG (Direct Approach and Data Mining based Approach). Data Mining based approach is our core contribution for compressed ECG based biometric, while direct approach served as proof of concept for the same.

We start this chapter, with a brief background on ECG morphology and existing ECG based biometric, challenges faced by existing ECG biometric techniques, general steps of a biometric system and then detailing our four ECG based biometric methods that overcome the challenges faced by existing ECG biometric.

### 3.1 Related Works on ECG based Biometric

Biometrics has been a topic of research for the last 2 decades [Jain et al., 2004; Yu et al., 2008; Wubbeler et al., 2007; Biel et al., 2001; Israel et al., 2003; Kyoso and Uchiyama, 2001; Kyoso, 2003; Shen et al., 2002; Shen, 2005; Shen and Tompkins, 2005; Wang et al., 2008; Plataniotis et al., 2006; Irvine et al., 2001; Israel et al., 2005; Poon et al., 2006; Bui and Hatzinakos, 2008; Chan et al., 2008]. Biometric data can be acquired from several sources like DNA, ear, face, facial thermogram, fingerprint, gait, hand geometry, hand vein, iris, keystroke, odor, palm print, retina, signature, voice etc [Jain et al., 2004; Yu et al., 2008]. In recent years, fingerprint and iris have been most pervasively used in biometric authentications. Even joint fingerprint and ECG based multimodal biometric sensor is feasible, since recent study by [Chan et al., 2008] has already shown that person identification from ECG acquired from finger is possible. ECG biometric is possible because of difference in subtle patterns within these ECG waves or complexes, which is originated from the mechanical activities of the heart. Apart from reinforcing a stronger authentication technique by being a part of multimodal authentication, ECG can also be used as a standalone biometric authentication system [Jain et al., 2004; Yu et al., 2008; Wubbeler et al., 2007; Biel et al., 2001; Wang et al., 2008; Israel et al., 2003; Kyoso and Uchiyama, 2001; Kyoso, 2003; Shen et al., 2002; Shen, 2005; Shen and Tompkins, 2005; Plataniotis et al., 2006; Irvine et al., 2001; Israel et al., 2005; Poon et al., 2006; Bui and Hatzinakos, 2008; Chan et al., 2008].

One of the first attempts in establishing the fact that features extracted from the ECG can be used for person identification was shown by [Biel et al., 2001]. Since then there have been a surge of researches in ECG based biometric recognition [Jain et al., 2004; Yu et al.,



2008; Wubbeler et al., 2007; Biel et al., 2001; Wang et al., 2008; Israel et al., 2003; Kyoso and Uchiyama, 2001; Kyoso, 2003; Shen et al., 2002; Shen, 2005; Shen and Tompkins, 2005; Plataniotis et al., 2006; Irvine et al., 2001; Israel et al., 2005; Poon et al., 2006; Bui and Hatzinakos, 2008; Chan et al., 2008].

[Biel et al., 2001] have utilized many time domain features of ECG that were conventionally used for cardiovascular diagnosis purposes only. Some of the time domain features (features shown in Table 2.1) demonstrate a degree of uniqueness. This uniqueness of feature is the basis of biometric. It should be mentioned that the features associated with QRS complex shows the highest degree of uniqueness according to recent findings [Wubbeler et al., 2007]. Apart from the features shown in Table 2.1 (that remain unchanged over time), there are other features that varies over time such as RR Interval, Heart Rate Variability (HRV), Instantaneous Heart Rate (IHR) etc. RR Interval is the time difference between two consecutive heart beats. HRV is the reciprocal of the RR Interval ( $\frac{1}{RR}$ ) and IHR corresponds to heart rate calculated from a single RR Interval value ( $\frac{60}{RR}$ ). RR Interval, HRV, IHR features have also been used by [Wubbeler et al., 2007; Bui and Hatzinakos, 2008; Irvine et al., 2001] for person identifications.

Apart from the time domain ECG features, ECG based human identification is also possible with frequency domain features. [Chan et al., 2008] shows that employing wavelet based distance measurement techniques, ECG based biometric can attain a higher accuracy than different statistical approaches (e.g. Percentage Root-Mean-Square Deviation, Cross Correlation, etc.).

In addition to time domain and frequency domain features based techniques, there are

also other techniques that revolves around curve fitting (or polynomial based techniques). ECG biometric methods demonstrated in [Sufi et al., 2010a; Sufi and Khalil, 2008a; Khalil and Sufi, 2008a] fall under this category (details of [Sufi et al., 2010a] is described in Section 3.6).

### 3.2 Challenges Faced by Existing ECG based Biometric

The existing ECG based biometric authentication systems suffer from several pitfalls, which motivated us to pursue a new set of research on ECG based biometric. Few of these pitfalls of the existing ECG biometric techniques are summarized as follows:

- *Lack of Standardization of Fiducial Points:* Most of existing works related ECG biometric, including the earliest method shown in [Biel et al., 2001], rely heavily on the detection of ECG features namely the PQRST signature. Recent papers describe the ECG biometric performed in two possible ways; with or without fiducial point detection. ECG biometric based on fiducial point detection is inherently flawed as reported by recent research [Wang et al., 2008], since there is no standard definition as to where the ECG feature wave boundaries lie [Martinez et al., 2004]. Most of the medical grade ECG devices approximate these fiducial points since approximate locations are sufficient for medical diagnosis [Wang et al., 2008]. However, for the purpose of ECG being a biometric entity, the points need to be precise since the slightest variation of fiducial point locations will result in misclassifications within the enormous domain of human population (6.5 billion). The misclassification will be even severe when the same machine is not used for ECG acquisition, since each of the device vendors follows its own

definition of ECG wavelength boundaries [Wang et al., 2008].

- *Time Variant in Nature:* The second challenge inflicting the domain of ECG based biometric is the time varying nature of ECG. 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 for the same person [Israel et al., 2005], With the change of heart rates, different patterns like RR interval, QT interval, T duration of the ECG signal change for the same person [Srnmo and Laguna, 2003]. Therefore, if the acquired ECGs for the same person during both the enrolment stage and recognition stages are derived when the person is under different physiological conditions (exhausted, stressed, exercise, relaxed, anxious), most of the existing system on ECG based biometric will likely fail, since these time varying physiological changes were considered by very few algorithms [Israel et al., 2005]. Based on this time varying nature, which is one of the major challenges for ECG based biometric recognition, researchers have demonstrated the possibility of ensuring security on a body sensor network with multiple sensors communicating amongst themselves [Poon et al., 2006; Bui and Hatzinakos, 2008]. Researchers in [Poon et al., 2006; Bui and Hatzinakos, 2008] have proposed a scenario 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. 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 located within the same body. For these cases, the randomness and biometric nature of the heart is used as a substitute for a session

key for a secured communication.

- *Pertinence of random abnormality:* Certain random traces of ECG abnormality can prevail in normal person, ruining the ECG signature, which may result in misclassification for biometric recognition. One of these abnormalities is ectopic beat which often goes unnoticed for a normal person. Hardly any of the existing biometric recognition techniques employed any algorithms to deal with automated detection of non-standard beats. Application of only simple beat averaging techniques employed by earlier researches [Shen et al., 2002; Shen, 2005; Shen and Tompkins, 2005] results in the storage of faulty template, giving misclassifications when applied to few seconds of ECG acquisition with an ectopic beat present.
- *Longer duration for ECG acquisition:* For a biometric system to be widely accepted, the time required to acquire the biometric data should be as minimal as possible. Present biometric solutions based on finger print take less than a second of acquisition time, which is one of the reasons of fingerprint being pervasively accepted where urgency is crucial (military operations, medical service providers etc.). Many of the previous researches adopted beat averaging for 20 beats, which might take up to 20 seconds of acquisition time. Therefore, these ECG based biometric systems are not feasible for time critical operations.
- *Lack of portability and higher computational cost:* One of the major challenges in the world of biometrics is reduction of the number of features for biometric recognition. Therefore, principal component analysis and similar measurements have been obtained

by earlier works on ECG biometrics [Biel et al., 2001; Israel et al., 2005]. The sizes of the templates for iris, face and voice are 512 bytes, 150-300 Kbytes and 2-10 Kbytes respectively [Yu et al., 2008]. Even the most recent work demonstrated on ECG based human identification requires at least 600 bytes (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 a biometric template (enrolment / verification data) [Wubbeler et al., 2007]. Even though the size of the template appears to be insignificant, when this information is matched using the  $O(N^2)$  algorithm, across a recognition database on only 100 people, the computational latency/cost is noticeable for many of the existing ECG biometric systems [Chan et al., 2008; Wang et al., 2008; Plataniotis et al., 2006]. Therefore, for organizations comprising of thousands of the workers, many of the existing biometric algorithms are unsuitable for commercialization, even though their research value is significant. Therefore, an algorithm where one-to-many matching is performed only for limited number of values (vectors with minimal elements) is an optimal choice for future ECG based biometric system seeking commercial exposure.

Apart for all these challenges, research communality is continuously endeavoring for more accurate biometric solutions. All the previous researches related to ECG based biometric system [Jain et al., 2004; Yu et al., 2008; Wubbeler et al., 2007; Biel et al., 2001; Israel et al., 2003; Kyoso and Uchiyama, 2001; Kyoso, 2003; Shen et al., 2002; Shen, 2005; Shen and Tompkins, 2005; Wang et al., 2008; Plataniotis et al., 2006; Irvine et al., 2001; Israel et al., 2005; Poon et al., 2006; Bui and Hatzinakos, 2008; Chan et al., 2008] show moderate level of accuracy in identifying person by template matching or

feature comparison techniques.

Existing ECG based biometric systems are constantly being challenged by higher misclassification error, longer acquisition time, larger template size, slower processing time and pertinence of abnormal beats within the biometric template. These challenges are the prime hindrance for ECG based biometric being commercialized as a pervasive authentication mechanism. At least, ECG based biometric can provide a secured mechanism for cardiac patients being monitored over telephony network.

### 3.3 Stages of Biometric Systems

A conventional biometric system has the following three stages:

- **Enrolment Stage:** In this stage, the biometric entity (ECG recordings, Fingerprint, Handprint, Retina etc.) is acquired and used as a template. This template is saved in a biometric template database along with other templates from different individuals. At later stages of verification or identification, this template is used for template matching purposes.
- **Verification Stage:** During this stage, the system validates the claimed identity of a particular person. The person provides a PIN number, name or smart card to identify himself and his acquired biometric entity is matched (one to one matching) with his own template, which was acquired during an earlier stage of enrolment.
- **Identification Stage:** At this stage, an individual's biometric entity is recorded and template matching is performed throughout the biometric template database records.

After this one to many matching, whenever a match is found within a set threshold the individual is identified. In 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 case of no match, the person remains unidentified.

Throughout this chapter, the biometric entity template is referred as enrolment data and the data acquired during the verification or identification stage is termed as recognition data.

### 3.4 Types of ECG Biometric

In this chapter, we will present four different types of ECG biometric techniques, which we developed during the course of this research. These four techniques, namely Weighted Signal Processing (WSP) Approach, Polynomial Distance Measurement (PDM) Approach, Direct Approach on compressed ECG and Data Mining (DM) Approach on Compressed ECG, will be detailed in the following four sections.

WSP Approach and PDM Approach are designed to work for telemonitoring based on uncompressed ECG (i.e. ECG is not transmitted and maintained in compressed format [Hung and Zhang, 2003; Lee et al., 2007; Gao et al., 2005; Zhou et al., 2005; Blount et al., 2007; Jasemian and Arendt-Nielsen, 2005]). On the other hand, Direct Approach and DM Approach on compressed ECG work on tele-monitoring platforms that transmit and maintain ECG in compressed format. As mentioned earlier, PDM method of ECG biometric is our core contribution on biometric from plain ECG. On the other hand, DM approach on

compressed ECG is our core contribution on compressed ECG based biometric.

### 3.5 Weighted Signal Processing (WSP) Approach

Researchers have used Percentage Root-Mean-Square Deviation (PRD) [Zigel et al., 2000b], Cross Correlation (CC) [Last et al., 2004] and Wavelet Distance Measurement (WDM) [Chan et al., 2008] techniques on enrolled ECG and recognition ECG to successfully identify persons [Chan et al., 2008].

PRD is widely used to measure the quality of reconstructed ECG after lossy ECG compression [Chan et al., 2008], PRD provides a measurement of dissimilarity between two signals as in Eq. 3.1.

$$PRD = \sqrt{\frac{\sum_{i=1}^N [x(i) - \hat{x}(i)]^2}{\sum_{i=1}^N [x(i)]^2}} \times 100 \quad (3.1)$$

CC is a technique used in statistics to match the similarity of two vectors or signals as represented in Eq. 3.2 [Chan et al., 2008]. We employed CC using Eq. 3.2 as it was utilized by previous studies [Chan et al., 2008], for ECG based biometric recognition.

$$r_{cc} = \frac{1}{M} \sum_{i=1}^N x(i) \times \hat{x}(i) \quad (3.2)$$

The ECG waveform can be comprised of multiple pulses, where the timing and shape of the pulses provide the distinguishing characteristics of the waveform. Wavelets offer a means



of representing a signal in a manner that simultaneously provides both time and frequency information; hence, it would provide an appropriate representation of the ECG waveform. Detail coefficients of the discrete wavelet transform  $\lambda^{q,v}$ ; detail coefficient  $v$  from the  $q$ th level of decomposition are computed for each signal. Using these coefficients, a distance is computed as WDM.

The numerator of Eq. 3.3 is the absolute difference of the wavelet coefficients from the recognition data 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 unknown signal. The denominator also includes a threshold value ( $\xi$ ) to avoid relatively small wavelet coefficients from overemphasizing differences. For the WDIST measure, the person associated with the enrolled data with the lowest WDIST is selected as a match. For this WDM, the mother wavelet was chosen to be sym5 with a five-level decomposition.

$$WDIST = \sum_{q=1}^Q \sum_{v=1}^V \frac{|\gamma_0^{q,v} - \gamma_z^{q,v}|}{\max(|\gamma_0^{q,v}|, \xi)} \quad (3.3)$$

We have also implemented similar ECG based biometric authentication with the intention of using it as a metric for measuring successful ECG anonymization (for securing ECG), as well as for ECG based authentication (i.e. ECG biometric). In [Chan et al., 2008], all the three methods (PRD, CC and WDM) resulted in misclassifications. Therefore, our initial thought was to implement a weighted approach involving all these three techniques.

First, determination of threshold values for PRD, CC and WDM for successful identifica-

tion is required. To obtain these thresholds, 15 subjects were taken for ECG acquisition and the ECGs were stored in an SQL Server database. These ECGs were used as templates (enrolled data) for biometric recognition. After one month, ECGs from the same subject group were taken to be used as recognition data. Therefore, ECGs collected at different times from the same subject (one to one matching) were used for the calculation of PRD, CC and WDM. This particular experiment provided the knowledge of the threshold for successful person identification. We call it thresholds for successful identification, since two ECGs from the same person were utilised for the threshold calculation. Figure 3.2 shows the enrolment ECG for the first five subjects. Figure 3.3 shows the recognition ECG for the same 5 subjects acquired one month after the collection of their enrolment ECG. Table 3.1 shows the variance of values for PRD, CC and WDM for different persons (same persons ECG were used for calculation).

For all the cases, PRD were less than 13.3, CC greater than 0.0351 and WDM were less than 5.4. Accounting calculation and experimentation errors PRD, CC and WDM values for identification were determined to be less than 14, greater than 0.051 and less than 6, respectively. Therefore, based on the experimentation result, we concluded that following are the conditions for a person being unidentified:

- $PRD > 14$  (since all PRD values were less than 13.3 during successful identification)
- $CC < 0.055$  (since all CC values were greater than 0.051 for successful identification)
- $WDM > 6$  (since all WDM values were less than 6)

After the successful discerning of the thresholds for identification, the condition was hard-

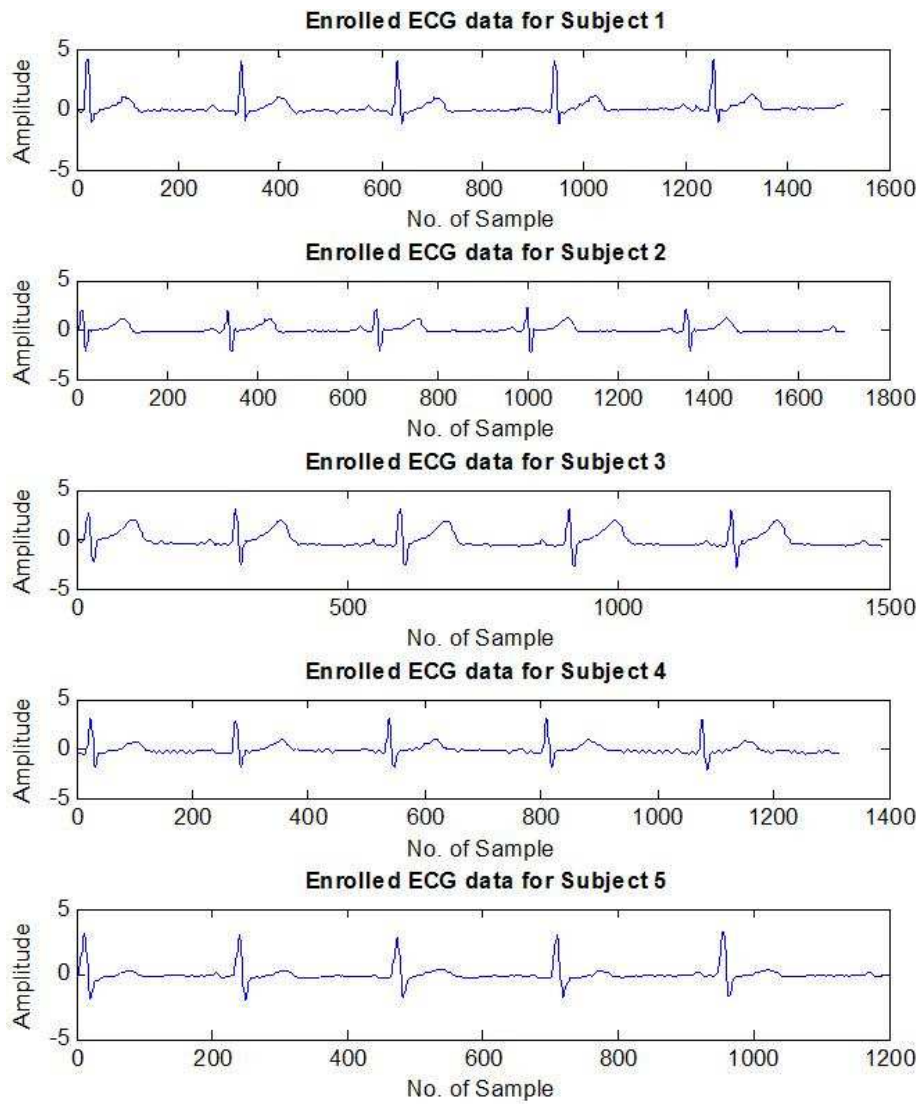


Figure 3.2: The ECG Template (Enrolment ECG) for the First Five Subjects

Table 3.1: Variance of Values for PRD, CC and WDM on Different Subjects. <sup>1</sup> = Enrolment ECG and <sup>2</sup> = Recognition ECG. The Enrolment and Recognition ECGs are in Bytes.

Subject	PRD	CC	WDM	CL	Length	EECG <sup>1</sup>	RECG <sup>2</sup>
1	11.3	0.16449	5.576	73.49925	1511	16,273	14,611
2	13.116	0.072614	4.2031	70.4348	1701	16,554	16,555
3	12.387	0.1375	3.7496	73.46595	1488	14,153	14,090
4	13.194	0.059062	4.0596	70.89825	1314	12,783	12,838
5	13.109	0.068704	3.141	71.11985	1195	11,749	11,663

coded to develop a rule based ECG biometric system. The whole system was implemented under .Net environment with MS Visual Studio 2005. Enrolment data were maintained in SQL Server 2000. Biopac system was used for ECG acquisition (enrolment, verification and identification). The software system presented in Figure 3.4 requires the location of the ECG file containing recognition data (captured with biopac system). After locating the ECG file, *Identify Person* option performs template matching (using PRD, CC and WDM) across the SQL Server database (one to many). The best match (the profile of the identified) pulled up from the database and presented by the system. Recognition data is also shown on the screen. However, the recognition ECG data contains vital cardiovascular details [Kusumoto, 2009]. Therefore, only selected personnel with proper authorization will be able to view this ECG signal. Otherwise, only noised ECG is shown. This noise obfuscation procedure has been explained in the next chapter of this thesis.

### 3.6 Polynomial Distance Measurement (PDM)

The history of polynomial being used in signal processing tasks for filtering noisy signals, interpolation of data and data compression started about 30 years ago [Hou and Andrews, 1978; Liou, 1976; Sandman and Sapir, 1988]. However, polynomials being used for ECG data

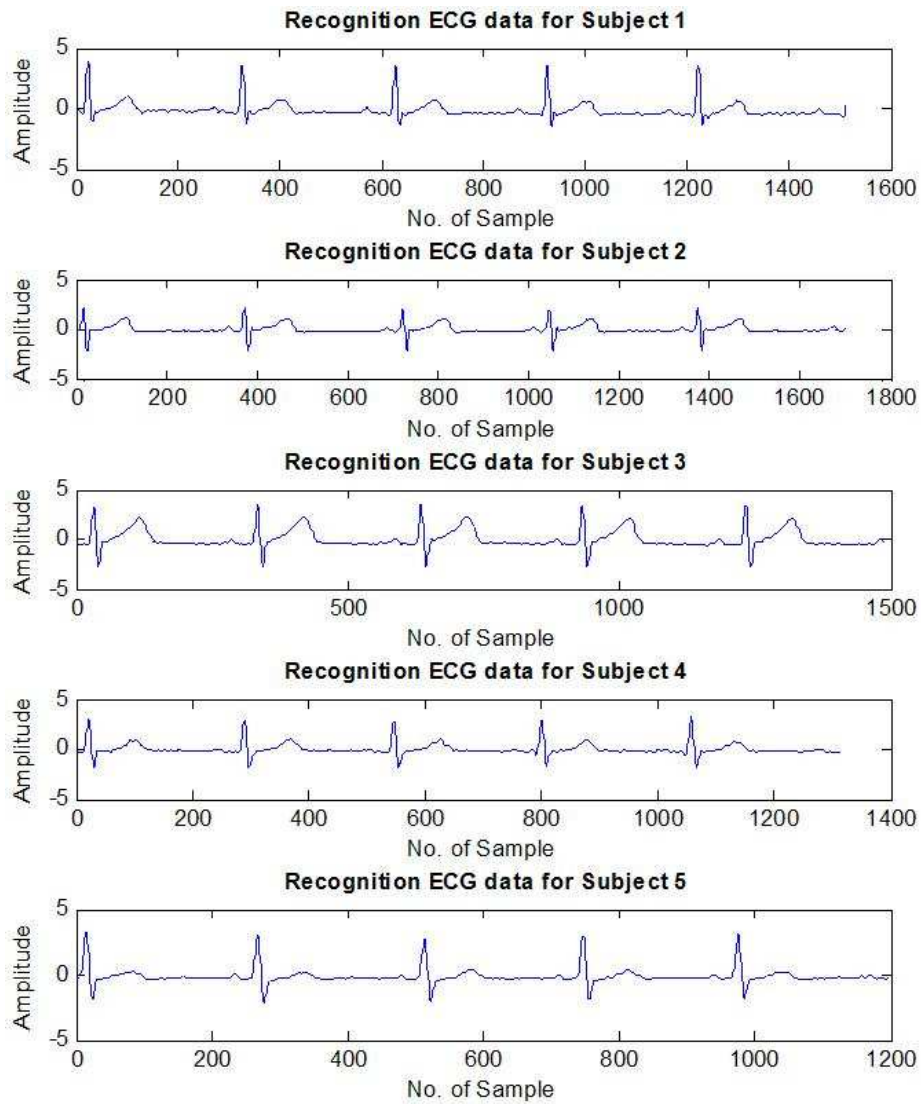


Figure 3.3: Recognition ECG (for Verification or Identification) for the First Five Subjects

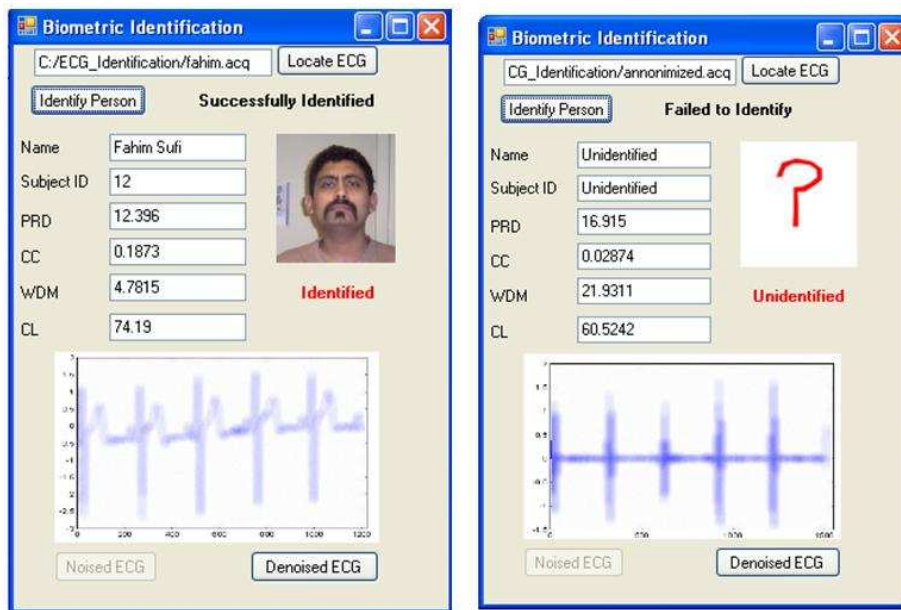


Figure 3.4: Front End of the Implemented (Using .Net) ECG Biometric System

processing have a history of 15 years [Philips and Jonghe, 1992; Philips, 1993; 1996; Poli et al., 1995; Linh et al., 2003]. Polynomials entered the arena of ECG signal processing with ECG data compression [Philips and Jonghe, 1992; Philips, 1993], then ECG noise removal [Philips, 1996] and recently it has been bringing about promising solutions for heart beat recognition problem [Poli et al., 1995; Linh et al., 2003]. Apart from that, polynomial has long been used for biometric authentication purposes such as fingerprint based biometric authentications [Nandakumar et al., 2007; Toh et al., 2004].

In this section, we propose a polynomial based ECG biometric detection. The application Polynomial Distance Measurement (PDM) has never been explored for ECG based biometric, according to the best of our knowledge. Apart for implementing a new approach for ECG biometric, the proposed PDM model has the following contributions towards ECG biometric:

- Performs faster than many of the existing ECG biometric algorithms (12 times, 8.33

times and 4.82 times faster than PRD, WDM and CC based methods [Chan et al., 2008]).

- Possesses a reduced feature set resulting storage and transmission efficiency (6.5 times for PRD/CC [Chan et al., 2008], 4.03 times for WDM [Chan et al., 2008], 1.74 times for [Wubbeler et al., 2007])
- Provides higher feasibility for biometric authentication with lower acquisition time (only 2.49 s on average)
- Inherits reduced misclassification errors compared to previous models (as low as 0%)
- Shows a degree of robustness in dealing with abnormal beats that may occupy with normal ECG signals

Apart from these contributions, the proposed PDM was deployed on a multilayer authentication mechanism for mobile phone based telemonitoring to demonstrate its applicability in realtime patient healthcare monitoring. This obviates the need to collect any additional biometric data, since ECG, which is being monitored for cardiac health, is also used for biometric authentication.

### 3.6.1 System & Method for PDM Biometric

In the proposed PDM based ECG biometric approach, ECG features are extracted before obtaining the polynomial coefficients of the ECG features. The difference between the enrolment and recognition coefficients is crucial for PDM Biometric. Mathematically, ECG can be represented by Eq. 3.4.

$$x(n) = \{x(1), x(2), x(3), \dots, x(N)\} \quad (3.4)$$

where  $N$  is the length of the ECG signal. If  $x(n)$  is the enrolment ECG, recognition ECG can be represented by Eq. 3.5.

$$\hat{x}(n) = \{\hat{x}(1), \hat{x}(2), \hat{x}(3), \dots, \hat{x}(N)\} \quad (3.5)$$

In our proposed PDM method, the complete ECG biometric is performed in three basic steps:

### **ECG Feature Extraction**

During both enrolment and recognition steps, the original ECG is processed first to detect all the fiducial points, namely QRS complex, T wave and P wave (Step 2, Figure 3.5). This detection of ECG features is performed by using our own ECG feature extraction technique, which is presented in chapter 4. This ECG feature extraction method basically extracts the different ECG features based on the similarity between the subset of ECG and an input feature template by using Eq. 3.6. The input feature template,  $f(m)$ , can be P wave, T wave or QRS complex.  $M$  is the length of the feature template. Equation 3.6 is evaluated in a window sliding fashion with  $j = 0$  to  $(N - M)$  to ascertain the similarity vector,  $r(j)$ , presented in Eq. 3.7. During sliding, the local maximas above the similarity threshold



(experimentally 92%) are stored as the possible candidates for ECG features (within feature vectors). Therefore, final outcome of the feature extraction process is P vector, P (comprising of all P waves), QRS vector, QRS (comprising of all QRS complexes) and T vector, T (comprising of all T waves) (Eq. 3.8-3.10).

$$r(j) = \left( 1 - \sqrt{\frac{\sum_{m=1}^M [x(m+j) - f(m)]^2}{\sum_{m=1}^M [x(m+j) - \bar{x}]^2}} \right) \times 100 \quad (3.6)$$

During this sliding process only the value of  $j$  is incremented and therefore,  $j = 1, 2, 3, \dots, (N - M)$

$$r(j) = \{r(1), r(2), r(3), \dots, r(N - M)\} \quad (3.7)$$

$$P = \{p(1), p(2), p(3), \dots\} \quad (3.8)$$

$$QRS = \{qrs(1), qrs(2), qrs(3), \dots\} \quad (3.9)$$

$$T = \{t(1), t(2), t(3), \dots\} \quad (3.10)$$

Cardinalities of P, QRS and T are dependent on the acquisition time for both enrolment

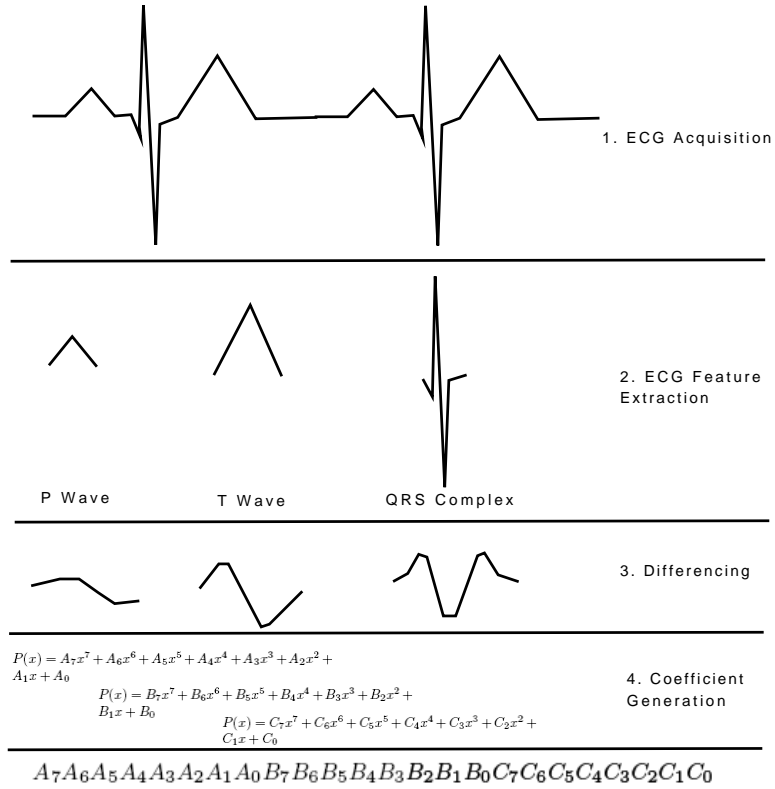


Figure 3.5: Coefficient Generation Process with Polynomial

and recognition stage. However, these cardinalities are independent of the ECG sampling frequency during data acquisition process.

### Coefficient Generation for PDM

After the detection of the ECG features, those features ( $\forall P, \forall QRS, \forall T$ ) are first differentiated (Step 3, Figure 3.5) using Eq. 3.11.

$$y(l) = x(n) - x(n - 1) \tag{3.11}$$

where  $l = 1, 2, 3, \dots, (M - 1)$ . The first differenced values are then used to construct a polynomial equation (approximated) (Step 4, Figure 3.5). In general, the approximated polynomials take the form of Eq. 3.12.

$$y = C_0 + \sum_{i=1}^I C_i \times x^i \quad (3.12)$$

These accumulated coefficients create the coefficient sets for P wave, T wave and QRS complex as seen in Eq. 3.13-3.15.

$$C_P = C_1^P, C_2^P, C_3^P, \dots, C_A^P \quad (3.13)$$

$$C_T = C_1^T, C_2^T, C_3^T, \dots, C_B^T \quad (3.14)$$

$$C_{QRS} = C_1^{QRS}, C_2^{QRS}, C_3^{QRS}, \dots, C_D^{QRS} \quad (3.15)$$

where, A, B and D are the lengths of the coefficient sets for P wave, T wave and QRS complex respectively. From the coefficient sets, the order of the polynomial can be obtained by following:

$$A = |C_P| - 1, B = |C_T| - 1, D = |C_{QRS}| - 1 \quad (3.16)$$

Therefore, the entire polynomial can be recreated just from the transmitted coefficient to the other side. The heart vector is created with combining the coefficients generated from the polynomial equations for P wave, T wave and QRS complex. Therefore, the heart vector is the union of  $C_P$ ,  $C_T$  and  $C_{QRS}$  as shown in Eq. 3.17.

$$h = C_P \cup C_T \cup C_{QRS} \quad (3.17)$$

Similarly, recognition heart vector can be obtained from the recognition data and modeled as

$$\bar{h} = \bar{C}_P \cup \bar{C}_T \cup \bar{C}_{QRS} \quad (3.18)$$

### Polynomial Distance Measurement (PDM) Process

The coefficients of the polynomial equation are used as the biometric feature, which is compared against the same (extracted features) for recognition data. At the beginning of the proposed PDM method, the system extracts all the coefficients from both enrolment heart vector,  $h$  and recognition heart vector,  $\bar{h}$ . Then, the distances from the coefficients are

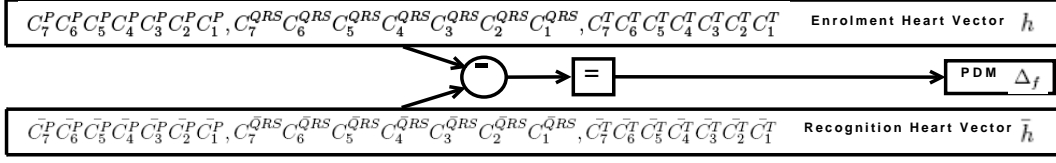


Figure 3.6: Polynomial Distance Measurement

measured using Eq. 3.19-3.21.

Whenever, this distance (calculated from both the enrolment data and recognition data) lies within a set threshold, person identification is thought to be successful.

$$\Delta_P = \sum_{i=0}^A \frac{|C_i^P - \bar{C}_i^P|}{C_i^P} \quad (3.19)$$

$$\Delta_T = \sum_{i=0}^B \frac{|C_i^T - \bar{C}_i^T|}{C_i^T} \quad (3.20)$$

$$\Delta_{QRS} = \sum_{i=0}^D \frac{|C_i^{QRS} - \bar{C}_i^{QRS}|}{C_i^{QRS}} \quad (3.21)$$

In an ideal case, for an identity,  $S_k$ , following condition should be met:  $\min(\Delta_P(k)) \wedge \min(\Delta_P(k)) \wedge \min(\Delta_P(k))$ , where,  $k = 1, 2, 3, \dots, K, K + 1$ .  $S_{K+1}$  simply means no identity could be matched. Thus, the proposed ECG biometric model is based on Polynomial Distance Measurement (PDM) between the enrolment data and recognition data.

### 3.6.2 Experimentation & Results for PDM

A total of 25 healthy subjects were employed for validation of the proposed biometric system. GE Mac 5500 ST stress testing ECG acquisition device was used for data acquisition purposes. This device is equipped with automatic noise cancellation feature, to provide uniformity in the recorded data. Using the on screen menu the data was saved on to an SD card, in XML format. The acquired ECG files were then transferred to the computer for further analysis. However, to decode the GE proprietary format of ECG to computer readable ECG format, a .Net data conversion software were written. The conversion software only selected lead I data and converted it to binary format. Then from the binary format, data was read in little Endian format. Finally, the formatted data were multiplied with 4.88 to retrieve amplitude (in millivolts) for the acquired ECG samples. Three healthy beats were taken for pre-processing and feature extraction (on average), during both enrolment and recognition. Figure 3.7, 3.8, 3.9 and 3.10 show the approximated polynomials created during the enrolment stage. After obtaining data at a later recognition phase, the polynomials were created again. These figures make it apparent that inter person polynomials for the ECG features are different. Table 3.2, 3.3 and 3.4 also reflexes the same fact that the coefficients derived from different persons for P wave, T wave and QRS complex are dissimilar, which is the basis of the proposed PDM approach. Table 3.5, 3.6 and 3.7 reflects the crucial fact that human identification is possible by matching his/her coefficients obtained at different times. The distances were measured, using Eqs. 3.19, 3.20 and 3.21. For 23 cases out of total 25 subjects, the 85% of the recognition coefficients lied within coefficient boundaries provided by 95% confidence level curves, which was calculated from the approximated enrolment

*Table 3.2: Dissimilarity of Coefficients for P Wave Across 5 Subjects*

Coef.	Subject 1	Subject 2	Subject 3	Subject 4	Subject 5
C1	-1.327e-006	-7.586e-007	-4.975e-013	-1.955e-012	1.051e-012
C2	8.751e-005	4.989e-005	9.305e-011	4.172e-010	-2.383e-010
C3	-0.001955	-0.001101	-6.783e-009	-3.699e-008	2.25e-008
C4	0.01679	0.008849	2.336e-007	1.767e-006	-1.146e-006
C5	-0.04484	-0.02414	-3.245e-006	-4.932e-005	3.417e-005
C6	0.02343	0.09011	-1.589e-005	0.0008172	-0.0006048
C7	-	-	0.0009748	-0.007817	0.006164
C8	-	-	-0.009851	0.04007	-0.03322
C9	-	-	0.03505	-0.09481	0.07834
C10	-	-	-0.02285	0.08755	-0.04594

*Table 3.3: Dissimilarity of Coefficients for T Wave Across 5 Subjects*

Coef.	Subject 1	Subject 2	Subject 3	Subject 4	Subject 5
C1	2.604e-011	2.716e-010	-6.759e-012	1.842e-016	3.619e-016
C2	-4.502e-009	-4.94e-008	2.605e-009	-6.463e-014	-1.94e-013
C3	3.093e-007	3.48e-006	-2.603e-007	8.639e-012	4.108e-011
C4	-1.074e-005	-0.000119	6.382e-006	-5.641e-010	-4.505e-009
C5	0.0002	0.002031	0.0001737	2.274e-008	2.794e-007
C6	-0.001996	-0.01618	-0.00717	-1.003e-006	-9.997e-006
C7	0.01056	0.0529	0.06448	4.516e-005	0.0002012
C8	-0.02643	-0.02168	-	-0.001094	-0.002081
C9	0.04858	-	-	0.01083	0.008961
C10	-	-	-	-0.02014	-0.002099

polynomials.

During our experimentation, we found that QRS complex inherits the most uniqueness, which is required for successful person identification. For the successful candidate (recognized person), the value of distance was always less than 4.69. However, this distance for QRS complex would soar as high as 51 for wrong person. T wave showed moderate level of uniqueness for person identification, which can contribute towards higher confidence level for person identification with QRS complex only. However, P wave possessed the lowest level of uniqueness, while varying the most (4 to 76). Our conjecture for this lower level of

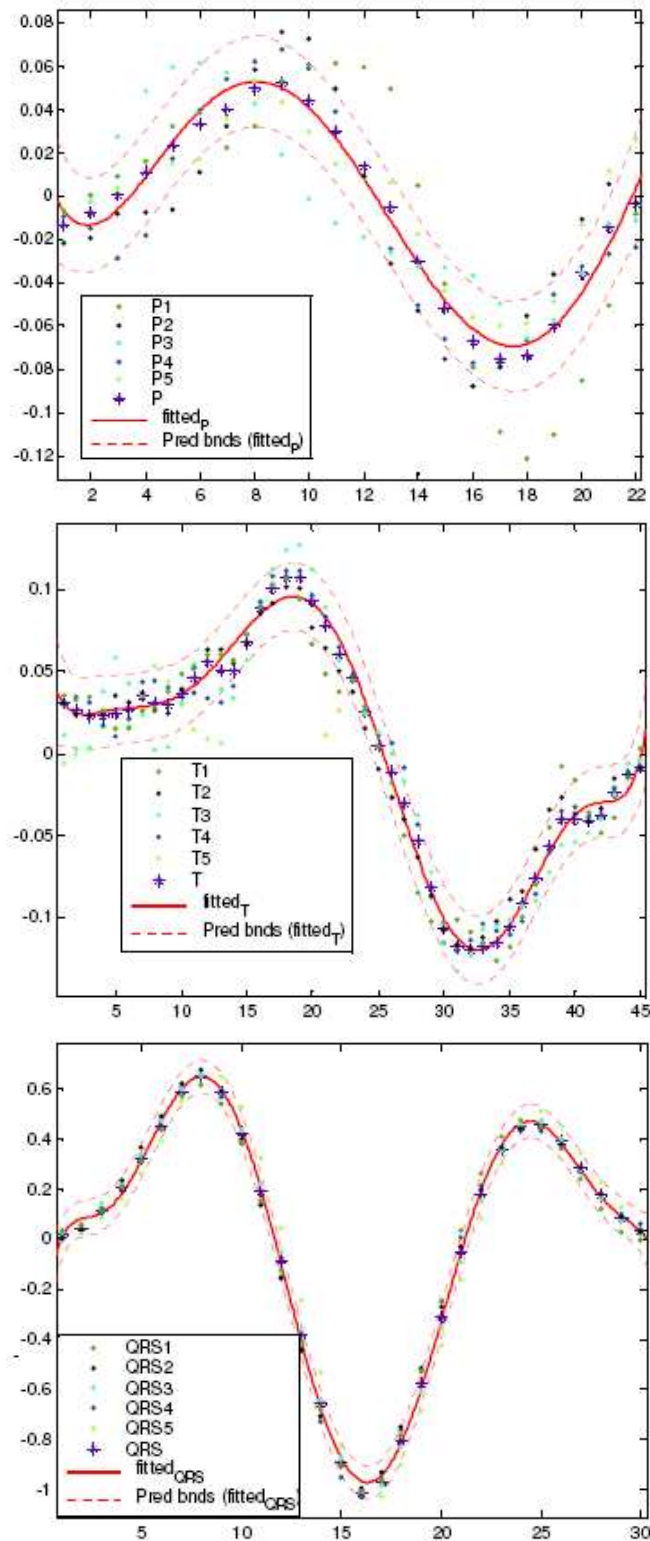


Figure 3.7: Polynomial Creation for Subject 5 (for P Wave, T Wave and QRS Complex)



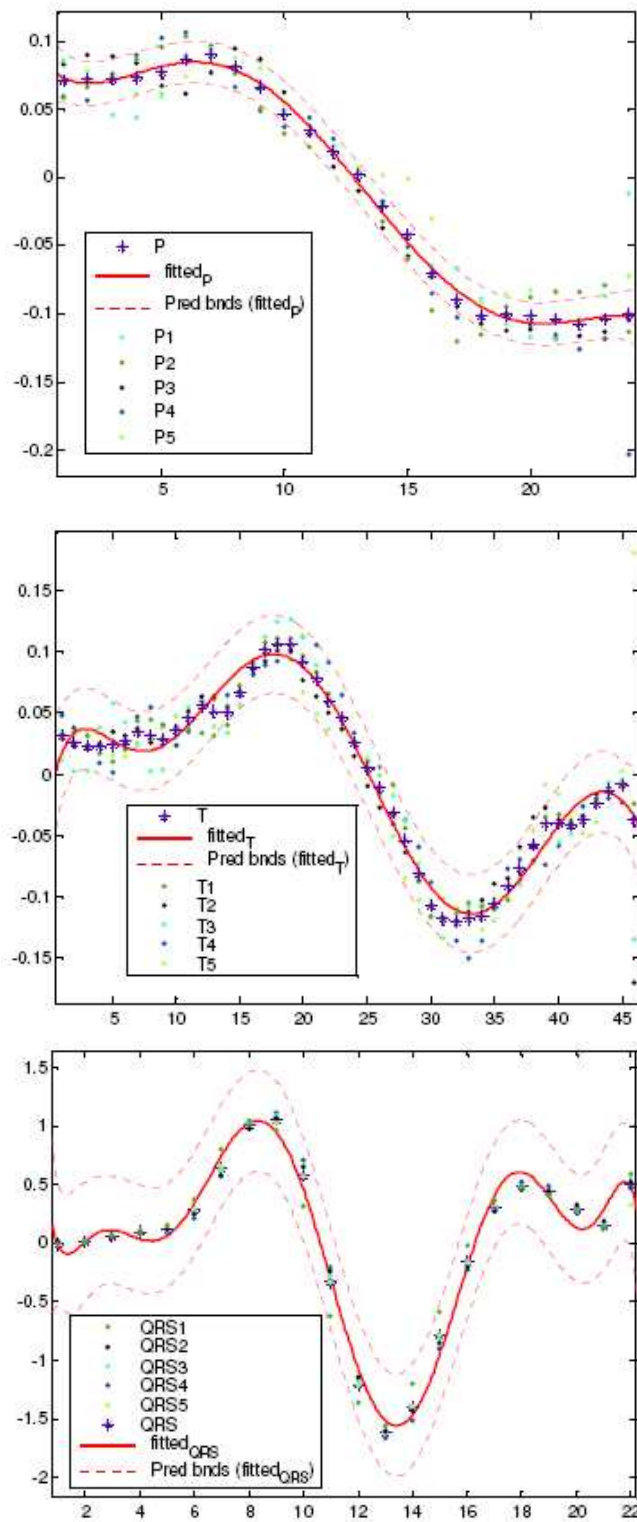


Figure 3.8: Polynomial Creation for Subject 10 (for P Wave, T Wave and QRS Complex).

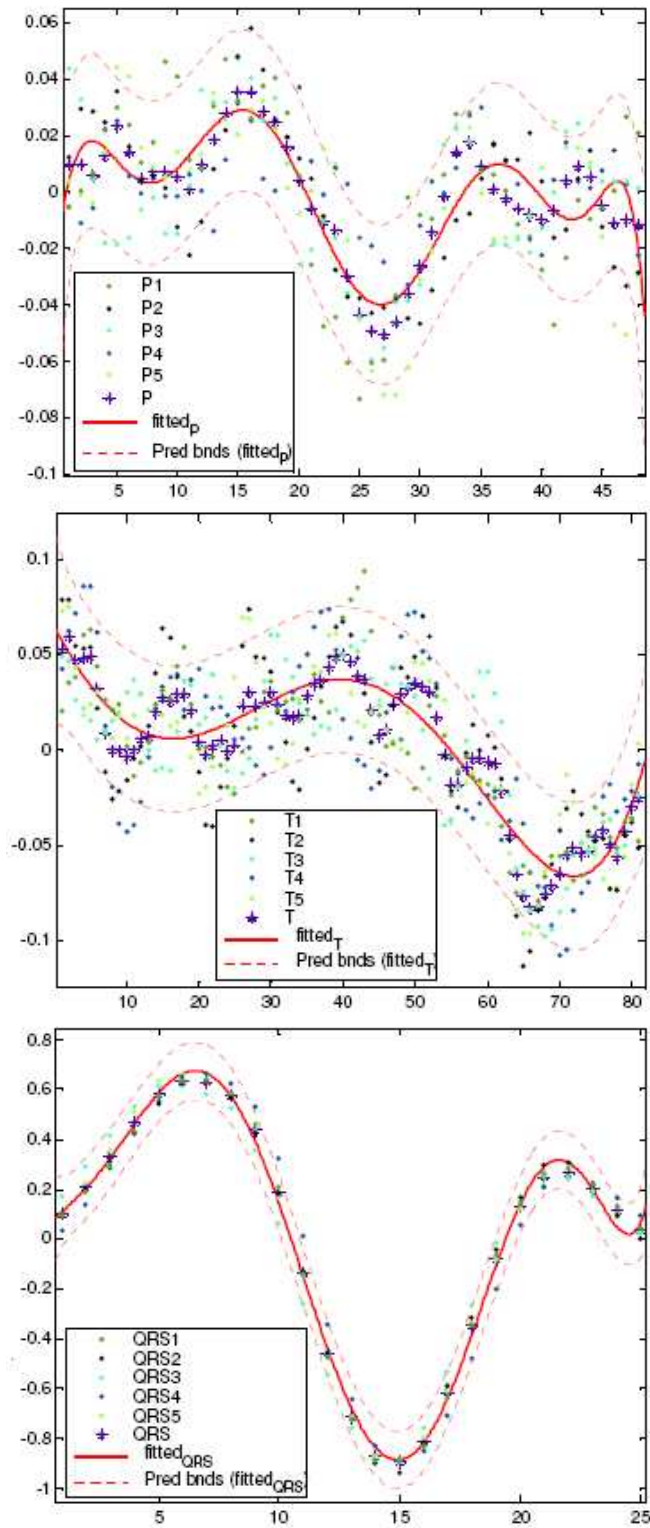


Figure 3.9: Polynomial Creation for Subject 15 (for P Wave, T Wave and QRS Complex).

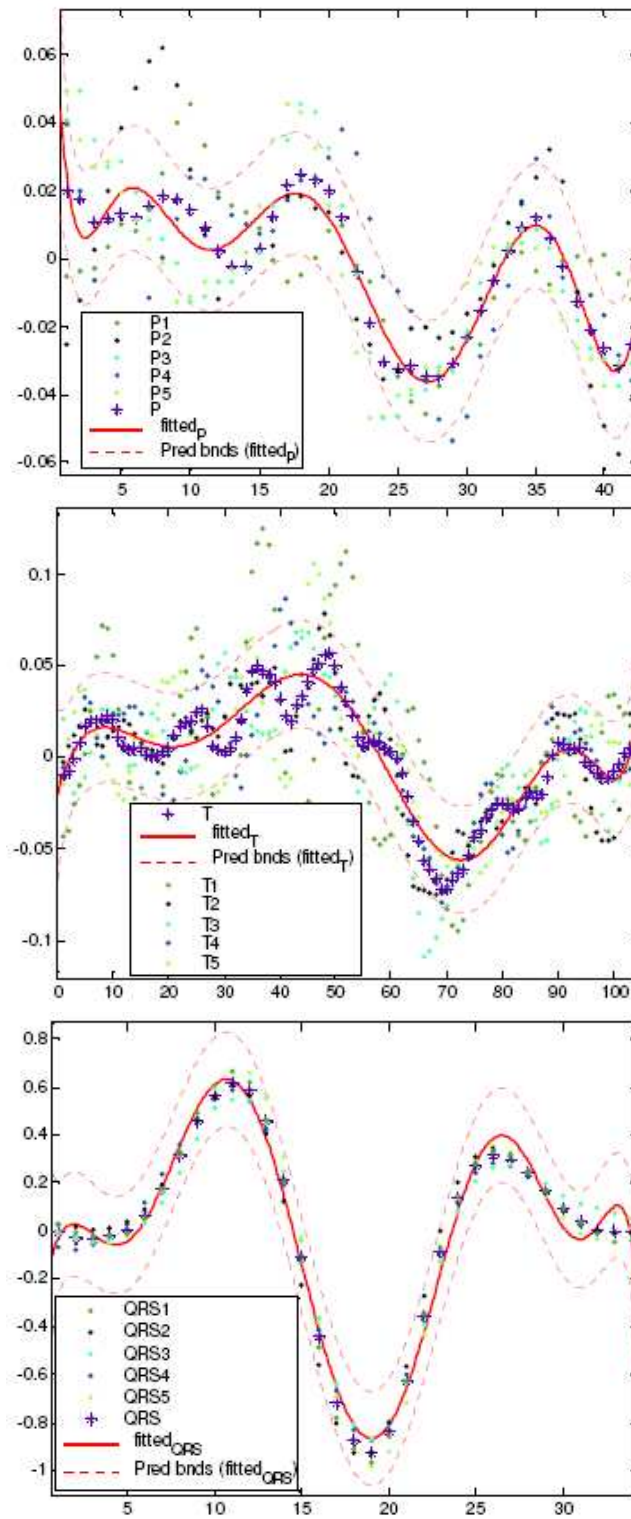


Figure 3.10: Polynomial Creation for Subject 20 (for P Wave, T Wave and QRS Complex).

Table 3.4: Dissimilarity of Coefficients FOR QRS Complex Across 5 Subjects

Coef.	Subject 1	Subject 2	Subject 3	Subject 4	Subject 5
C1	-6.103e-009	-4.016e-008	1.593e-007	-1.858e-010	-9.457e-014
C2	7.831e-007	4.081e-006	-1.287e-005	2.518e-008	3.318e-011
C3	-4.039e-005	-0.0001724	0.0003861	-1.338e-006	-4.829e-009
C4	0.001066	0.003916	-0.005221	3.439e-005	3.778e-007
C5	-0.01513	-0.05185	0.03069	-0.0003999	-1.723e-005
C6	0.1124	0.4063	-0.07337	0.0006271	0.0004647
C7	-0.4075	-1.845	0.1677	0.02647	-0.007194
C8	0.7095	4.597	-0.01157	-0.1988	0.05886
C9	-0.397	-5.572	-	0.4743	-0.2125
C10	-	-	-	-0.337	0.2189

Table 3.5: Similarity of P Wave Coefficients for an Individual Across all the ECG Features

Coef.	Upper Boundary	Instance 1	Instance 2	Instance 3	Lower Boundary
C1	-1.836e-006	-3.387e-006	-3.452e-006	-9.171e-007	-8.181e-007
C2	5.812e-005	0.0002062	0.000211	6.383e-005	0.0001169
C3	-0.002574	-0.00441	-0.004527	-0.001475	-0.001336
C4	0.01103	0.03852	0.03975	0.013	0.02255
C5	-0.06743	-0.1199	-0.1251	-0.03635	-0.02225
C6	-0.004528	0.08586	0.08779	0.02507	0.05138

Table 3.6: Similarity of T Wave Coefficients for an Individual Across all the ECG Features

Coef.	Upper Boundary	Instance 1	Instance 2	Instance 3	Lower Boundary
C1	1.889e-011	2.578e-011	2.381e-011	1.961e-011	3.319e-011
C2	-5.82e-009	-4.434e-009	-4.031e-009	-3.199e-009	-3.184e-009
C3	2.093e-007	3.039e-007	2.697e-007	1.996e-007	4.094e-007
C4	-1.478e-005	-1.06e-005	-9.047e-006	-5.774e-006	-6.708e-006
C5	0.000107	0.0002017	0.0001606	6.972e-005	0.0002929
C6	-0.003221	-0.002141	-0.001504	-2.109e-005	-0.0007716
C7	0.001847	0.01287	0.007369	-0.005691	0.01927
C8	-0.05548	-0.03952	-0.01663	0.03598	0.002614
C9	0.01628	0.0701	0.03941	-0.03239	0.08089

Table 3.7: Similarity of QRS Complex Coefficients for an Individual Across all the ECG Features

Coef.	Upper Boundary	Instance 1	Instance 2	Instance 3	Lower Boundary
C1	-6.829e-009	-6.506e-009	-6.005e-009	-5.661e-009	-5.376e-009
C2	6.929e-007	8.326e-007	7.582e-007	7.343e-007	8.733e-007
C3	-4.502e-005	-4.284e-005	-3.839e-005	-3.828e-005	-3.577e-005
C4	0.0009393	0.001128	0.0009902	0.00102	0.001192
C5	-0.01711	-0.01603	-0.01365	-0.01464	-0.01316
C6	0.09465	0.1197	0.09703	0.1102	0.1302
C7	-0.4949	-0.4391	-0.3304	-0.4067	-0.3201
C8	0.5052	0.7659	0.5594	0.7278	0.9137
C9	-0.5597	-0.4117	-0.3208	-0.4026	-0.2343

uniqueness by P is, presence of noise. Since P wave possess the lowest amplitude of all the ECG features, it gets easily corrupted with noises (such as, muscle artifacts, motion artifacts and instrumentation artifacts arising from loose conductivity). With proper measurements, the effects of noises and artifacts can be removed, providing better uniqueness for P wave.

When QRS complex is not prioritized for distance measurement, misclassification occurred while computing the minimum values of distances (Eq. 3.18, 3.19 and 3.20). For this specific case of misclassification, which is shown in Figure 3.12, PDM distances of P and T waves for subject 25 were minimum while performing identification for subject 16. However, subjects 16s own PDM distance for QRS wave was minimum, while performing that identification. As a result, when the minimum values of distances are averaged across all ECG features ( $\Delta_P$ ,  $\Delta_T$  and  $\Delta_{QRS}$ ) a misclassification took place. As discussed earlier, QRS distance measurements for all the subjects shows maximum dissimilarity. Hence, obtaining Algorithm 1 protects misclassification for subject 16 as shown in Figure 3.12.

Since a person might have abnormal beats, such as ectopic beat, which can occur for any healthy beings at random points, only normal beats should be taken for enrolment data,

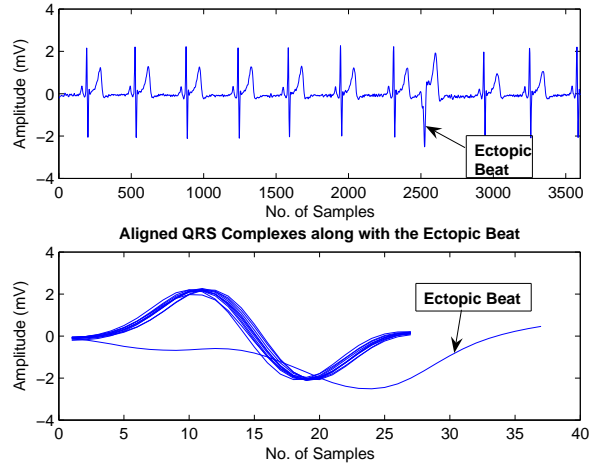


Figure 3.11: Occurrence of Ectopic Beat in Healthy Subject

as random occurrence of ectopic beats is not an ECG feature for a healthy subject. As an example, Figure 3.11 shows an occurrence of ectopic beat for subject 22. This ectopic beat occurred during the acquisition of the enrolment data. However, for all the other cases of ECG acquisition from the same subject there were no more occurrence of ectopic beat. The higher PDM distance between the enrolment coefficients from the ectopic beat and the recognition coefficients resulted in misclassification. Therefore, to overcome misclassifications arising from ectopic beats, algorithm 2 was adopted.

Our experimentation results uphold the polynomial distance measurement as a highly accurate ECG based person identification when both algorithm 1 and algorithm 2 are employed for the proposed PDM measurement. Figure 3.13 show a successful candidate for identification. This figure shows, subject 12 is identifiable because of lower distance,  $\Delta_f$  for P wave, T wave and QRS complex.

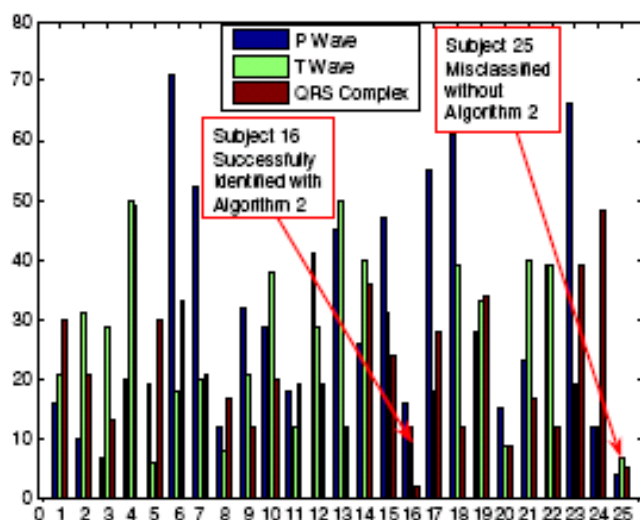


Figure 3.12: Misclassification Resulting from not Prioritizing the Distance Measurement

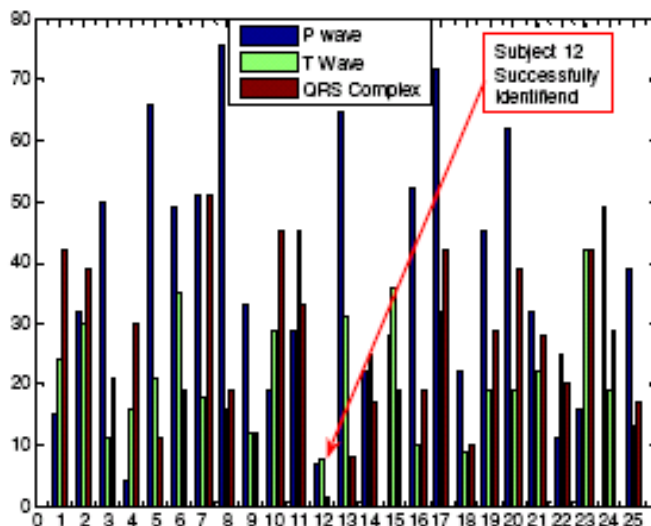


Figure 3.13: Successful Identification of Subject 12, using PDM + Algorithm 1 + Algorithm 2

---

Algorithm 1: Distance Measurement based on Wave Priority

---

```

select  $D_k$  based on  $\min(\Delta_{QRS})$ 
if  $k > 1$  then
    select  $D_k$  based on  $\min(\Delta_T)$ 
    if  $k > 1$ 
        select  $D_k$  based on  $\min(\Delta_P)$ 
    end if
end if

```

---

---

Algorithm 2: Abnormal Beat Cancellation

---

```

i = 0
Acquire beat i
i ++
Acquire beat i
i ++
compute  $\Delta_f$  for beat i - 1 and beat i
while ( $\Delta_f >$  threshold)
    Acquire beat i
    i ++
    compute  $\Delta_f$  for beat i - 1 and beat i
end while
calculate heart vector h from average (beat i - 1, beat i)

```

---

### 3.6.3 An Implementation Scenario

In previous research [Yu et al., 2008], multiple factor pertaining to authentication mechanism was outlined. They are knowledge factor, possession factor and biometric factor. Knowledge factor, which is conventional password / PIN number based security scheme, is often under threat when password is lost or when password is hacked with heuristic brute force attack. Possession factor, where token or smart card or RFID is utilized, can also be stolen and captured by an impostor, who then can gain access to a secured facility. However, biometric based security provides direct binding between the user and his trait. Unlike knowledge and possession based security scheme, biometric can be continuously monitored without active user intervention. Therefore, it can be ideally suited for mobile phone based cardiovascular condition monitoring. In that particular scenario, cardiovascular data is acquired by miniature heart monitor (e.g. Alive Heart Monitor). Then the captured ECG data is transmitted to the mobile phone via Bluetooth. Mobile phone then transmits the data securely to an authentication server, where polynomial coefficients are calculated and with PDM user is



identified. After identification, the user is allowed to access the secured medical facility. In fact, incorporation of knowledge factor, possession factor and biometric factor can be ideal for a highly secured mobile phone based telemonitoring solution (as seen in Figure 3.14). Java 2 Micro Edition (J2ME) is used program this secured solution [Sufi, 2007; Yuan, c2004]. Possession based security was implemented with near field communication (NFC) toolkit offered by Nexperis [NFC, Accessed 2008; Nex, Accessed 2008] and JSR-257 (Contactless Communication API) [JCP, Accessed 2008]. Alive Heart Monitor [Ali, Accessed 2009] was communicated with the mobile phone via Bluetooth with JSR-82 (Bluetooth API) [JCP, Accessed 2008]. The ECG segments were transmitted to the authentication server with Java Wireless Messaging API 2.0, JSR 205 [JCP, Accessed 2008]. The authentication message was also transmitted to the user with HTTP.

Hence, Figure 3.14 reflects the fact that cardiovascular patients are initially authenticated with their username and password. Then they are asked to provide a form of possession factor based authentication (e.g. Smart Card, NFC Card, RFID etc.). Once the patients are identified with their possession factor, their ECG is collected to perform the proposed PDM for ECG based biometric authentication. Thus, Figure 3.14 is an ideal implementation scenario for highly secured cardiovascular patient authentication system that employs knowledge factor, possession factor and biometric factor.

The crucial benefit of using ECG based biometric authentication for this particular scenario is no further requirement for a separate biometric device. The user can be re-authenticated intermittently, while cardiovascular monitoring is in progress. Application of multimodal biometric security scheme using mobile phones camera (JSR 135: Mobile Media

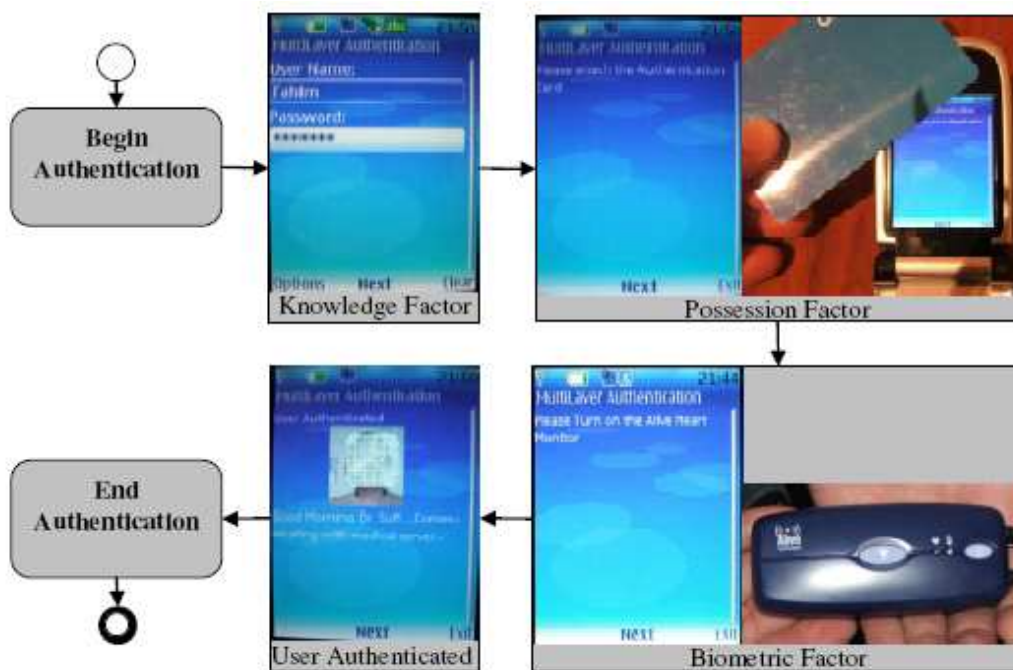


Figure 3.14: PDM method for ECG based biometric authentication on a mobile phone based cardiovascular condition monitoring scenario (the picture within the User Authenticated screen has been intentionally obfuscated for privacy reasons)

API [JCP, Accessed 2008]) with Alive Heart Monitor can also be performed, which is one of our topic for future research.

### 3.7 Direct Approach on Compressed ECG

Adoption of compression technology is often required for wireless cardiovascular monitoring, due to the enormous size of ECG signal and limited bandwidth of Internet. However, compressed ECG must be decompressed before performing human identification using present research on ECG based biometric techniques. This additional step of decompression creates a significant processing delay for identification task. This becomes an obvious burden on a system, if this needs to be done for a trillion of compressed ECG per hour by the hospital.

Even though the hospital might be able to come up with an expensive infrastructure to tame the exuberant processing, for small intermediate nodes in a multihop network identification preceded by decompression is confronting. In this section, we report a technique by which person can be identified directly from their compressed ECG. This technique completely obviates the step of decompression and therefore upholds biometric identification as less intimidating towards the small nodes in a multihop network. The biometric template created by this new technique is lower in size compared to the existing ECG based biometrics as well as other forms of biometrics like face, finger, retina etc (up to 8302 times lower than face template and 9 times lower than existing ECG based biometric template). Lower size of the template substantially reduces the one to many matching time for biometric recognition, resulting in a faster biometric authentication mechanism.

Therefore, in a mobile phone based cardiovascular patient monitoring scenario [Sufi and Khalil, 2008b; Lee et al., 2007; Car, Accessed 2009; Hung and Zhang, 2003], where ECG is transmitted in compressed format, it is possible for the intermediate nodes to identify the patient even without decompressing the ECG signal. Every node within the multihop network have their own listing of routing information. After identifying the patient from their compressed ECG, the route listing is pulled up internally by these nodes. Based on the routing information the compressed ECG reaches the correct destination. Apart from patient identification by the intermediate routing nodes, the hospital (which is the final destination for these compressed ECG) similarly identifies the patient from their compressed ECG and provides appropriate cardiovascular monitoring facility to the subscribed patient.

### 3.7.1 System Design for Direct Approach on Compressed ECG

The compression algorithm described in Chapter 2 represents an ECG signal losslessly. Therefore, the encoding function,  $\epsilon(\cdot)$  transforms the ECG signal,  $X_n$  to a compressed ECG,  $C_r$  (Eq. 3.22). As the ECG features set,  $F$  is a subset of ECG signal  $X_n$  (Eq. 3.23), therefore, feature waves are subset of encoded ECG  $C_r$  (Eq. 3.24). Innovative algorithm can be designed to reveal these encoded ECG feature set (that represents original ECG feature set) and then perform matching between the enrolment and recognition data. This is the core theory behind using encoded ECG to identify a person.

$$\epsilon(X_n) = C_r \quad (3.22)$$

$$F \subset X_n \quad (3.23)$$

$$F \subset C_r \quad (3.24)$$

Examples will clarify the theory behind person identification with compressed ECG. Figure 3.15 to 3.21 show ECG signals from three different individuals. All these ECG signals were collected from MIT BIH Normal Sinus Rhythm Database (known as nsrdb) [Phy, Accessed 2009]. The sampling frequency of the ECG samples used for our experiment (from NSRDB) was 128 Hz with 10 bit resolution. Figures 3.15 to 3.21 basically illustrate the

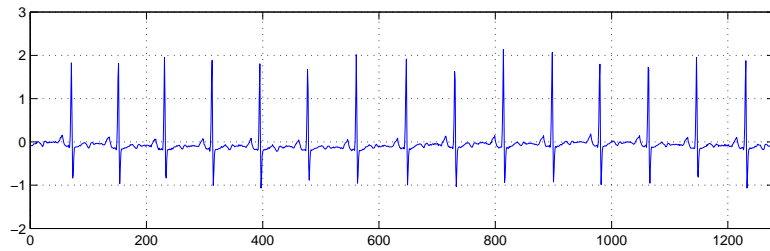


Figure 3.15: An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry no. 16420. X Axis Shows the Number of Samples and Y Axis Shows the Corresponding ECG Amplitude in mV (millivolt) Range

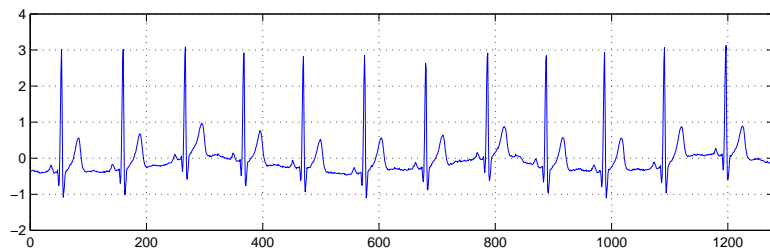


Figure 3.16: An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry no. 16773. X Axis Shows the Number of Samples and Y Axis Shows the Corresponding ECG Amplitude in mV (millivolt) Range

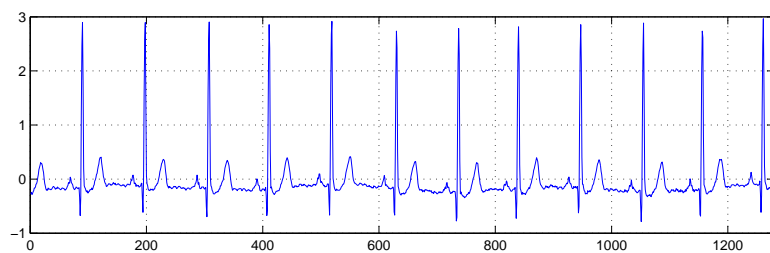


Figure 3.17: An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry no. 16786. X Axis Shows the Number of Samples and Y Axis Shows the Corresponding ECG Amplitude in mV (millivolt) Range

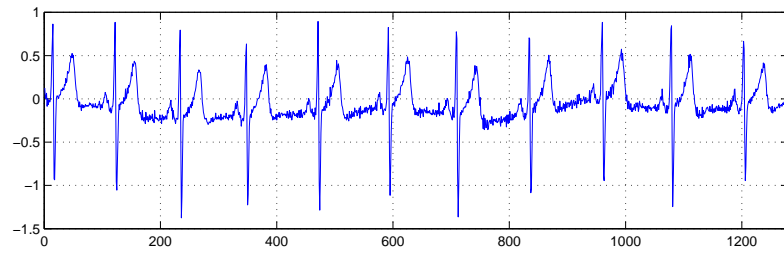


Figure 3.18: An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry no. 16795. X Axis Shows the Number of Samples and Y Axis Shows the Corresponding ECG Amplitude in mV (millivolt) Range

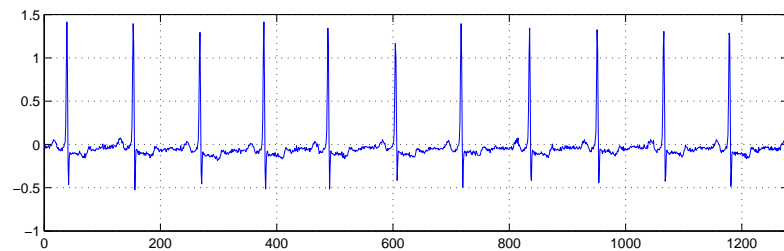


Figure 3.19: An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry no. 17052. X Axis Shows the Number of Samples and Y Axis Shows the Corresponding ECG Amplitude in mV (millivolt) Range

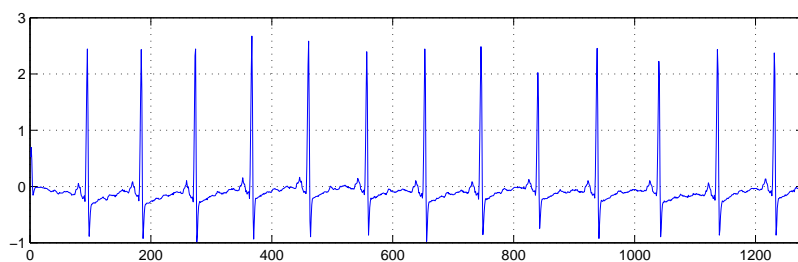
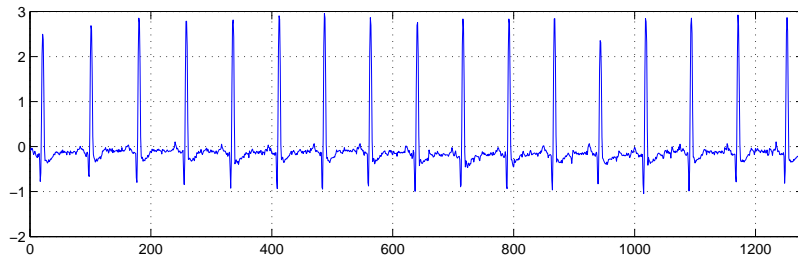
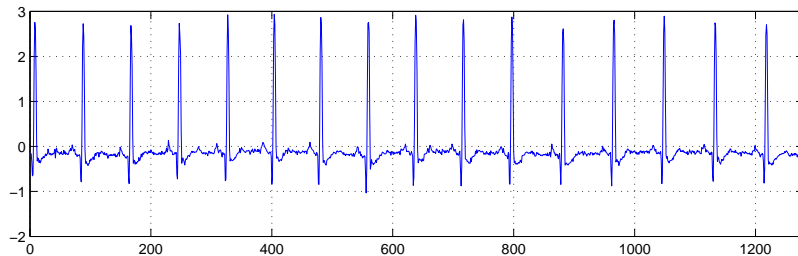


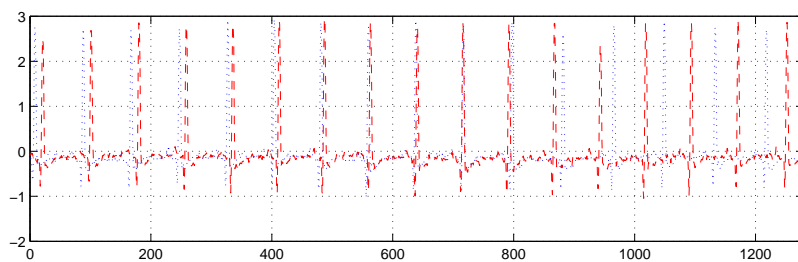
Figure 3.20: An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry no. 17453. X Axis Shows the Number of Samples and Y Axis Shows the Corresponding ECG Amplitude in mV (millivolt) Range



*Figure 3.21: An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry no. 16265 (used as Enrolment Data). X Axis Shows the Number of Samples and Y Axis Shows the Corresponding ECG Amplitude in mV (millivolt) Range*



*Figure 3.22: An ECG Segment of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry no. 16265 (used as Recognition Data). X Axis Shows the Number of Samples and Y Axis Shows the Corresponding ECG Amplitude in mV (millivolt) Range*



*Figure 3.23: Two Overlapped ECG Segments of MIT BIH Normal Sinus Rhythm Database (nsrdb) Entry No. 16265. X Axis Shows the Number of Samples and Y Axis Shows the Corresponding ECG Amplitude in mV (millivolt) Range*



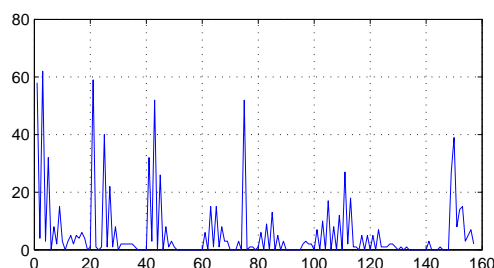
Figure 3.24: Compressed ECG Segment of nsrdb Entry 16420 (of Figure 3.15)



Figure 3.25: Compressed ECG Segment of nsrdb Entry 16773 (of Figure 3.16)

fact that there are minute difference in the ECG signals collected from different individuals. These differences are mostly obvious within the features waves (P wave, QRS complex and T wave). Previous research identified the feature waves using different feature detection algorithms and performed biometric identification based on the ECG features. However, for fast and efficient transmission of ECG signals in telecardiology services, researchers are increasingly using compressed ECG. As shown in Eq. 3.22 - 3.24, compressed ECGs reveals ECG features. Extracting features from compressed ECG is generally faster than feature extraction from plain text (uncompressed) ECG, as minimal characters are read from compressed ECG. Therefore, faster cardiovascular diagnosis has recently been established based on compressed ECG [Sufi et al., 2009a]. Within this section, we also utilize compressed ECG, however to fulfil a different objective of patient identification. Similar to faster cardiovas-





*Figure 3.26: Character Frequency of Compressed ECG Segment in Figure 3.15. X Axis Shows the Number of Encoding Characters (157 Characters in Total), Y Axis Shows the Corresponding Frequency (or the Number of Occurrence for that Character within a Compressed ECG Packet).*

cular diagnosis from compressed ECG, patient identification from compressed ECG is faster because of minimal data length (in compressed ECG) and processing. Figures 3.24 and 3.25 show the compressed ECG of ECG segments of Figure 3.15 and Figure 3.16 respectively.

In a telecardiology scenario, while the ECG segments are being routed through different nodes, each node will quickly calculate the character frequency of the compressed ECG. This tally of character frequency is an inexpensive process and therefore can be easily performed by the limited resources of the nodes. Our experiments reveal the fact that for each individual the distribution of encoding character set (from the compressed ECG) is different. This fact can be observed from Figure 3.26 to Figure 3.28, where X axis and Y axis correspond to individual characters and their frequency counts respectively.

However, for a particular person, the distribution of character frequency is identified (as seen in Figure 3.28), even if their original ECG may look different at different point in time (as seen in Figure 3.23).

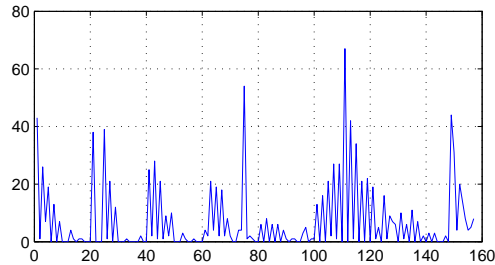


Figure 3.27: Character Frequency of Compressed ECG Segment in Figure 3.16. X Axis Shows the Number of Encoding Characters (157 Characters in Total), Y Axis Shows the Corresponding Frequency (or the Number of Occurrence for that Character within a Compressed ECG Packet).

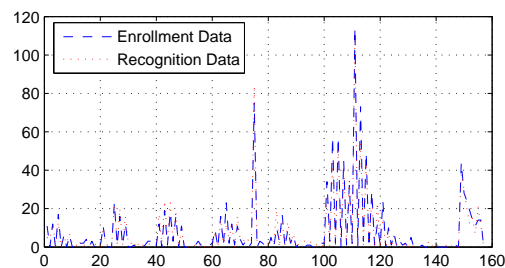


Figure 3.28: Overlap of Character Frequency of Compressed ECG Segments in Figure 3.21 and 3.22. X Axis Shows the Number of Encoding Characters (157 Characters in Total), Y Axis Shows the Corresponding Frequency (or the Number of Occurrence for that Character within a Compressed ECG Packet).

### 3.7.2 An Algorithm for Biometric Feature Creation

Based on the fact that character frequency distribution from the compressed ECG taken at two different times (enrolment and recognition data for biometric) for a single person is similar, we can write an algorithm for person identification with compressed ECG. However, before performing the matching, we need to generate a shortened feature character set that represents a person. Selection of feature set is crucial for biometric identification, as optimal selection of feature set results in faster and accurate processing of identification task. Algorithm 3 establishes a process that generates individual features from their compressed ECG. The algorithm first calculates the character frequency followed by sorting of the character frequency. After the sorting, the first  $l$  number of frequent characters can be collected. This ordered (sequential) character set (referred to as  $\Lambda$  in algorithm 3) is a biometric feature that uniquely identifies a person. The two dimensional feature set,  $\Lambda = \begin{pmatrix} C \\ A \end{pmatrix}$  contains both the selected character,  $C$  and their respective frequencies,  $A$ . The character set,  $C = C_1, C_2, C_3, \dots, C_N$  ranges from 1 to  $N$  (Length).  $\Lambda$  for different entries are clearly different according to our experiments on random MIT BIH ECG entries (as it is seen for entry 16420, 16773, 16786, 16795, 17052, 17453 and 16265). On the other hand, features created for the same entry (same person) at different point in time are similar. As we can observe this similarity for entry 16265,  $\Lambda_{16265E}$  is used as enrolment data and  $\Lambda_{16265R}$  is used as recognition data. This difference in biometric feature set across different individuals and the similarity of feature set for the same individual establish the basis for person identification based on compressed ECG. Figure 3.29 shows the distance value,  $\psi$  is minimum when

enrolment and recognition ECG templates of 16265 are calculated using Eq. 3.25. Similarly, figure 3.30 shows correct matching (with minimum  $\psi$  value) of entry 16795.

$$\psi = \frac{\sum_{n=1}^l (A_n^E - A_n^R)^2}{l} \quad (3.25)$$

$A_l^E$  and  $A_l^R$  are the frequency counts of Enrolment and Recognition (respectively) for  $l_{th}$  template parameter. Table 3.8 shows the 12 different template parameter for enrolment data of 16265. According to our experimentation, all the template attributes varies greatly (Table 3.8), except for the case when same person's enrolment and recognition data are used (as shown in Figure 3.29). It should be mentioned that one person's ECG template parameter may not be present in another person's selected parameter. In those cases, the values of the missing parameters are thought to be zero (during the calculation of Eq. 3.25). Experimentation was performed using the 18 entries of MIT BIH of NSRDB [Phy, Accessed 2009] with no cases of misclassification. NSRDB was chosen for our experimentation, since this database contains normal ECG signals. Most of the other MIT BIH database contains abnormal ECG (generally, used for validating cardiovascular abnormality detection algorithms [Hamilton and Tompkins, 1986; Friesen et al., 1990]). Abnormal ECG signals (from other MIT BIH database) has almost never been used in other existing ECG based biometric systems [Sufi et al., 2010a; Khalil and Sufi, 2008a; Sufi and Khalil, 2008a; Sufi et al., 2008e; 2009b; Biel et al., 2001; Chan et al., 2008; Wubbelier et al., 2007; Poon et al., 2006; Israel et al., 2005; Irvine et al., 2001; Bui and Hatzinakos, 2008; Kyoso and Uchiyama, 2001; Kyoso, 2003; Shen

$$\begin{aligned}
 \Lambda_{16420} &= \left( \begin{array}{cccccccccccc} \$ & ] & @ & ; & \hat{U} & \ae & 50to100 & \grave{e} & / & p & 0to50 & ? \\ 62 & 59 & 58 & 52 & 52 & 40 & 39 & 32 & 32 & 27 & 27 & 26 \end{array} \right) \\
 \Lambda_{16773} &= \left( \begin{array}{cccccccccccc} p & \hat{U} & 0to50 & @ & r & \ae & ] & t & 50to100 & ; & l & n \\ 67 & 54 & 44 & 43 & 42 & 39 & 38 & 34 & 31 & 28 & 27 & 27 \end{array} \right) \\
 \Lambda_{16786} &= \left( \begin{array}{cccccccccccc} \hat{U} & p & \$ & \ae & r & @ & ] & t & \grave{u} & 50to100 & \grave{e} & \acute{E} \\ 81 & 72 & 67 & 50 & 42 & 35 & 34 & 31 & 30 & 30 & 28 & 26 \end{array} \right) \\
 \Lambda_{16795} &= \left( \begin{array}{cccccccccccc} p & r & \hat{U} & t & j & l & v & h & n & x & 50to100 & f \\ 124 & 85 & 80 & 74 & 66 & 60 & 57 & 57 & 52 & 48 & 46 & 36 \end{array} \right) \\
 \Lambda_{17052} &= \left( \begin{array}{cccccccccccc} \hat{U} & ] & ; & \$ & \ae & \grave{e} & \acute{I} & p & \grave{I} & ? & / & \acute{E} \\ 82 & 63 & 48 & 46 & 41 & 37 & 33 & 32 & 32 & 32 & 28 & 26 \end{array} \right) \\
 \Lambda_{17453} &= \left( \begin{array}{cccccccccccc} \$ & ] & ; & @ & \ae & 150to200 & / & 0to50 & \hat{U} & \grave{e} & 50to100 & p \\ 74 & 56 & 56 & 55 & 43 & 28 & 27 & 25 & 23 & 23 & 23 & 22 \end{array} \right) \\
 \Lambda_{16265E} &= \left( \begin{array}{cccccccccccc} p & \hat{U} & r & j & h & t & l & 0to50 & f & n & v & 50 - 100 \\ 114 & 75 & 73 & 57 & 57 & 49 & 45 & 44 & 34 & 32 & 29 & 28 \end{array} \right) \\
 \Lambda_{16265R} &= \left( \begin{array}{cccccccccccc} p & \hat{U} & r & j & t & h & l & 0to50 & n & 50to100 & f & v \\ 110 & 84 & 54 & 51 & 44 & 44 & 42 & 38 & 36 & 30 & 26 & 25 \end{array} \right)
 \end{aligned}$$

et al., 2002; Shen, 2005; Shen and Tompkins, 2005; Wang et al., 2008; Plataniotis et al., 2006; Kanade and Jain, 2005]. To obtain a more accurate evaluation of the algorithm presented within this section, experimentation needs to be carried out on a substantially larger sample (different ECG segments from different persons) size. This could be done in future, when MIT-BIH accommodates more normal ECG samples (at present, there are only 18 entries available in NSRDB [Phy, Accessed 2009]).

### 3.7.3 An Algorithm for Biometric Feature Matching

The compressed ECG feature  $\Lambda$  has three major characteristics: character set, order of character set and the frequency of the individual characters.

- **Character Set:** Character set for each feature set representing a particular individual shows a degree of uniqueness. As an example, in the case of entry 17052, character  $\acute{I}$  and  $\grave{I}$  is not present in entries 16420, 16773, 16786, 16795, 17052, 17453, 16265 (both

Table 3.8: Standard Deviations of the ECG Biometric Template Values (Templates for  $\Lambda_{16265E}$ )

Attribute	Value Range
p	$64.86 \pm 40.70$
$\hat{U}$	$65.14 \pm 23.04$
r	$31.86 \pm 33.08$
j	$16.71 \pm 28.87$
h	$14.43 \pm 24.93$
t	$26.14 \pm 28.12$
l	$18.43 \pm 24.89$
0to50	$19.14 \pm 19.01$
f	$8.86 \pm 15.4$
n	$12.57 \pm 21.96$
v	$11.71 \pm 22.04$
50-100	$28.43 \pm 14.55$

---

Algorithm 3: Feature Extraction from Compressed ECG

---

//Notation Description:

// $F$  holds the feature set comprising of compressed character.

Count the frequency of the encoding characters from compressed ECG

$$\Gamma = \begin{pmatrix} C_1 & C_2 & C_3 & \dots & C_N \\ A_1 & A_2 & A_3 & \dots & A_N \end{pmatrix}$$

Sort  $\Gamma$  based on the frequency Count  $A$  in a descending order

$$\Upsilon = \begin{pmatrix} C_p & C_q & C_r & \dots & C_s \\ A_p & A_q & A_r & \dots & A_s \end{pmatrix}$$

Where,  $A_p \geq A_q \geq A_r \geq A_s$

Create feature template  $\Lambda$  by taking first  $l$  number of entries from  $\Upsilon$

$$\Lambda = \begin{pmatrix} C_p & C_q & C_r & \dots & C_l \\ A_p & A_q & A_r & \dots & A_l \end{pmatrix}$$


---

in enrolment and recognition). Therefore, existence of some characters reduces the domain of similar ECGs (for biometric matching purpose). In most of the cases, the enrolment data is found within this limited set of similar ECGs.

- **Order of Characters:** Once a limited subset of ECG templates is established, representing the possible candidates for successful biometric match, ordering of the character set is considered. It is obvious from the enrolment and recognition data of entry 16265 that for the first 7 characters the sequence (or ordering) of the characters are nearly the same, with an exception of characters  $t$  and  $h$ . For this example, these two characters ( $t$  and  $j$ ), just swapped their corresponding positions. Higher matching of character sequence also reduces the number of candidates for biometric matching. When this candidate subset reduces to one, this means the completion of human identification task.
- **Character frequency:** If the previous steps of character set and order of characters still leaves few candidates, then the frequency of each characters are matched. For the ECG pairs, having closer match according to the character frequency is given preference to be selected as biometric recognition / identification.

#### 3.7.4 Discussion

Here, we reported an algorithm for selecting biometric feature template from compressed ECG and a methodology for performing matching. The ECG biometric technique presented here is particularly useful for mobile phone based cardiovascular monitoring in the following respects (as seen from Figure 3.31).

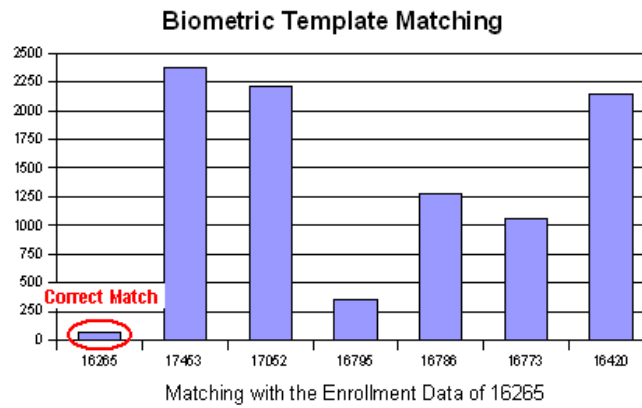


Figure 3.29: Matching Enrolment Data of 16265, 17453, 17052, 16795, 16786, 16773, 16420 with Recognition Data of 16265. X Axis Represents Different Individual and Y Axis Represents  $\psi$  Value of Equation 3.25. Matching Occurs with the Minimum Value of  $\psi$ .

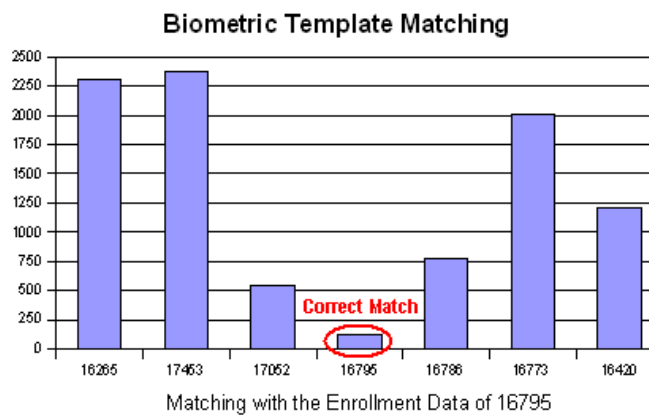
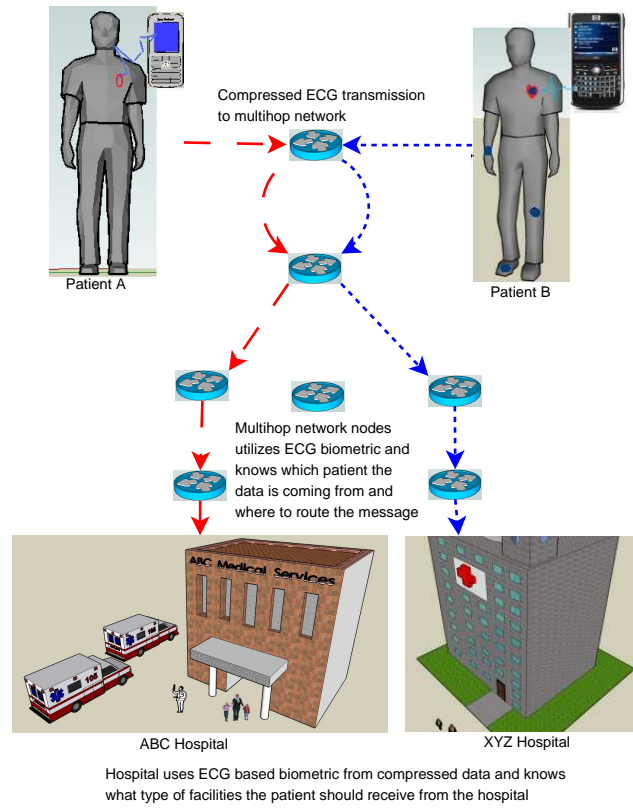


Figure 3.30: Matching Enrolment Data of 16265, 17453, 17052, 16795, 16786, 16773, 16420 with Recognition Data of 16795. X Axis Represents Different Individual and Y Axis Represents  $\psi$  Value of Equation 3.25. Matching Occurs with the Minimum Value of  $\psi$ .



- **Intermediate Nodes:** The template (feature) matching algorithm is simple enough to be implemented within the limited computational resources of an intermediate node that is responsible for relaying the compressed ECG within a multihop network. By successfully identifying the person from compressed ECG, the intermediate node knows the destination of that compressed ECG packet, provided that the intermediate node possess the knowledge of subscriber listing for different cardiovascular monitoring services (or hospitals).
- **Hospital or Cardiovascular Monitoring Service Provider:** The monitoring facility can also identify the person from the compressed ECG sent to them. The primary goal of identification is to check whether that person is actually subscribed for the facility. If the person is found to be a valid subscriber, then the list of subscribed services for that person is retrieved. This biometric authentication and authorization is made possible by ECG biometric from compressed ECG.

Our direct approach on compressed ECG based biometric technique is the first of its kind for ECG based biometric authentication. This technique has several advantages over existing ECG based biometric authentication. This technique is fast and efficient (this will be discussed further in Performance Comparison section of this chapter). Being convinced with this initial assessment of an ECG biometric technique from compressed ECG, further research was conducted for developing a more robust biometric method with data mining techniques.



*Figure 3.31: ECG based Biometric (from Compressed ECG) being used by the Multihop Network Node as well as The Hospital*

### 3.8 Data Mining Methods on Compressed ECG

This section proposes a novel method of ECG biometric directly from compressed ECG harnessing data mining (DM) techniques like attribute selection and clustering. The template size (and also the matching time) is up to 8533 times lower than face template, 61 times lower than existing PRD ECG based biometric template and 9 times smaller than Polynomial Distance Measurement (PDM) based ECG biometric. This improved method of compressed ECG biometric has even lower template size compared with our previous direct method on compressed ECG biometric. Lower size of the template substantially reduces the one to many matching time for biometric recognition, resulting in a faster biometric authentication mechanism and ECG stream verification directly from compressed ECG.

In wireless body sensor networks (BSN), ECG and other physiological data forwarded by one node to the other also need to be verified and authenticated to thwart against intruder attacks. Incorporation of biometric based ECG packets validation and patient authentication in these scenarios basically enable secured remote monitoring for the patients.

Here we reported a technique of patient authentication from compressed ECG using data mining techniques. This ECG biometric directly reads the compressed ECG to obtain unique features that can identify an individual using Expectation Maximization (EM) based clustering. As the lengths of the compressed ECG segments are substantially smaller than plain text ECG, minimal reading operations are performed for biometric authentication compared to the existing ECG based biometrics (as they need to read larger plain ECG packets). Also, the biometric templates created from the compressed ECG are substantially reduced in size (61 times smaller than PRD based ECG biometric [Chan et al., 2008], 38 times smaller than

WDM [Chan et al., 2008], 16 times smaller than ECG biometric of [Wubbeler et al., 2007] and 9 times smaller than PDM based ECG biometric [Sufi et al., 2010a; Sufi and Khalil, 2008a]). Reduced template size only means faster biometric authentication and processing of data validation, which makes way for faster diagnosis and treatment of emergency cardiac patients in wireless telecardiology applications. In addition, the proposed ECG biometric from compressed ECG packets is computationally inexpensive for authentication in telecardiology applications, as the requirement of decompression step is completely obviated.

As seen from Figure 3.32, in an automated CVD detection mechanism, a patient can subscribe to a monitoring facility for instant diagnosis service, onsite cardiologist visit, immediate ambulance call, specialized treatment facility etc. To know what services the patient is subscribed for can only be ascertained after successful identification of the patient, for which ECG biometric provides automated identification, as well as a continuous validation of ECG data stream. It should be noted that conventional patient identification mechanisms using user name and password ([Blount et. al., 2007]) might not be ideal for patients having cardiac anomaly, as abnormal rhythm can have direct impact on patients autonomous nervous system (ANS) [Kumar et al., 2007]. Therefore, during a time of cardiac arrest ANS might prevent the CVD patients to correctly type their username and password as it was done by previous researchers [Blount et. al., 2007]. Moreover, ECG based biometric authentication is more secured than user name and password based authentication, since it depicts liveness.

Apart from automating the patient authentication and minimizing delays in treatment, the compressed ECG based biometric can be useful in the following three areas:

- *Authentication between the ECG Acquisition Device and the Patient's Mobile Phone:*

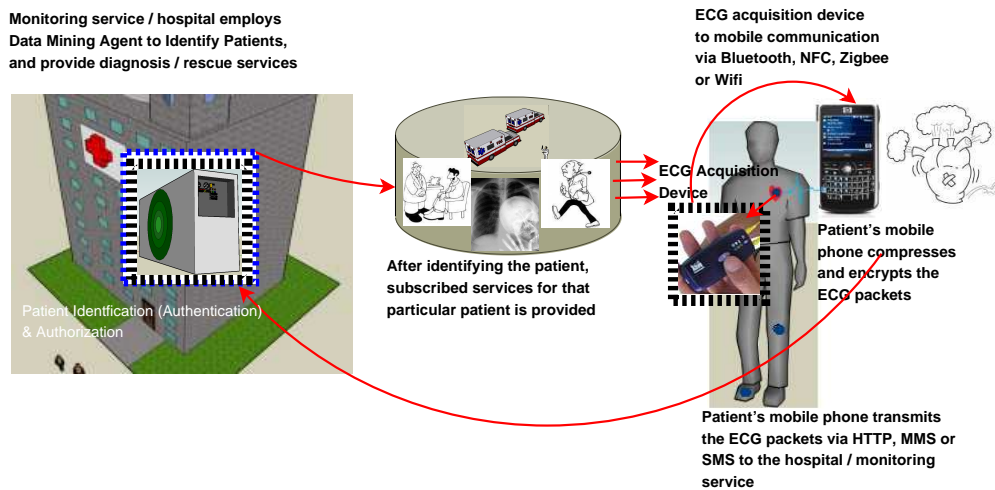


Figure 3.32: Architecture of the Data Mining based Patient Identification from Compressed ECG

The communication between the ECG acquisition device and patient's mobile phone can be made secured with compressed ECG based biometric presented within this section. The patient's mobile phone should only allow patient's ECG packets to be transmitted to the hospital.

- *Authentication within the Routing Nodes:*

After the ECG packets are released from the patient's mobile phone, they are channelled from one or more routing node towards the appropriate hospital. Implementing compressed ECG based biometric, these nodes can identify the valid ECG packets coming from authenticated sources (patients). Therefore, DDoS attack can be prevented by the routing nodes, by discarding all the ECG packets stemming from unauthenticated sources.

- *Authentication of Patient in the Hospital:*

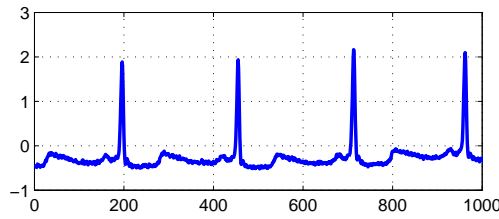


Figure 3.33: A Normal ECG Segment of a Monitored Patient at Instance A (ECG Obtained from CU1 Entry MIT BiH CU Ventricular Tachyarrhythmia Database) [Phy, Accessed 2009]

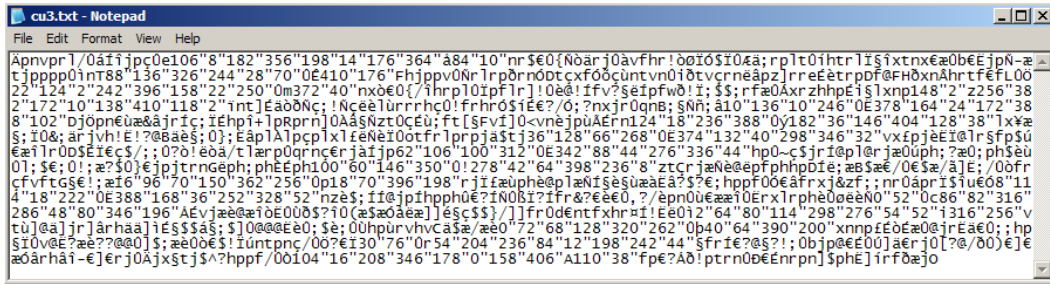


Figure 3.34: Compressed ECG for Figure 3.33 (using Algorithms Presented Earlier in Chapter 2)

The hospital or the cardiovascular monitoring services (e.g. [www.cardionet.com](http://www.cardionet.com)) may want to authenticate their subscribed patients before sending in emergency personnel or releasing other services that the patient is subscribed for. In that case, the hospital can instantly identify their subscribed patients straight from their compressed ECG packets, using the techniques described within this section.

Without utilizing compressed ECG based biometric (or authentication), each compressed ECG packets requires additional step of decompression (creating massive delays) for all the areas, where authentication can play a role (acquisition device to mobile phone communication, intermediate routing nodes and hospital side patient authentication).

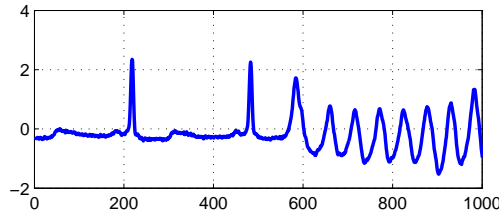


Figure 3.35: An Abnormal ECG Segment of the Monitored Patient at Instance  $A+1$  (ECG Obtained from CU1 Entry of MIT BiH CU Ventricular Tachyarrhythmia Database) [Phy, Accessed 2009]

### 3.8.1 Architecture of the Proposed Patient Identification System

Figure 3.33 shows the normal ECG signal for an event based monitored patient (Entry ID CU1 of CU Ventricular Tachyarrhythmia database [Phy, Accessed 2009]) at instance  $A$ . At the next instance all on a sudden, that patient encounters abnormal heart beats as seen in Figure 3.35. Patient's mobile phone detects the abnormality using existing abnormality detection algorithms [Sufi et al., 2009a]. Then the patient's mobile sends both normal and abnormal ECG packets in compressed format. The normal compressed ECG (Figure 3.34) is used in identifying the patient and the abnormal ECG is used for diagnosis of the cardiac abnormality (using algorithms presented in Chapter 5). After identifying the patient directly from the compressed ECG (Figure 3.34), the patient can then be provided for the services he is entitle to (e.g. ambulance facility, onsite specialist etc.).

Eq. 5.12 and 5.13 basically demonstrates the fact that lossless compression algorithm (presented in Chapter 2) preserves the subtle ECG features responsible ECG based biometric. Therefore, these features can be directly obtained from the compressed ECG (Eq. 5.14). Our proposed DM model presented in this chapter examines only a limited feature set (highly correlated with person identification) and assigns a recognition ECG into a known enrolment

cluster.

The 148 characters and the numeric values (0 - 9) are used to compress (or encode) the plain text ECG signal, as seen from Figure 3.37 (ECG compression is performed inside patient's mobile phone). The Data Mining Agent (DMA) of the hospital (Figure 3.32) needs to be trained for patient identification with enrolment ECG (compressed) of all its subscribers. After being trained, the DMA can be tested with recognition ECG (compressed) of a particular patient. Figure 3.36 shows during this testing phase a recognition data is passed to the trained DMA, and DMA then decides the closest distance with the trained clusters (i.e. 1, 2, 3, 4, ... $N$ , where  $N$  is number of patients). This cluster matching (testing phase 2 in Figure 3.36) can be done either with EM or with Algorithm 5, which will be presented later on.

### 3.8.2 Training of the Proposed Model

During the training phase, the proposed model learns the cluster means and standard deviations for all the clusters, where each cluster uniquely identifies a particular patient. Figure 3.38 shows the main stages of this learning process from compressed ECG.

*Character Frequency Calculation:* As shown in Figure 3.38, from the compressed ECG, the frequency of each encoded characters is computed first. There are about 148 characters and 6 numeric subgroups for which the frequencies are generated (Figure 3.37). The frequency of these 157 character (and numeric sub groups) are utilized as the attributes for clustering.

However, 157 attributes are too many for generating clusters (one cluster per subscribed patient). Therefore, the attribute subset selection is necessary. Using proven techniques, we



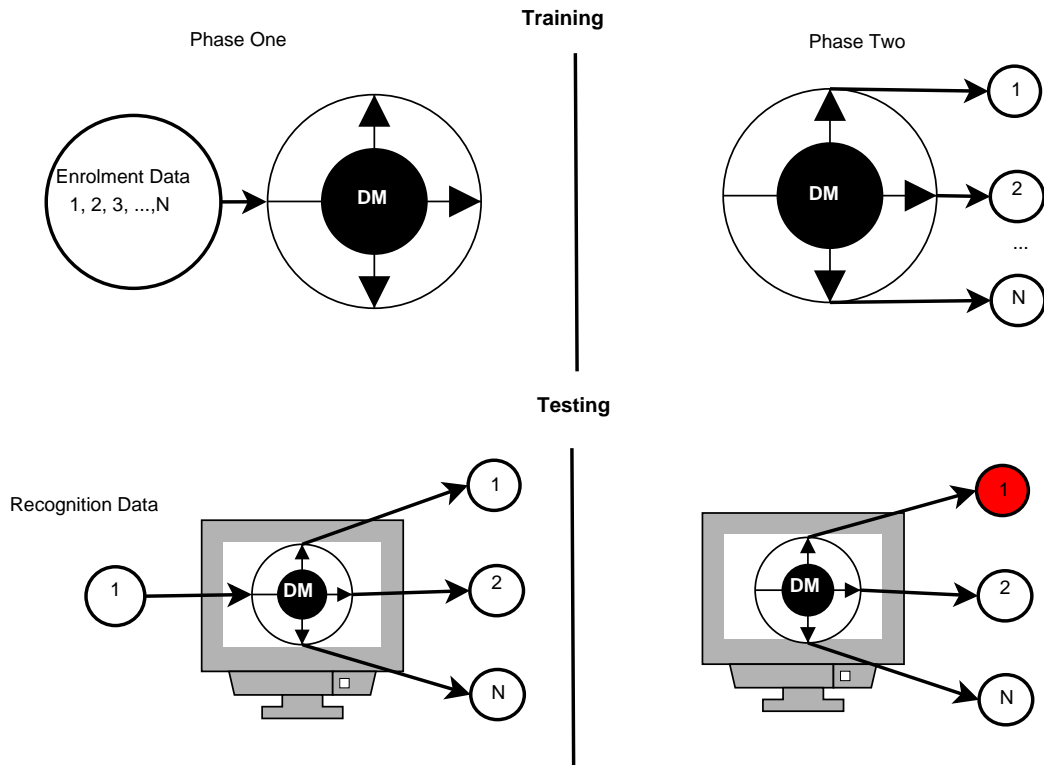


Figure 3.36: Training with Enrolment Data and Testing with Recognition Data

**Characters**

```
@f$¥èúìòçøåä_{}[~]|€æåßÉ
!#%&()*+,-./:;<?;šžäöñüàAAA
AAEEIIIIiðN000000U00Uÿpáãäçè
éíîïðóôõúýabcdefghijklmnopq
rstuvwxyzABCDEFGHIJKLMNOPS
TUVWXYZ\
```

**Numeric Sub Groups**

- 0-50
- 50-100
- 100-150
- 150-200
- 200-250
- 250-300
- 300-350
- 350-400
- 400-500

Figure 3.37: 157 Character and Numeric Sub Groups (Attributes) used for Generating Compressed ECG (from Plain ECG Signal). Details of this Character Substitution based Compression Techniques have been Described in Chapter 2

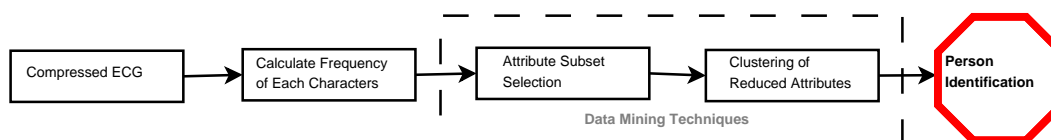


Figure 3.38: Step by Step Procedure of the Proposed Patient Identification System

first select characters from the compressed ECG that are mainly responsible for identifying individuals (i.e. attribute subset selection). Then, based on the selected characters (or attributes) clusters (representing individuals) are generated.

*Attribute Subset Selection:*

Data pre-processing with attribute selection is an important step in data mining [Han and Kamber, 2006]. The goals of feature subset selection are the followings:

- To reduce the dimensionality of the data to be analysed
- For faster execution of Data Mining algorithms
- To improve predictive accuracy of data mining techniques
- To generate a comprehensive of the output

Existing studies have demonstrate the fact that attribute subset selection helps improve the performance of clustering algorithms with reduced attributes [Talavera, 1999a;b]. In this section, we performed attribute selection with Correlation based Feature Selection (CFS) algorithm.

CFS algorithm filters or ranks feature subsets according to a correlation based heuristic evaluation function. There are two important criteria that effect this feature selection process.

1. Features that are highly correlated with the class

## 2. Features that are uncorrelated with each other

The first criterion ensures that irrelevant features will be removed (since they are not correlated with the class). On the other hand, the second criterion mandates that redundant features should be removed (since they are correlated with other features).

CFS feature subset evaluation function is represented by Eq 3.26.

$$M_S = \frac{k\overline{r_{cf}}}{\sqrt{(k + k(k-1)\overline{r_{ff}})}} \quad (3.26)$$

where,  $M_S$  is the heuristic merit of a feature subset  $S$  containing  $k$  features,  $\overline{r_{cf}}$  is the mean feature-class correlation ( $f \in S$ ), and  $\overline{r_{ff}}$  is the average feature-feature intercorrelation. The denominator of Eq. 3.26 represents the redundancy of the features and the numerator indicates how predictive of the class, a set of features are.

In this section, we have used *Best First* search algorithm for searching through the candidate subsets the local optimal solution. *Best First* search can operate in following two different modes:

- Start with no features at all and search progresses forward through the search space adding single features
- Start with all features and search moves backward through the search space removing single feature

A stopping criteria is imposed to prevent *Best First* search from exploring the entire

feature subset search space.

*Clustering of Individual Patients from their Compressed Enrolment ECGs:*

EM is basically iterates between two core steps, called the E-Step and the M-Step. In the E-Step, assignment of the probabilities for each instances being a member of a particular class is performed. On the other hand, M-Step updates or re-estimates the probability values by calculating the log likelihood data [Han and Kamber, 2006].

As shown in Algorithm 4, our implementation of EM revolves around the idea that every single patient is assigned to a cluster for identification purpose. We assume that there are  $l$  number of clusters  $(A_1, A_2, A_3, \dots, A_l)$ , representing  $l$  number of persons to be identified with a defined set of features (derived from the frequency of the compressed characters).

At the beginning of Algorithm 4, we start of with initial value of cluster means, standard deviation for each of the class (or patients). As the algorithm iterates though the loops, the value of standard deviation and cluster means are refined and updated. At the end of this process (at convergence), we will have the same number of cluster means and standard deviation as the number of subscribed patients (i.e. clusters).

EM can decide how many clusters to create by cross validation, or it may be specified apriori (as is the case in the present study).

### **Testing the Identification Model with Compressed Recognition ECG**

After successful training phase, the model possesses the knowledge of cluster means and standard deviations for all the patients. Therefore, EM based model can easily be tested with recognition data.

---

Algorithm 4: EM for Indetifying Patients

---

//Notation Description:

//Input: Start with initial value of parameters mean  $\mu$ , standard deviation  $\sigma$

//Input: and probability  $p$  (for Clusters  $\{A_1, A_2, A_3, \dots, A_l\}$ )

//Output: Final Value of value of parameters mean  $\mu$ , standard deviation  $\sigma$

//Output: and probability  $p$  (for Clusters  $\{A_1, A_2, A_3, \dots, A_l\}$ ) height

Loop (For each iteration  $j$  - Number of instances)

Calculate the probability that instance  $I$  belongs to clusters  $A_1, A_2, \dots, A_l$ :

$$P(A_1|I) = \frac{p_{A_1}^j P^j(I|A_1)}{P^j(I)}, \dots, P(A_l|I) = \frac{p_{A_l}^j P^j(I|A_l)}{P^j(I)}$$

The probability of  $P(I|A_1)$  can be modelled using any distribution function.

For the commonly used Gaussian distribution, it can be given by,

$$P(I|A_1) = \frac{1}{\sqrt{(2\pi)\sigma_{A_1}}} \exp \frac{-(I-\mu_{A_1})^2}{2\sigma^2}$$

Update the mixture parameters on the basis of the new estimates:

$$\begin{aligned} p_{A_1}^{j+1} &= \frac{\sum_I P(A_1|I)}{n}, \dots, p_{A_l}^{j+1} = \frac{\sum_I P(A_l|I)}{n} \\ \mu_{A_1}^{j+1} &= \frac{\sum_I I \times P(A_1|I)}{\sum_I P(A_1|I)}, \dots, \mu_{A_l}^{j+1} = \frac{\sum_I I \times P(A_l|I)}{\sum_I P(A_l|I)} \\ \sigma_{A_1}^{j+1} &= \frac{\sum_I P(A_1|I)(I-\mu_{A_1}^{j+1})^2}{\sum_I P(A_1|I)}, \dots, \sigma_{A_l}^{j+1} = \frac{\sum_I P(A_l|I)(I-\mu_{A_l}^{j+1})^2}{\sum_I P(A_l|I)} \end{aligned}$$

End Loop

---

---

Algorithm 5: Person Identification with Cluster Distance Measurement

---

//Notation Description:

//Input: Attribute values for all the instances

//Input: Cluster means of all the clusters for all the attributes

//Output: Identified patient

---

**Step 1**

Create distance vector,  $A_1, A_2, \dots, A_M$  for  
Cluster 1, 2...M, where M is the total number of clusters  
(or total number of subscribed patient)

$$A_1 = \sqrt{\sum_{i=1}^I (f_i - C_i^1)^2}$$

$$A_2 = \sqrt{\sum_{i=1}^I (f_i - C_i^2)^2}$$

⋮

$$A_M = \sqrt{\sum_{i=1}^I (f_i - C_i^M)^2}$$

here,  $f_i$  is the attribute value vector for all I  
attributes and  $C_i^1, C_i^2, \dots, C_i^M$  are the centroid  
vectors of cluster means 1, 2, ..., M

where  $i = 1, 2, 3, \dots, I$  is the number of attributes

**Step 2**

The identified person,  $m$  has the lowest value of  $A_m$   
(i.e.  $\text{Min}(A_1, A_2, A_3, \dots, A_m, \dots, A_M)$ )

---

When recognition compressed ECG is received by the trained model, the frequencies for the selected attributes (characters),  $f_i$  are calculated first, where  $i$  is the number of attribute and  $C_i^m$  is the centroid vector of cluster  $m$  (which can range between 1 to  $M$ ). Algorithm 5 calculates the distance of recognition ECG with all the classes. The least distant class (with the recognition ECG) signifies the fact that the person belongs to the particular class.

### 3.8.3 Experimentation and Results

To demonstrate the fact that ECG based biometric authentication is possible from compressed ECG, we have selected 120 ECG segments from publicly available database (so that the experimentation can be reproduced by other researchers). These ECG data were processed in five stages (data collection, ECG compression, frequency calculation, attribute selection and finally clustering) and at the end, our experimentation showed that ECG segments collected from the same individual (nsrdb entry) are highly correlated (i.e. they belonged to a single cluster).

#### Data Collection

Even though we had experimented with 30 different entries from different databases in physiobank [Phy, Accessed 2009] to validate our proposed model of biometric authentication, for thorough demonstration purposes, we refer to 9 entries of Normal Sinus Rhythm Database (NSRDB) [Phy, Accessed 2009]. From each entry four randomly selected ECG segments were used for our experimentations. The sampling frequency of the collected ECG signals was 128 Hz. The duration of each of the ECG segments were 5 seconds (i.e.  $5 \times 128$  or 640 samples in one ECG segment). Table 3.9 shows the segments (time duration) used for different entries in our experimentation (middle column). The right column lists the number of beats (QRS complex) contained within each of the ECG segments (four segments per person).

Figure 3.39 shows 4 different ECG segments of entry 16265 (nsrdb of MIT BIH) on the left column and 4 different ECG segments of entry 16272 (nsrdb of MIT BIH) on the right column. Therefore, the left column demonstrates the self similarity of the same person's

*Table 3.9: ECG Segments Collection from NSRDB, Entry No. and Segments Obtained. Four ECG Segments were Obtained for Each of the Entries (i.e. 36 ECG Segments Obtained for our Experimentation)*

Entry No.	Segmentation Position	Number of Beats in each segments
16265	[08:04:00.000]-[08:04:09.992] [08:22:50.000]-[08:22:59.992]	[8,7,7,8]
16273	[08:15:10.000]-[08:15:19.992] [08:16:10.000]-[08:16:19.992]	[6,7,6,6]
16483	[10:02:00.000]-[10:02:09.992] [10:07:00.000]-[10:07:09.992]	[7,7,7,7]
16773	[09:50:20.000]-[09:50:29.992] [09:54:20.000]-[09:54:29.992]	[6,6,6,6]
16786	[11:48:00.000]-[11:48:09.992] [11:53:00.000]-[11:53:09.992]	[6,6,6,6]
16795	[11:21:00.000]-[11:21:09.992] [11:28:00.000]-[11:28:09.992]	[5,4,6,5]
17052	[11:20:00.000]-[11:20:09.992] [11:27:00.000]-[11:27:09.992]	[6,5,5,6]
17453	[09:49:00.000]-[09:49:09.992] [09:54:00.000]-[09:54:09.992]	[6,7,6,7]
18177	[12:05:00.000]-[12:05:00.359] [11:33:00.000]-[11:33:09.992]	[7,9,8,9]



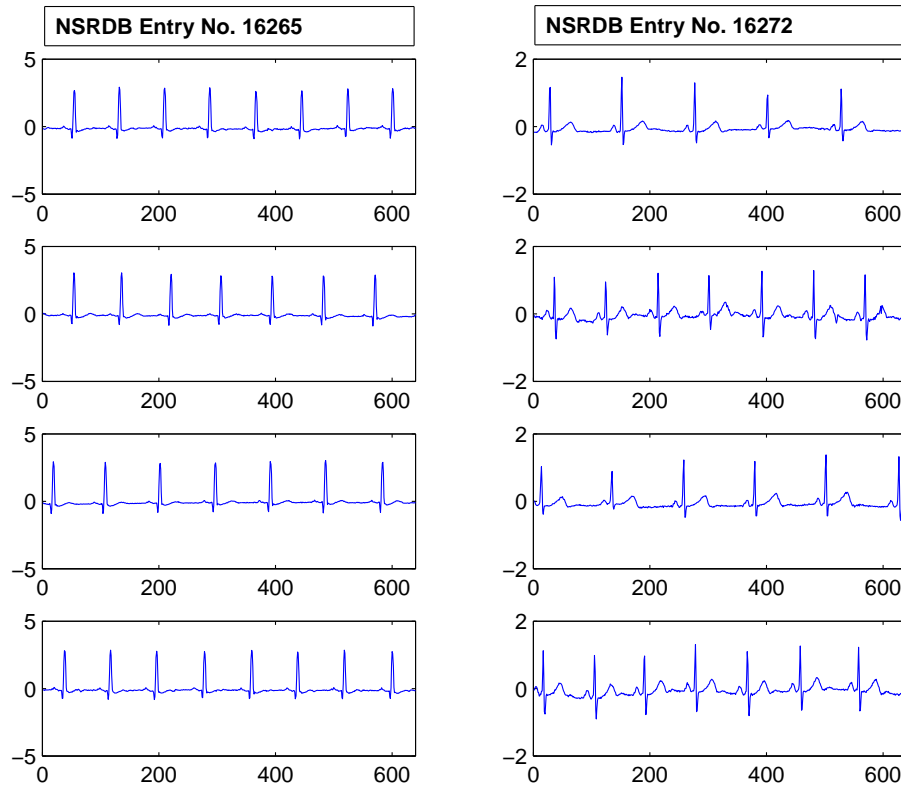


Figure 3.39: Eight Different ECG Segments for nsrdb Entry 16265 (4 Segments - in First Column) and 16272 (4 Segments - in Second Column)[Phy, Accessed 2009]

ECG at different times. This is the basis of ECG biometric. However, there are minute differences even for the same person's ECG taken at a different point of time (as in the case of Entry 16272 - Figure 3.39). Attribute selection process can be utilized to select only the features or attributes that are responsible for identifying person.

### **ECG Compression**

As discussed earlier, compressed ECG provides transmission efficiency for wireless telecardiology application (Figure 3.32) and this section outlines a technique that identifies person (or patient) from their compressed ECG. Therefore, to prove our theory laid earlier, we compressed the 36 ECG segments collected from 9 different individuals. The compression algorithm used is well documented in Chapter 2 and also the ECG segments used are from public ECG database ([Phy, Accessed 2009]).

As seen from Figure 3.40, for human being it is hard to distinguish two individuals just by gazing at their compressed ECG (manual inspection). Also, it takes enormous amount of efforts on an individual to identify self similarity of compressed ECG collected from the same person at different point in time. Therefore, a DMA was employed to automate the process of person clustering from compressed ECG. Successful clustering of individuals basically demonstrates the rationality of person identification.

### **Frequency Calculation**

To employ an automated DMA for clustering of individuals from their compressed ECG, attribute selection needs to be performed. In our experiments, we require compressed character



Figure 3.40: Eight Different ECG Segments for nsrdb Entry 16265 (4 Segments - in First Column) and 16272 (4 Segments - in Second Column) are Compressed using Compression Algorithm Described in Chapter 2

---

Algorithm 6: Frequency Calculation of Compressed ECG Characters from the Compressed ECG Segment

---

**//Notation Description:**  
**//Input: CompressedCharacter[157] as One dimensional Array of Characters**  
**//Input: CompressedECG as String**  
**//Output: Freq[157] as Two Dimensional Array of Integer**

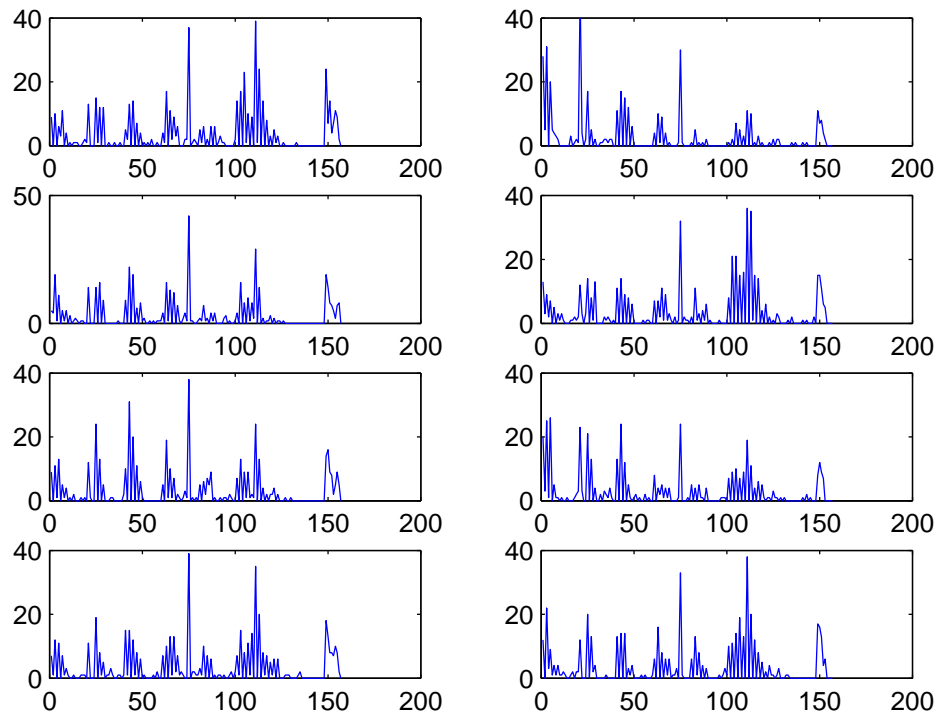
---

**Loop Until the end of CompressedECG**  
    **Find the index, i of CompressedCharacter that matches**  
    **ReadChar(CompressedECG)**  
    **Freq[i]= Freq[i] + 1**  
**End Loop**

---

(the 157 alpha and numeric characters shown in Figure 3.37) and their frequencies as the attribute for DMA. To obtain the character frequencies of 157 characters (both alpha and numeric), we first populate all this 157 characters (Figure 3.37) in an array (CompressedCharacter[157] in Algorithm 6). Algorithm 6 then reads all the characters from the compressed ECG segment and increments the corresponding frequencies (Freq[i], where  $i$  is the matched character read from compressed ECG). ReadChar() function in Algorithm 6 reads one character from the compressed ECG segment and forwards the position. Eventually, the looping procedure reads all the characters present in the compressed ECG segment and updates the frequency of each characters (CompressedCharacter[157]).

After using Algorithm 6, frequencies for all the 36 ECG segments (each segment has 157 frequencies) was calculated (5652 Character frequencies in total for the 9 different nsrdb entries and 18840 character frequencies in total for the full 120 entries). Figure 3.41 shows the character frequencies of Entry 16265 and 16272 for different ECG segments (shown in Figure 3.40).



*Figure 3.41: Frequencies of 157 Characters on the Eight Different ECG Segments for nsrdb Entry 16265 (4 Segments - in First Column) and 16272 (4 Segments - in Second Column)[Phy, Accessed 2009]*

Table 3.10: Average Frequencies of the 16 Selected Attributes for the Nine Entries (or Patient). ECG Segments Collected from Public Database [Phy, Accessed 2009]

Att	16265	16273	16483	16773	16786	16795	17052	17453	18177
@	7.5	25.75	40.75	18.5	15	20	42.25	21.25	16.25
\$	13	24.75	27.25	16.75	27.25	20.5	42.25	19.75	15.5
+	0.5	4.75	0.5	1.5	0	5.25	1	0	0.75
i	0.25	0	0	1.75	0	2.25	0.25	0.5	0
Ö	1	0.75	0.75	0	1.25	0	0.25	0	1.75
Û	39	29.25	30.25	29	41.75	17.25	40.75	15	36.75
r	17.75	22.75	16	27.5	26.5	12.5	1.75	12.5	32.25
v	4.5	9.5	9.5	13	16	7.5	0.75	6	12
D	0	5	4	7.25	2.5	1.5	0.5	0.5	3.5
Z	0	0	2.75	0.75	0	0	0	1.25	1.5
0-50	18.75	12	19.75	20.75	11.25	15	11	11.5	21.75
100-150	9.75	6.25	9	5	4.5	2.25	6.5	12	16.25
200-250	5.25	3.5	9.25	9	4.75	3	2	5.75	2
250-300	7	5	4.25	4	5.5	0.75	3.5	1.75	0
300-350	8.25	5.25	0	2	7.25	0	0	2	0
350-400	4.25	6.75	0	1.5	2.25	0	0	4.5	0

### Attribute Selection

In the attribute selection process, FilteredSubsetEval was used as evaluator with BestFirst searching (refer to WEKA, <http://www.cs.waikato.ac.nz/ml/weka/>). This resulted in selection of 16 key attributes (or compressed characters) that can be used for identifying person (each person representing one class). This is substantially less number of attributes compared to the 157 total attribute for which the frequencies have been created earlier (Algorithm 6). These selected attributes were used for clustering individuals.

Figures 3.42 and 3.43 show the selected character frequencies for entry 15265 and 16272 for different cases.

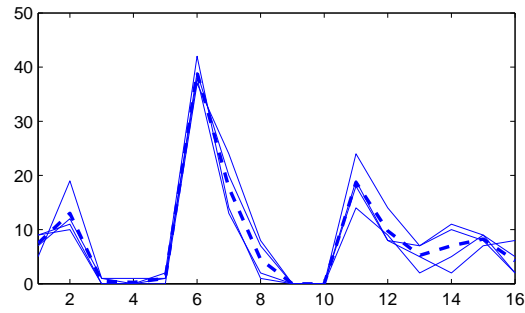


Figure 3.42: Frequencies of 16 Selected Characters (or Attributes) for Entry no 16265

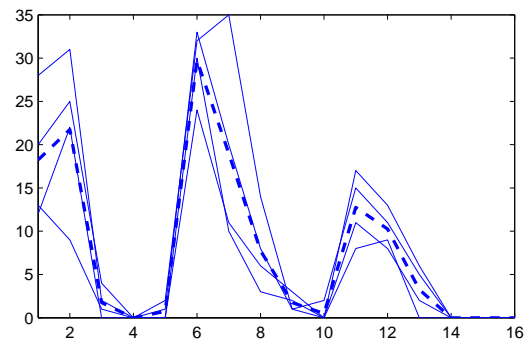


Figure 3.43: Eight Different ECG Segments for nsrdb Entry 16265 (4 Segments - in First Column) and 16272 (4 Segments - in Second Column)[Phy, Accessed 2009]

### Clustering

EM was chosen to cluster the 36 ECG entries (collected from 9 nsrdb entries) into 9 classes (each class represents a particular individual or Entry no.). A 100 % accuracy was obtained with EM, classes to cluster evaluation. Therefore, each of the nine classes contained four ECG segments grouped by a particular nsrdb entry. Table 3.11 shows the cluster means (M) and cluster deviation (S) from their corresponding means for all the attributes (16 attributes) against 9 classes.

The log likelihood value for applying EM on the selected attribute set to form 9 clusters (apriori) was -32.62486.

Then we extended our experimentation with 21 other entries (therefore, 30 entries in total) from other databases of physiobank [Phy, Accessed 2009] and could successfully group them.

This successful clustering demonstrates the fact that person can be identified from their compressed ECG, from where only 16 attributes are used.

### 3.9 Performance Comparison

Performance comparison of the PDM method and Data Mining based ECG biometric from compressed ECG were conducted against many of the existing ECG biometric techniques in terms of misclassification rate, template size and computational cost. Our proposed methods were proven to perform better than existing algorithms when compared for lower misclassification rate, smaller template size and minimal computational requirements while performing template matching.



Table 3.11: Cluster Means (Denoted by  $M$ ) and Deviations (Denoted by  $S$ ) for all the 9 Clusters, Against Each of the 16 Selected Attributes)

Att	Cls1	Cls2	Cls3	Cls4	Cls5	Cls6	Cls7	Cls8	Cls9
1 M	40.75	21.25	7.5	20.0001	18.5	16.25	15	25.75	42.2501
1 S	10.1088	3.6997	1.6583	4.2428	2.6926	3.9607	4.6368	1.9203	6.1796
3 M	27.25	19.75	13	20.5001	16.75	15.5	27.25	24.75	42.25
3 S	3.4187	2.3848	3.5355	8.6459	1.479	3.6401	6.9417	3.8971	6.3787
37 M	0.5	0	0.5	5.25	1.5	0.75	0	4.75	1
37 S	0.5	2.4068	0.5	2.8614	1.118	1.299	2.4068	2.3848	1.2247
46 M	0	0.5	0.25	2.25	1.75	0	0	0	0.25
46 S	0.9694	0.5	0.433	1.0897	0.8292	0.9694	0.9694	0.9694	0.433
72 M	0.75	0	1	0	0	1.75	1.25	0.75	0.25
72 S	0.8292	0.7617	0.7071	0.7617	0.7617	0.433	0.433	0.433	0.433
75 M	30.25	15	39	17.2502	29	36.75	41.75	29.25	40.75
75 S	1.479	1.8708	1.8708	3.7672	2.1213	1.299	2.586	3.9607	6.057
113 M	16	12.5	17.75	12.4999	27.5	32.25	26.5	22.75	1.75
113 S	2.5495	2.958	4.4931	3.6401	4.3875	5.6734	6.0622	2.3848	1.479
117 M	9.5	6	4.5	7.5	13	12	16	9.5	0.75
117 S	3.9051	1.5811	3.0414	2.0616	2.1213	3.0822	3.1623	3.2016	1.299
125 M	4	0.5	0	1.5	7.25	3.5	2.5	5	0.5
125 S	1	0.5	2.7813	0.866	2.3848	3.3541	1.118	0.7071	0.5
147 M	2.75	1.25	0	0	0.75	1.5	0	0	0
147 S	1.299	0.8292	1.1166	1.1166	0.8292	0.5	1.1166	1.1166	1.1166
149 M	19.75	11.5	18.75	15	20.75	21.75	11.25	12	11
149 S	3.9607	2.6926	3.562	1.5811	2.586	3.4911	1.479	3.0822	2.1213
151 M	9	12	9.75	2.25	5	16.25	4.5	6.25	6.5
151 S	0.7071	1.2247	2.4875	2.2776	1.5811	6.3787	2.0616	2.0463	0.5
153 M	9.25	5.75	5.25	3	9	2	4.75	3.5	2
153 S	1.0897	2.586	2.0463	0.7071	1.4142	2	1.7854	2.0616	1.4142
154 M	4.25	1.75	7	0.75	4	0	5.5	5	3.5
154 S	1.0897	1.9203	3.6742	0.433	2.2361	2.9519	2.1794	1.5811	1.8028
155 M	0	2	8.25	0	2	0	7.25	5.25	0
155 S	3.4257	1.5811	0.8292	3.4257	0.7071	3.4257	1.6394	2.8614	3.4257
156 M	0	4.5	4.25	0	1.5	0	2.25	6.75	0
156 S	2.6203	1.118	2.4875	2.6203	0.866	2.6203	0.8292	1.0897	2.6203

### 3.9.1 Misclassification Rate

At first, our methods were compared against existing methods of ECG biometric with PRD, CC and WDM based technique. These tests were performed by the most recent research in ECG biometric. Three seconds ECG packets were obtained in two different times from 25 persons resulting in 50 ECG segments in total.

When PRD, CC and WDM were applied to recognize person, they resulted in higher misclassification rate. Whereas, the polynomial coefficient distance measurement technique resulted in a substantially lower rate of misclassifications. Out of the 25 person only two persons were misclassified. As already mentioned before, these misclassification occurred because of not prioritizing the ECG features and occurrence of abnormal beats. However, we adopted Algorithm 1 (for PDM), which assigned priority for distance measurements with QRS complex being the highest priority and P wave being the lowest priority. To deal with the problem of ectopic beat, Algorithm 2 (for PDM) was obtained during the acquisition phase. Therefore, all the misclassification could be avoided. Table 3.12 compares the lower misclassification rate of the proposed PDM method with recent ECG biometric matching algorithms. Table 3.13 compares the PDM method with other biometric modalities. According to our experimentation, ECG Biometric from Compressed ECG using DM technique didn't have any misclassifications.

### 3.9.2 Template Size

As mentioned earlier, the size of the template for biometric data has a huge impact on the overall performance of the biometric system. A system that requires larger vector of

Table 3.12: Misclassification Rate for PRD, CC, WDM and the Proposed ECG Biometric from Compressed ECG (Applying Data Mining Agent (DMA))

Method	Misclassification Rate (%)
PRD [Chan et al., 2008]	25
CC [Chan et al., 2008]	21
WDM [Chan et al., 2008]	11
PDM (without Alg. 1, without Alg.2) [Sufi et al., 2010a; Sufi and Khalil, 2008a]	8
PDM (with Alg. 1, without Alg.2) [Sufi et al., 2010a; Sufi and Khalil, 2008a]	4
PDM (with Alg. 1, with Alg.2) [Sufi et al., 2010a; Sufi and Khalil, 2008a]	0
ECG Biometric from Compressed ECG using DM	0

Table 3.13: FRM and FNRR Across Different Modalities

Modality	FMR (%)	FNMR (%)	Reference
Face	1	10	[Phillips et al., Last accessed: Jan. 2009]
Fingerprint	0.01	2.54	[Maio et al., 2004]
Iris	0.00129	0.583	[Group, 2005]
On-line signature	2.89	2.89	[D.-Y. et al., 2004]
Speech	6	6	[Reynolds et al., 2004]
ECG	4	4	PDM (without Alg. 1, without Alg. 2) [Sufi et al., 2010a; Sufi and Khalil, 2008a]
ECG	2	2	PMD (with Alg. 1, without Alg. 2) [Sufi et al., 2010a; Sufi and Khalil, 2008a]
ECG	0	0	PDM (with Alg. 1 + with Alg. 2) [Sufi et al., 2010a; Sufi and Khalil, 2008a]
ECG	0	0	ECG Biometric from Compressed ECG using DM

enrolment data can encompass processing delay while performing identification tasks on a reasonable data set. Moreover, there are issues surrounding longer transmission time and higher storage requirements of the enrolment data. Therefore, for faster performance, faster transmission of biometric data and minimal storage, the size of the template data should be minimal. As seen from Table 3.2, 3.3 and 3.4 the biometric data required for subject 1 is only 318 bytes. During our experimentation, the active range for this template (enrolment or recognition data) was 228 -402 bytes, with an average of 340 bytes. The most recent work based on ECG based human identification requires at least 600 bytes (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 (enrolment/verification data) [Wubbeler et al., 2007]. For ECG biometric presented in [Chan et al., 2008], experimentation with PRD, CC and WDM based measurement was performed with variable length of ECG from 32 ms to 512 ms. For 32 ms ECG segment, with a 360 Hz sampling frequency results in 12 ECG samples ( $.36 \times 322$ ) or 126 bytes of data. Similarly, with larger ECG segment of 512 ms with the same sampling frequency, 185 ECG samples are required (with an average size of 1846 bytes). However, with only 12 sample (for the case of 32 ms ECG segment), the misclassification rate is higher, since it can only represent one third of QRS complex (for 360 Hz sampling frequency). Therefore, not even a single feature can be represented within 126 bytes ECG segment (360 Hz). According to Table 3.14, the proposed polynomial distance measurement technique shows highest level of accuracy with minimal biometric template size.

According to Table 3.14, the ECG Biometric from Compressed ECG without DM technique has minimal template size. Compared to the face recognition biometric template size

*Table 3.14: Comparison of Template Sizes*

Biometric Data Type	Size in bytes
Iris [Yu et al., 2008]	512
Face [Yu et al., 2008]	153600-307200
Voice [Yu et al., 2008]	2048-10240
ECG [Wubbelier et al., 2007]	600
ECG (WDM) [Chan et al., 2008]	1371
ECG (PRD / CC) [Chan et al., 2008]	2210
ECG (PDM) [Sufi et al., 2010a; Sufi and Khalil, 2008a]	340
ECG Biometric from Compressed ECG without DM	37
ECG Biometric from Compressed ECG using DM	36

of 307200 bytes [Yu et al., 2008], the biometric template of ECG Biometric from Compressed ECG without DM is approximately 8302 times smaller in size. On the other hand, compared to the PDM technique of ECG based biometric, ECG Biometric from Compressed ECG without DM biometric template is at least 9 times smaller in template size.

If matching of 1 byte takes  $t_b$  amount of time, then according to Table 3.14, ECG Biometric from Compressed ECG using DM consumes  $(36 \times t_b)$  time respectively. Therefore, ECG Biometric from Compressed ECG using DM method is approximately 8533 times faster than Face [Yu et al., 2008] recognition template with 307200 bytes of data. Also, the template size of the proposed method is 61 times smaller than existing PRD [Chan et al., 2008] and up to 9 times smaller than our previous ECG biometric method based on Polynomial Distance Measurement (PDM) [Sufi et al., 2010a; Sufi and Khalil, 2008a]. Clearly, the proposed method requires less storage and executes faster for person identification task compared to the existing biometric mechanisms.

*Table 3.15: Comparison of Number of Operations (NOP) for PRD, CC, WDM and PDM*

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	1158	463	800	96

### 3.9.3 Computational Cost

Computational cost is one of the major factors that determine the acceptability of a biometric system, since many of the biometric systems are integrated within a small box with less computational power. For this research, we performed the comparison of computational power based on the number of operations required to compute similarity matching between the enrolled data and recognition data. Table 3.15 shows the computational cost for PRD, CC, WDM and the proposed PDM method while performing these matching. Matching is thought to be the core computational cost involved for biometric, since this matching is required to be performed across all the entries (templates) within the database. If the database contains 100 biometric entries, 100 matching are needed to ascertain the minimum distance. On the other hand, wavelet decomposition to calculate the wavelet coefficients for WDM [Chan et al., 2008], or polynomial creation to calculate the values of polynomial coefficients for PDM are only one time cost. Therefore, the cost for polynomial computation is only a minute fraction of the cost associated with database wide matching.

The ECG segment to calculate PRD, CC and WDM (both for Table 3.14 and Table 3.15)

were 231 samples, which contained a single heart beat with all the ECG feature waves. For WDM calculation of Table 3.15 256 coefficients were generated for 231 ECG sample points. Out of these 256 coefficients, only 136 coefficients were utilized after taking the threshold value ( $\xi$ ) into consideration (please refer to Eq. 3.3). Therefore, conditional operations were evaluated as well, considering the denominator of Eq. 3.3. It is evident from Table 3.15 PDM is computationally more inexpensive and viable than many of the existing algorithms.

### 3.9.4 Conclusion

In this chapter, the second research question of faster patient authentication was answered with new ECG biometric methods. First, we proposed two ECG biometric techniques that do not need fiducial point detection and suitable for telecardiology application not adopting our compression mechanism. Then, we proposed another two ECG biometric algorithms based on compressed ECG packets, generated by our proposed compression algorithm (Chapter 2). Apart from reading less input, the proposed ECG based biometric executes faster than the existing ECG based biometric techniques because of smaller template size (Table 3.14). The compressed ECG biometric with DM method was found to be 61 times faster than PRD based ECG biometric [Chan et al., 2008], 38 times faster than WDM [Chan et al., 2008], 16 times faster than ECG biometric of [Wubbeler et al., 2007] and 9 times faster than our previous ECG biometric method of PDM.

Now that we have the innovative techniques available for efficient transmission and faster authentication, we need technologies for secured ECG transmission, so that the patient's privacy is protected. In our next chapter, we will investigate more on secured ECG trans-

mission.



## Chapter 4

# Securing the ECG

In our previous chapters, we have successfully ensured faster and efficient transmission (with a faster ECG compression algorithm) and automated authentication (with ECG biometric). Our third research question deals with the establishment of secured ECG transmission to protect a patient's privacy. This chapter is our effort in answering the third research question.

After the introduction of Health Information Protection and Privacy Act (HIPPA) of 1996 in US, physiological signals are required to be transmitted securely during remote monitoring of patients [Cen, Accessed 2008; Pub, 1996; Off, Accessed 2009; Lee and Lee, 2008]. A telemonitoring platform that ignores protection of private health information is a threat to patient's privacy. Unfortunately, existing telemonitoring platforms do not integrate any encryption, obfuscation/ anonymization technique for the conformance of HIPPA regulations. However, few researchers [Blount et. al., 2007] argue that if physiological signals (like ECG) are sent without the name of person, then there can be no way to determine (by a hacker) whose physiological signal is transmitted. Unfortunately, the work done in the

previous chapter and recent studies in ECG based biometric [Biel et al., 2001; Chan et al., 2008; Wubbeler et al., 2007; Poon et al., 2006; Israel et al., 2005; Irvine et al., 2001; Bui and Hatzinakos, 2008; Kyoso and Uchiyama, 2001; Kyoso, 2003; Shen et al., 2002; Shen, 2005; Shen and Tompkins, 2005; Wang et al., 2008; Hou and Andrews, 1978; Plataniotis et al., 2006; Kanade and Jain, 2005] shows that ECG can successfully be used to identify person. Hence, even though the name of the patient is disassociated from the physiological signal, it is possible to identify that person and retrieve his health information by using ECG biometric (as described in Chapter 3). Therefore, research in encryption, obfuscation/ anonymization is deemed to be crucial for a health monitoring platform seeking wide acceptance. In this respect, we have successfully designed and implemented three methods of encoding/ encryption, obfuscation/ anonymization which can be easily integrated within our proposed mobile phone based telemonitoring framework.

The encoding/ encryption mechanism is based on character substitution and permutation ciphers on the compressed ECG. This method was also compared with conventional AES and DES encryption techniques. The proposed encoding/ encryption method provides a substantially higher security strength and realtime performance on mobile platform (experimented on smart phones and PCs).

Secondly, a novel anonymization technique was designed and developed which segregates the low frequency components from the ECG signal and performs partial encryption with DES. The segregation of the low frequency component was performed by utilizing both discrete wavelet transform (DWT) and packet wavelets. However, during the packet wavelet implementation the secret key size was nearly halved, compared to that of DWT. We realized

that the key size can be further reduced for more efficient key distribution. Therefore, we researched on an alternative method that works on uncompressed ECG.

Finally, an alternative obfuscation/ anonymization method was designed and implemented that detects each of the ECG features (P Wave, QRS Complex and T Wave) and replaces them with a noised ECG. The key size generated by this method was several times lower than our previous wavelet based anonymization technique. Moreover, the noised ECG appears to be a regular ECG, while in reality it is substantially different to the original one. Therefore, to the hacker, existing hacking tools including brute force attack become useless.

#### 4.1 Why Do We Need Secured ECG Transmission?

Biosignals like ECG contains crucial health information of the patient [Kusumoto, 2009; Clifford et al., 2006; Akselrod et al., 2007]. However, these biosignals are often transmitted without any encryption from the acquisition device to the local server and from the local server to the central server (as seen in Fig. 4.1). It is most vulnerable to security threats while being transmitted from local server to central server over the public internet. Existing algorithms automatically reads the ECG signals and successfully classify whether a patient has Bradycardia, Tachycardia, Atrial Premature Beats, Atrial Flutter, Atrial Fibrillation, Premature Ventricular contraction (PVCs) with minimal errors [Bartolo et al., 2001; Kumar et al., 2007; Hamilton and Tompkins, 1986; Friesen et al., 1990; Clifford et al., 2006]. Apart from releasing cardiovascular details, ECG can successfully identify a particular person as shown in Chapter 3. Some existing mobile phone based remote health monitoring platform uses patient identifiers, which is transmitted along with the biosignal [Blount et. al., 2007],

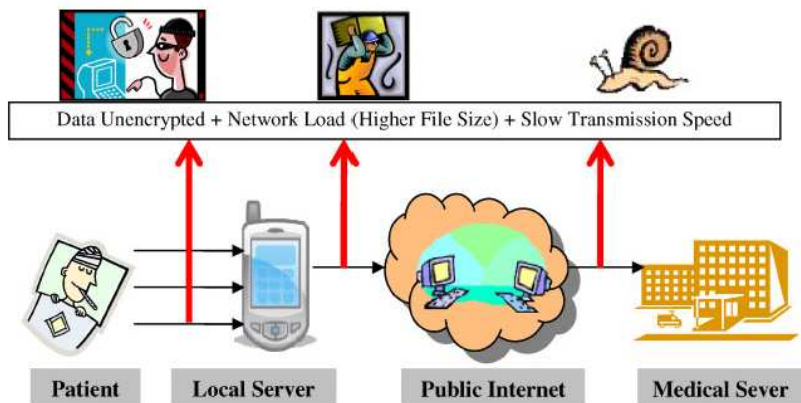
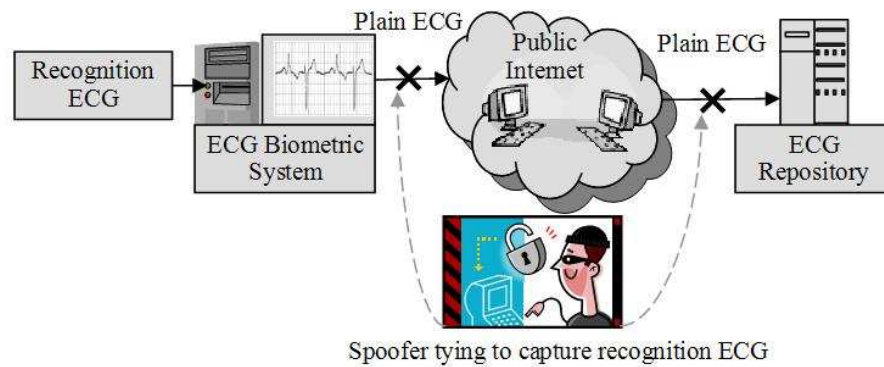


Figure 4.1: Typical Realtime Telemonitoring Scenario

instead of patients' name. Even though, just from the patient ID, the patient is thought to be unidentified (since, the mapping between patient ID and patient particulars are maintained in secured server as in [Blount et. al., 2007]), recent research in ECG analysis shows that ECG can serve as a biometric entity for person Identification. Hence, the platform presented in [Hung and Zhang, 2003; Jasemian and Arendt-Nielsen, 2005; Blount et. al., 2007; Lee et al., 2007; Gao et al., 2005; Zhou et al., 2005] and previous Chapters can not be directly implemented for transmission of ECG signals, without providing additional security mechanisms for protection of private health information.

In one possible scenario as shown in Fig. 4.2, transmission of recognition ECG over the public network (Internet) as plain text can subject to spoof attack, where a malicious user intercepts the ECG recognition data and records it, without being noticed. It is possible for this spoofer to use the recognition ECG to gain access to a secured service by replay attack, where an unauthorized person uses the captured ECG (of an authorized personnel) for ECG based biometric system. Therefore, for prevention of possible replay attack by the spoofers, ECG data must be anonymized before transmission over the public media.



*Figure 4.2: Possible Attack points to Acquire Recognition ECG for Replay Attack*

Spoofing is a critical threat to biometric entities like fingerprint and iris as we learned recently that they are likely to be spoofed [Reynolds et al., 2004; Matsumoto, 2004; Matsumoto et al., 2002]. Spoof attacks can occur by using artificially created biometrics by attacking via input port and at database, or even by reproduction of data such as a noise obfuscated facial image that allow to establish a fake identity [Schuckers, 2002]. For handprint, fingerprint, key stroke pattern, face, hand shape and couple of other biometric measurement (except DNA) standard information security applies for making it spoof resistant. ECG biometric is even more vulnerable to spoofing attack, since ECG is not only a biometric entity, but also a container of cardiovascular information as mentioned earlier.

Therefore, encryption of ECG is required before transmission through the public telephony / mobile network for three crucial reasons; 'protection of person identification', 'protection of ECG biometric template' and 'protection of cardiovascular condition'. Application of innovative anonymization technique on ECG, not only prevents future spoofing for identity theft but also protects health privacy. This private health information is emphasised to follow strict privacy regulation standardized by Health Insurance Portability and Account-

ability Act (HIPAA) [Cen, Accessed 2008; Pub, 1996]. Many countries are coming forward to enforce health related privacy regulations stipulating domestic laws [Off, Accessed 2009; Lee and Lee, 2008].

## 4.2 Securing the ECG: Encryption, Obfuscation/ Anonymization

Now that we know the motivation for securing ECG, proper methodology for hiding ECG feature waves (P wave, QRS complex and T wave) must be researched. Within this chapter, we will be focusing on three different types of methodologies for securing the ECG signal.

1. *ECG Encryption*: For ECG encryption, we have used permutation cipher during the encoding phase (chapter 2). After this encoding, with character shuffling the ECG becomes secured and without the knowledge of the permutation key, original ECG can not be retrieved. Moreover, using existing compression techniques (like, AES, DES, Rinjadel) with existing compression algorithms (like WinZip, bzip, pkzip etc.) security strength of the encoded ECG can be raised further.
2. *ECG Anonymization with Wavelet*: We used two novel ECG anonymization techniques based on Discrete Wavelet Transform and Wavelet Packets. The wavelet packets were proven to be providing 100% anonymization, showing robustness against replay attack by the spoofer. Even with the most recent available technology, the anonymized ECG remained totally unidentified. A key, which is only 5.8% of the original ECG (with Wavelet Packets), is securely distributed to the authorized personnel for reconstruction of the original ECG. Wavelet based anonymization served the purpose of initial assessment for securing uncompressed ECG signal (i.e. plain text ECG). However, a smaller

key size makes the key distribution more efficient. Therefore, an alternative method with even lower key size required to be sought.

3. *ECG Obfuscation with Noise*: A new ECG obfuscation method was designed and implemented on different subjects using added noises corresponding to each of the ECG features. This obfuscated ECG can be freely distributed over the internet without the necessity of encryption, since the original features needed to identify personal information of the patient remain concealed. Only authorized personnel possessing a secret key will be able to reconstruct the original ECG from the obfuscated ECG. Distribution of the key is extremely efficient and fast due to small size (only 0.04% to 0.09% of the original ECG file). The key size of noise based ECG anonymization method was approximately 64.44 times lower in size than our wavelet based ECG anonymization technique. Moreover, if the obfuscated ECG reaches to the wrong hand (hacker), it would appear as regular ECG without encryption. Therefore, traditional decryption techniques including powerful brute force attack are useless against this obfuscation.

### 4.3 Joint Encoding, Compression and Encryption

In chapter 2, an Encoding (compression) mechanism to compress ECG signal was presented. However, Without the knowledge of the algorithm that was used to compress a plaintext, compression can serve the purpose of a very basic encryption, which is why a joint compression and encryption mechanism can strengthen security while reducing the overall file size of the chosen plaintext (Multimedia, Audio, Video, Speech etc.) [Wu and Kuo, 2005; Mao and Wu, 2006; Cheng and Li, 2000]. Previous research in joint compression and encryption has

addressed the problem of fast and secured transmission of multimedia, video, images, speech and other data files [Wu and Kuo, 2005; Mao and Wu, 2006; Cheng and Li, 2000]. However, content of ECG file has its own format, which is fundamentally different from multimedia, video, images and speech. We envisage a joint encryption and compression method that will be deployed in mobile phone based realtime telemonitoring scenario, where fast computation and fast data transmission are of paramount importance. Therefore, analysis of compression and encryption are required to be evaluated for ECG files on different platforms. Also, the ordering of encryption and compression performed on the same ECG file may generate different sizes of encoded ECG stream. Three different arrangements of encryption and compression are depicted in Figure 4.4 that are evaluated in this section. Most of the compression techniques, specifically entropy coder and encryption algorithms perform similar outcome by creation of redundancy free encoded text from plain text [Wu and Kuo, 2005]. To decode the encoded text specific information is required. In the case of encrypted text the cipher key is the information and in the case of entropy coded text it is statistical model [Wu and Kuo, 2005].

According to our literature survey, joint encryption and compression mechanism has not been researched for any physiological signals. This motivated us to pursue our research on an encoding scheme (joint compression and encryption) designed specifically for physiological signals, like ECG, to protect the patient's privacy.

We are proposing to use a permutation cipher before performing the actual character substitution. This basically means shuffling of the character sets, just before the character substitution starts. The specific order for the permutation can be used as a key for decryp-



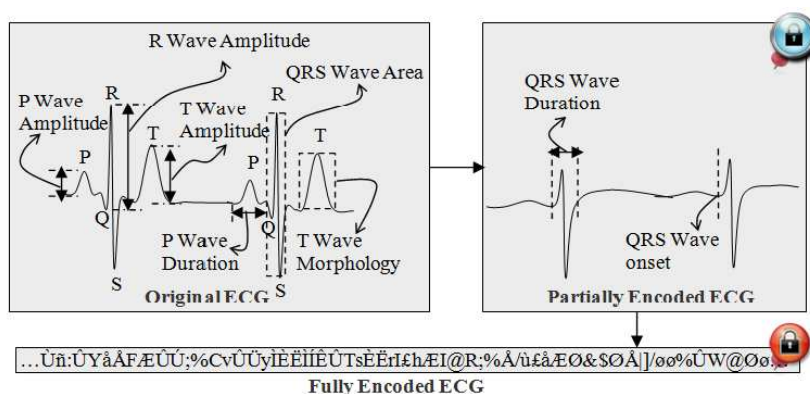


Figure 4.3: Transformation of the ECG with Proposed Encoding Method

tion. Figure 4.3 shows the basic transformation of ECG signal to an encrypted text using a permutation cipher.

#### 4.3.1 2 Phase Encryption-Compression

At first, we employed an encryption (DES Symmetric) mechanism on selected ECG files from MIT-BIH Arrhythmia database. We found an increase in file sizes as observed in Table I. Therefore, to obtain faster transmission, we compressed the encrypted files with standard Zip library. However, no benefit was observed in respect to faster file transmission, since no compression was achieved. This problem was also observed for multimedia encryption followed by compression in previous research [Mao and Wu, 2006]. The author concluded that since encryption significantly changes the statistical characteristics of the encrypted file, low level of compressibility is achieved by the compression algorithm [Mao and Wu, 2006]. Table 4.1 shows the results for this 2 Phase Encryption-Compression process. Here,  $S_o$ ,  $S_s$  and  $S_c$  refer to file sizes for original, encrypted and compressed ECG files in Bytes. Encryption and compression times (in ms) are respectively denoted by  $T_s$  and  $T_c$ . Other

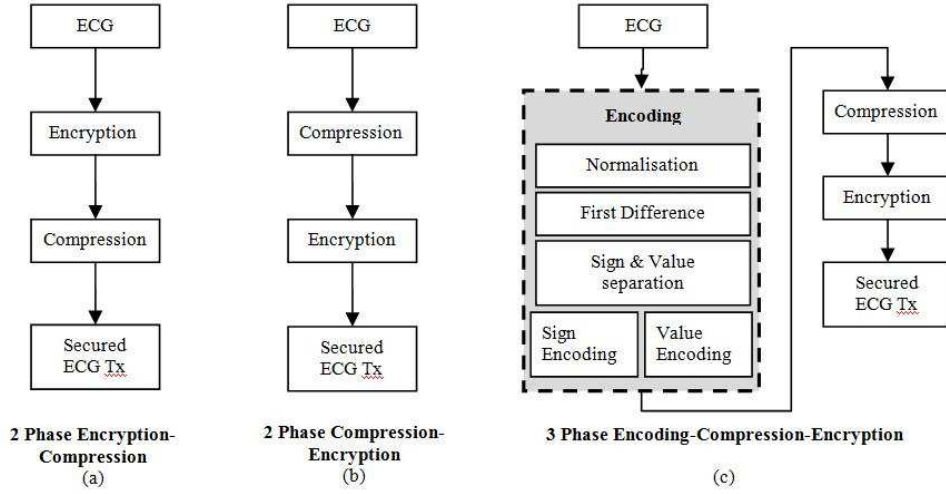


Figure 4.4: Arrangements of Encoding, Compression and Encryption (a) 2 Phase Encryption-Compression using existing encryption and compression techniques (b) 2 Phase Compression-Encryption using existing compression and encryption techniques (c) 3 Phase Encoding-Encryption-Compression using the proposed encoding and existing compression-encryption techniques.

parameters for Table 4.1 are defined in Eqs. 4.1, 4.2 and 4.3.

Compression Ratio after encryption,

$$CR_{os} = \frac{S_o}{S_s} \quad (4.1)$$

Compression Ratio after compression,

$$CR_{sc} = \frac{S_s}{S_c} \quad (4.2)$$

Total Compression Ratio,

$$CR_t = \frac{S_o}{S_c} \text{ or } CR_t = CR_{os} \times CR_{sc} \quad (4.3)$$

Table 4.1: Results for Securing ECG with 2 Phase Compression-Encryption Technique

MIT_BIH No.	$S_o$	Encryption		Compression		$CR_t$	$T_s$	$T_c$	$T_t$
		$S_s$	$CR_{os}$	$S_c$	$CR_{sc}$				
100	172197	172200	0.99	172405	0.99	0.99	10	46	56
102	171033	171040	0.99	171245	0.99	0.99	46	46	92
105	170912	170920	0.99	171125	0.99	0.99	10	46	56
111	169280	169288	0.99	169493	0.99	0.99	10	46	56
114	171214	171216	0.99	171421	0.99	0.99	10	46	56
201	171367	171368	0.99	171573	0.99	0.99	15	31	46
210	170549	170552	0.99	170757	0.99	0.99	10	46	56
213	168640	168648	0.99	168853	0.99	0.99	0	46	46
222	170355	170360	0.99	170565	0.99	0.99	15	31	46
228	168208	168216	0.99	168421	0.99	0.99	0	62	62
231	169048	169056	0.99	169261	0.99	0.99	15	31	46
234	170184	170192	0.99	170397	0.99	0.99	15	31	46

Therefore, total time for Table 4.1 is,

$$T_t = T_s + T_c \quad (4.4)$$

This achieved an average compression ratio of 0.99 (less than 1 or increased file size).

### 4.3.2 2 Phase Compression-Encryption

Compression can also be applied before encryption as in previous research [Mao and Wu, 2006] performed on multimedia data. Therefore, we implemented the second set of arrangement of 2 Phase Compression-Encryption mechanism as depicted in Fig. 4.4 (b). The results are summarized in Table 4.2. As clearly seen, with this mechanism, a higher compression ratio of up to 16.71 was achieved. For Table 4.2, compression ratios are defined in Eqs. 4.5, 4.6 and 4.7.

Table 4.2: Results for Securing ECG with 2 Phase Encryption-Compression Technique

MIT_BIH No.	$S_o$	Compression		Encryption		$CR_t$	$T_c$	$T_s$	$T_t$
		$S_c$	$CR_{os}$	$S_s$	$CR_{cs}$				
100	172197	20076	8.58	10488	1.91	16.42	531	10	541
102	171033	21700	7.88	11192	1.94	15.28	578	10	588
105	170912	23220	7.36	12368	1.88	13.82	593	10	603
111	169280	23647	7.16	12472	1.89	13.57	562	10	572
114	171214	21003	8.15	11224	1.87	15.25	562	10	572
201	171367	19851	8.63	10258	1.94	16.71	468	10	478
210	170549	22309	7.64	11640	1.92	14.65	593	10	603
213	168640	28330	5.95	14632	1.94	11.53	640	15	655
222	170355	21425	7.95	11248	1.90	15.15	562	0	562
228	168208	25073	6.71	13376	1.87	12.58	578	10	588
231	169048	23176	7.29	12144	1.91	13.92	531	10	541
234	170184	22365	7.61	11808	1.89	14.41	546	10	556

Compression Ratio after compression,

$$CR_{oc} = \frac{S_o}{S_c} \quad (4.5)$$

Compression Ratio after encryption,

$$CR_{cs} = \frac{S_c}{S_s} \quad (4.6)$$

Compression Ratio after encryption,

$$CR_t = \frac{S_o}{S_s} \text{ or } CR_t = CR_{oc} \times CR_{cs} \quad (4.7)$$

### 4.3.3 3 Phase Encoding-Compression-Encryption

Finally, we placed our encoding method, which already have the benefit of compression of the ECG signal with basic encryption, before applying general (existing) compression and encryption mechanisms. This method was referred as 3 Phase Encoding-Compression-Encryption (ECE) mechanism in Fig. 4.4 (c). This 3 Phase ECE resulted an amazing 20.15 (highest) compression ratio with increased security. Table 4.3 shows the improvements.  $S_e$  and  $T_e$  denotes the size of encoded ECG (in Bytes) and time required for encoding (in ms) in Table 4.3. Other parameters are derived from Eqs. 4.8, 4.9, 4.10, 4.11 and 4.12.

Compression Ratio after encoding,

$$CR_{oe} = \frac{S_o}{S_e} \quad (4.8)$$

Compression Ratio after compression,

$$CR_{ec} = \frac{S_e}{S_c} \quad (4.9)$$

Compression Ratio after encryption,

$$CR_{cs} = \frac{S_c}{S_s} \quad (4.10)$$

Total Compression Ratio,

$$CR_t = \frac{S_o}{S_s} \text{ or } CR_t = CR_{oe} \times CR_{ec} \times CR_{cs} \quad (4.11)$$

Total time,

$$T_t = T_e + T_c + T_s \quad (4.12)$$

#### 4.3.4 Analysis of Performance

Requirement of increased time is often the indication of higher computational complexities. Therefore, faster algorithm can be seamlessly integrated within the small device environment (with less computational resources) of telemonitoring. However, compression of enormous ECG file is also of crucial importance for faster data transmission. Henceforth, the mechanism that raises the compression ratio and security strength substantially with minimal computational complexity is highly desirable for telemonitoring. The result from Table 4.1, 4.2 and 4.3 was standardised with the concept of time required to raise one unit of compression ratio,  $T_{CR}$ , with Eq. 4.13.

Total time,

$$T_{CR} = \frac{T_t}{CR_t} \quad (4.13)$$

where,  $T_t$  and  $CR_t$  denotes the mean total time and mean total compression ratio. The purpose of  $T_{CR}$  is to present the competitive advantage for realtime telemonitoring by the 3 Phase ECE Mechanism over the other two mechanisms. It is apparent from Table 4.4 that 3 Phase ECE consumes minimal time in respect to raising the compression ratio of ECG file to a higher value. Our experimentation results indicate that higher compression

ratio can be achieved with DES rather than AES, even though AES offers higher security. Therefore, it (i.e. DES) is often preferred, when faster data transmission is crucial. Table 4.1, Table 4.2 and Table 4.3 reflect some of our best compressibility results achieved with DES. However, AES implementation is also part of our 18 preferred encryption implementations, which make our system robust in terms of security. More discussion about this robust security architecture will be presented later. Using AES before compression (on plain text ECG) results in a lower compression ratio (CRos of Table 4.1) of 0.75 as compared to 0.99 with DES (2 Phase Encryption Compression). Using AES after compression results in an average compression ratio (CRcs of Table 4.2) of 0.41 for 2 Phase Compression Encryption as compared to 1.905 with DES. AES Encryption implemented on 3 Phase ECE scenario produces an overall compression ratio (CRcs of Table 4.3) of 0.41 as compared to 1.893 achieved with DES. Therefore, it is evident from experimentation that for all the cases DES provides higher compressibility of ECG files at the expense of security.

As a comparison, the recent research of ECG compression shows that a compression ratio of 20 is achievable sacrificing a significant amount of data [Lu et al., 2000; Chen et al., 2006]. Percentage Root-Mean-Square Deviation (PRD) is the standard that quantifies the lost information. The PRDs are 7.52 and 6.13 respectively for [Lu et al., 2000] and [Lu et al., 2000], while raising the compression ratio to 20. However, the proposed 3 Phase ECE mechanism is completely lossless algorithm, where PRD is zero.

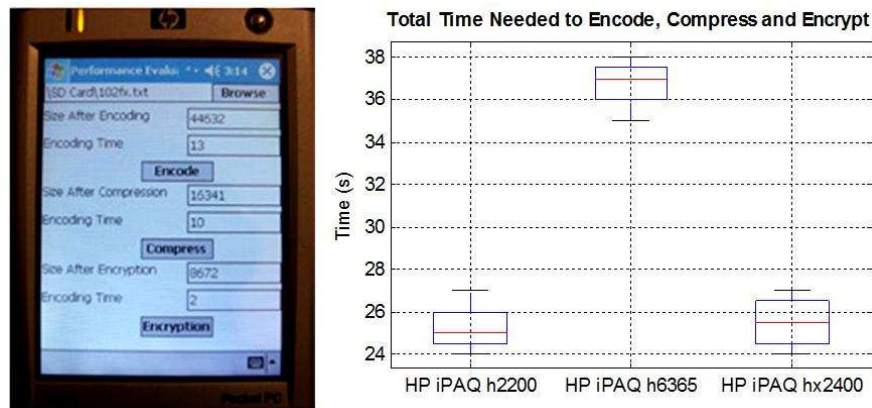


Figure 4.5: Time Requirement for 3 Phase Encoding-Compression-Encryption Mechanism on .Net Based Smart Device Platform (Pocket PC 2003 Device)

#### 4.3.5 Deployment of 3 Phase Encoding-Compression-Encryption Mechanism on the Mobile Platform

To evaluate whether faster execution speed indicates its suitability for less resourceful devices, 3 Phase ECE mechanism was deployed on both windows based pocket PC / Smart Phone platforms and Java based Mobile platform.

##### Deployment with .Net Compact Framework

The 3 Phase ECE mechanism was implemented on .Net Compact Framework environment with Microsoft Visual Studio 2005. It was executed on HP iPAQ h2200 Pocket PC, HP iPAQ hx2400 Pocket PC and HP iPAQ h6365 smart phone and execution times were noted for each of the three phase operations. These results are summarised in the box plot of Fig. 4.5.



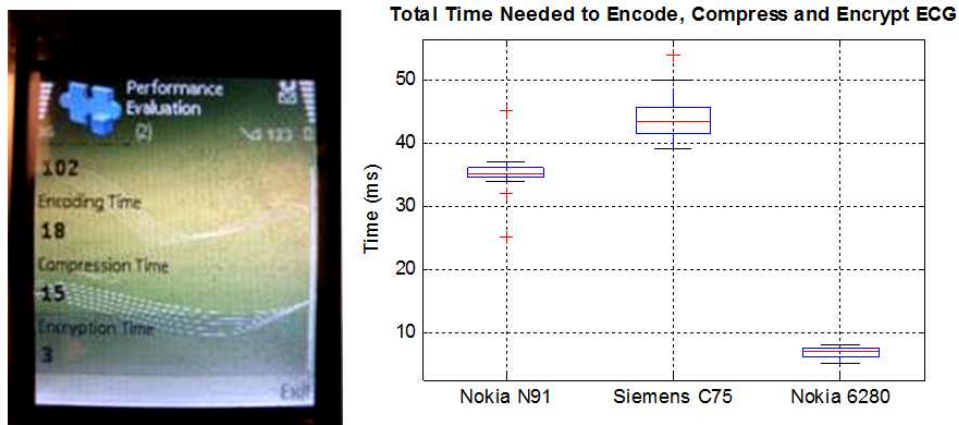


Figure 4.6: Time Requirement for 3 Phase Encode-Compress-Encrypt Mechanism on J2ME based MIDP (on CLDC) Platform

### Deployment with Java 2 Micro Edition

This mechanism was also programmed on Java 2 Micro Edition (J2ME) and implemented on Nokia N91, Siemens C75 and Nokia 6280 mobile phones. NetBeans 5.5 IDE with Mobility Pack was utilized to program, debug, test and deploy Java<sub>TM</sub> Midlets on the mobile phones. Surprisingly, the execution time requirement was minimal (ms ranges) as seen in Fig. 4.6.

HP iPAQ h6365 smart phone performed the worst during our experimentation with hand held and mobile platform. Therefore, the time distribution for that smart phone is presented to ascertain its real time applicability in Fig. 4.7.

#### 4.3.6 System Architecture for Joint Encoding, Compression & Encryption

Once the efficiency of proposed encoding method and 3 Phase ECE are revealed and evaluated on multiple platforms, it is ready to be placed on appropriate telemonitoring scenario. As depicted in Fig. 4.8, the system architecture contains three major building blocks: Secured Acquisition Device, Secured Mobile Phone and Central Server. There are two major

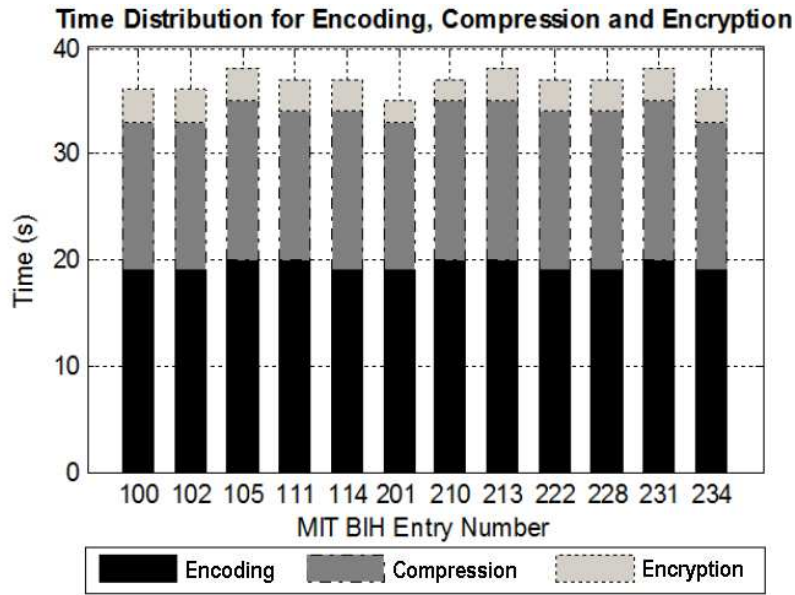


Figure 4.7: Time Distribution of 3 Phase Encoding-Compression-Encryption on HP iPAQ 6365

communication links to be secured: the link from the acquisition device to the mobile phone and the link from the mobile to the VPN mesh of Central servers.

### Secured Acquisition Device

We used Alive Heart Monitor [Ali, Accessed 2009] and in-house ECG acquisition device to collect ECG signal (from subjects) and transmit to the mobile device using well known Bluetooth protocol. Securing transmission of ECG signal from acquisition device to patient's mobile communication was done with 6 byte long globally unique Bluetooth Device Address (BDA), authentication, authorization, encryption and PIN exchange [Sufi et al., 2006b]. However, this Bluetooth based authentication consumes nearly 10 seconds of handshaking time and has security flaws, which may compromise integrity of the ECG data [Potter, 2004]. To minimize the authentication time while using in-house ECG acquisition device, we pro-

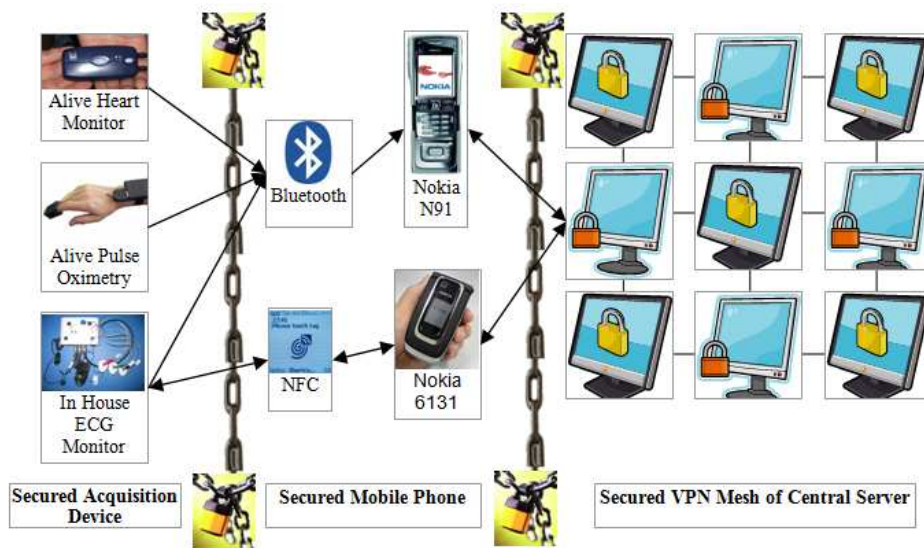


Figure 4.8: System Architecture of 3 Phase Encoding-Compression-Encryption Mechanism

posed and implemented RFID based touch scheme provided by Near Field Communication (NFC) [NFC, Accessed 2008] technology. The touch scheme allows us to initiate and establish Bluetooth link between the acquisition device (in-house only) and the mobile phone within seconds (nearly 2s). Nokia 6131 phone was utilized along with NFC starter kit (from Nextperts) [Nex, Accessed 2008] for deployment of NFC based authentication. We used JSR-257 Contactless Communication API and JSR-82 Bluetooth API within the mobile phone permitting NFC and Bluetooth based authentication-communication with the acquisition device [JCP, Accessed 2008].

Almost all of the existing devices (including Alive) transmit the ECG signal without encryption, ignoring privacy. However, our low complexity encoding method can be implemented directly on a microprocessor based acquisition device to secure transmission of ECG signals. This in-house ECG acquisition device supports compact flash based memory and has enough internal memory (buffer) to support both realtime and 'store-now-forward later'

operations. In the latter mode large amount of ECG data (several hours) can be stored depending on the size of the compact flash. Two major purposes of NFC module deployed in in-house acquisition device are 'fast and authorized establishment of Bluetooth link' and 'receiving of paired permutation key from the mobile phone to be used in our proposed encoding method (Fig. 4.9)'.

### **Secured Mobile Phone**

Once the mobile phone receives the ECG data, it is expected to be already encoded with the proposed encoding method (e.g. when ECG is acquired from the in-house acquisition device). However, that may not always be the case when the data is coming from commercially available monitoring devices like Alive Heart Monitor. In such a case, data must be encoded on the mobile phone with the proposed method, before performing compression and encryption.

As our 3 Phase ECE mechanism requires existing compression and encryption on the encoded text, we obtained algorithms of ICSharpCode.SharpZipLib (<http://www.icsharpcode.net>) library to compress the data. This library supports four types of compression (Zip, GZip, Tar, BZip2). Since this compression library was available in open source format, we could easily implement the algorithms in J2ME platform.

For encryption System.Security.Cryptography library was used in .Net platform. However on J2ME platform, our implementation of Encryption mechanism on regular mobile phone was through the usage of cryptographic algorithm API provided by Legion of the Bouncy Castle, which supported AES, AES Fast, AES Light, Blowfish, CAST5, CAST6, 3DES,

DES, IDEA, RC2, RC5 32 bits, RC5 64 bits, RC6, Rijndael, Serpent, Skipjack, Towfish block cipher as well as RC4 stream cipher [Yuan, c2004; Filho et al., 2004]. The usage of this API ensures data transfer security from the mobile phone to the medical servers as shown in Fig. 4.8. Although several alternative algorithms are available for both compression and encryption on mobile platform, the choice can be made at the central server, which then notifies the mobile platform about the specific algorithms to be used (Fig. 4.9).

### **Central Sever (CS)**

This is often referred as medical server. The predominant purpose of the central server is to act as a patient data repository. It collects ECG and other physiological data from IP enabled mobile phones carried by a large number of patients that are remotely monitored. Generally, medical servers are distributed in nature. Hence, the doctors and medical practitioners can issue queries to many of these servers. Security among these medical servers can be achieved with modern Virtual Private Networking built using IPsec protocol.

Since both acquisition devices and mobile phones (or Smart phones) have lower processing power, few of the computationally intensive tasks can be delegated to the central servers. For example, number of permutations for 256 ASCII characters is  $256 P 256 = 256!$ . For this tremendous value, processing and selection of a particular permuted set of ASCII value is not feasible on a mobile phone, because of immense computational requirements. Therefore, before transmission of the biosignal, the encoding mechanism may request a pair of permutation keys from the central server for a typical scenario presented in Fig. 4.9. Following the request, the CS sends a pair of permutation keys (for sign and value encoding)

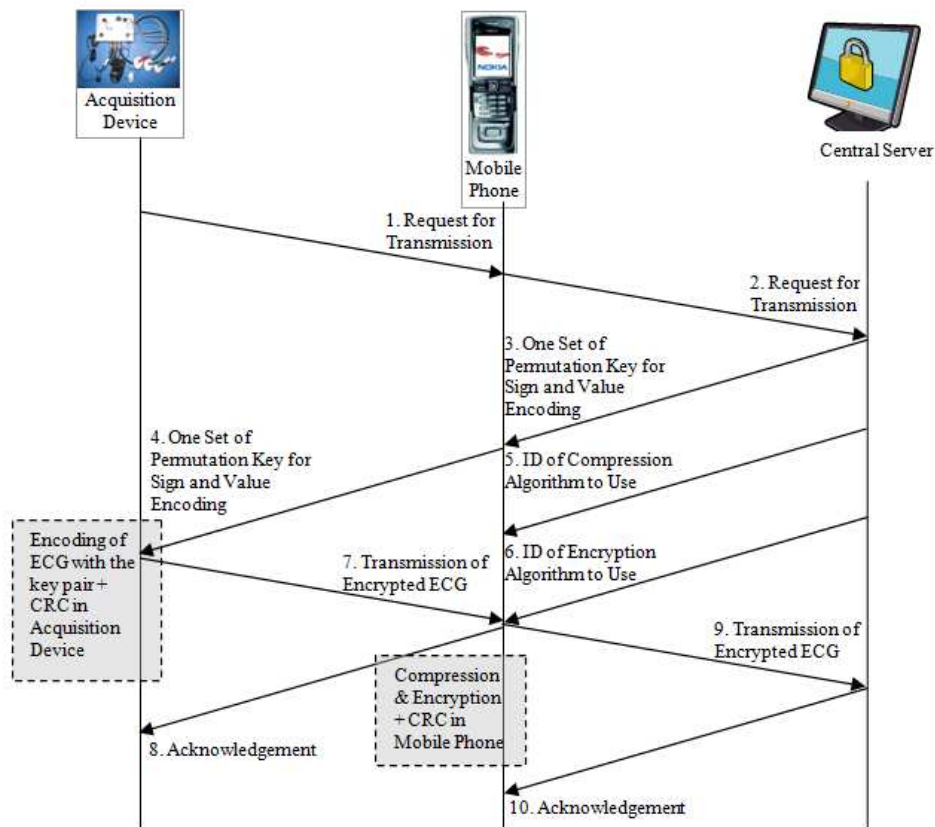


Figure 4.9: Communication Protocol Among Acquisition Device, Mobile Phone and Central Server

(e.g.  $P_s$  and  $P_v$ ) in a secured manner. These permutation keys are then used to perform the encoding with  $p(\cdot)$  primitive. To overcome the delay in obtaining the permutation keys, the mobile phone should receive them from the server (as encrypted message) on regular intervals before the expiry of the existing keys. Therefore, before transmission of the actual ECG signal begins (i.e. initiation of a session), the acquisition device can quickly receive the key pair from the mobile phone without invoking the central server and incurring additional delay.

While sending the permutation keys, the CS can also notify about the specific compression

and encryption methods to be used, since there are many possible schemes. Therefore, during our experimentation phase the CS packed Permutation Keys, Compression and Encryption identifiers and encrypted this piece of information with DES Symmetric algorithm before sending to the mobile phone. As explained already, this encrypted information is only needed to be transmitted before the commencement of actual ECG transmission, which may continue for few hours or even days. The CS randomly selects the existing compression and encryption schemes for the 3 Phase ECE mechanism. As stated earlier in Section 3, this not only enhances the security of ECG data transfer, but also significantly improves transmission time.

#### 4.3.7 Discussion-Security Strength for Joint Encoding, Compression & Encryption

A brute force attack is an exhaustive procedure that tries all possibilities until the right combination is determined. Therefore, the time required to complete the brute force attack primarily depends on the size of the search space,  $\Delta$ , which can be defined as:

$$\Delta = \prod_{f=1}^F \Delta_f \quad (4.14)$$

where  $\Delta_f$  is the factor search space,  $F = 3$  for the encoding mechanism and  $F = 5$  for 3 phase ECG mechanism. For encoding mechanism the value of  $\Delta_1$ ,  $\Delta_2$  and  $\Delta_3$  are 4, 256! and 256! respectively, which are defined in Table 4.5. Apart from the values of  $\Delta_1$ ,  $\Delta_2$  and  $\Delta_3$ , the 3 phase ECE mechanism requires  $\Delta_4 = 4$  and  $\Delta_5 = 18$  to expand its search space.

Therefore, it is evident that for the encoding method, the search space for brute force attack to obtain the source of ECG (for determining C) and right permutation keys (value and sign) is an enormous number  $4 \times 265! \times 256!$ . This enormous number is increases further when the number of possible supported devices ( $\Delta_1$ ) is raised. As  $\Delta$  tends to infinity the probability,  $P(1/\Delta)$  of the retrieving the right combination for deciphering tends to zero.

Only one out of the entire the combinations of  $\Delta$ , result in possible ECG samples (numerical floating points), only one of which constructs the right ECG segment. The only way to discern the right floating point from the wrong ones is to plot at least one segment of ECG comprising of all ECG features (P wave, T wave and QRS complex). Unlike dictionary based brute force attack, there is no automated solution to match ECG morphology in order to ascertain right combination of ECG sample from enormous search space. If in near future, a grid of super computers can compare a trillion trillion trillion ( $10^{36}$ ) combinations of one ECG segment (comprising 500 ECG samples) per second for ECG morphology matching, it will take approximately  $9.333 \times 10^{970}$  years ( $\frac{(4 \times 256! \times 256!)}{(3600 \times 24 \times 365 \times 10^{36})} \approx 9.333 \times 10^{970}$ ) to enumerate all the combinations. On average the correct combination would be found in half of that time. In addition, the 3 phase ECE mechanism conceals the statistical model of the encryption by allowing multiple compressions and encryption algorithms giving  $(4 \times 18) \times 9.333 \times 10^{970}$  years, even without considering the time required to decipher keys for existing encryption mechanisms. In fact, a device that could check a billion billion ( $10^{18}$ ) AES keys per second would require about  $3 \times 10^{51}$  years to exhaust the 256 bit key space. Eventually, at this point, one might question about the necessity of this ridiculous strength of security for ECG data transmission. However, we would like to reinforce the fact that the main strength of



this 3 phase ECE mechanism is inherited from the huge compression ratio (20.06) for ECG data transmission, which guarantees faster transmission of enormous amount of ECG signal.

#### **4.4 Wavelet based Anonymization Technique**

##### **4.4.1 Introduction - Discrete Wavelet based Anonymization**

In this section, we propose a secured ECG signal distribution architecture based on wavelet decomposition of ECG. Wavelet has been used for many years to process biomedical signals. After the wavelet decomposition, the important parts of the coefficients, which represent the P, QRS, T signature of the ECG, are segregated leaving the baseline or isoelectric line. Following this segregation both the parts are compressed. Unimportant part is uploaded to the public repository without encryption, since all the features (of ECG) that represent cardiovascular details have been removed from this part. However, the important coefficients are encrypted and securely distributed among the medical professionals, who need to analyse patient's ECG. Following this procedure, the encrypted important coefficients act a key to reconstruct the original ECG, which can be performed by the authorized personnel, conforming to the HIPAA regulations. According to the best of our knowledge, wavelet decomposition has never been used to protect patient's privacy, especially to encrypt ECG signal. Apart from introducing a new technique, the major contributions of this section are as follows:

- Faster and secured ECG transmission (overall) by the usage of joint compression and encryption mechanism (up to 2.81 compression ratio)
- Unlike the traditional approach, only minimal portion (25%-50%) of the ECG is re-

quired to be distributed (only the important part) to the medical professionals

- Rather than employing computationally expensive encryption algorithm of the whole ECG, only a segment (25%-50%) is selected for encryption
- Instead of traditional doctor centric approach, the overall architecture of the proposed system upholds modern patient centric approach, which guarantees faster diagnosis and treatment

#### **4.4.2 System & Methodology for Discrete Wavelet based Anonymization**

ECG signal has its unique features represented by P wave, QRS complex and T wave. If the ECG signal is represented with a number of coefficient with wavelet decomposition, and a limited set of coefficients is carefully extracted such that the newly constructed trimmed ECG signal from the remaining coefficients becomes featureless, then encryption will be achieved. The selected (important) coefficients, which represent the main features of ECG, are preserved with standard Cryptographic cipher (e.g. RSA Symmetric Cipher). Figure 4.10 demonstrates this process. In wavelet decomposition, filters of different cut-off frequencies are used to analyse the ECG signal at different scales (frequencies). The ECG is passed through a series of high pass filters (detail coefficients) to analyse the high frequencies, and it is passed through a series of low pass filters (approximation coefficients) to analyse the low frequencies. Wavelet decomposition at level 3 was used during our experimentation. Mother wavelet was bior5.5, since it is more suitable for speech, video and biomedical signals providing linear phase. Two individual methods were studied during the experimentation.

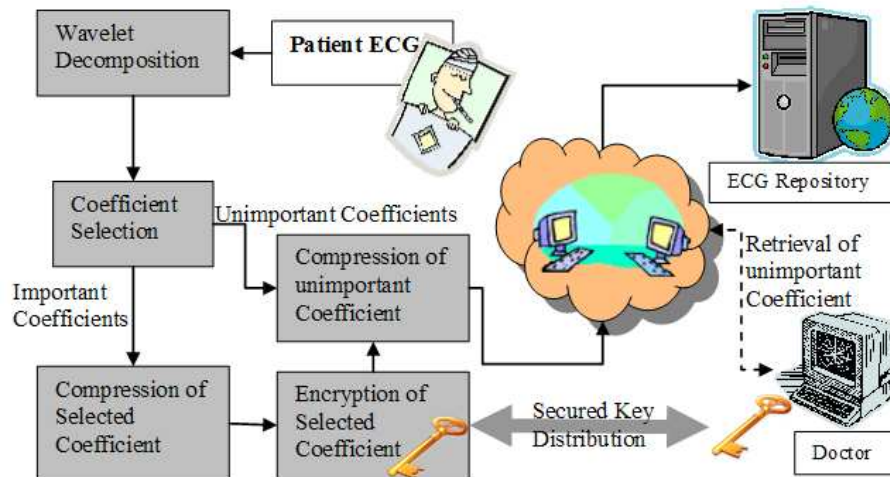


Figure 4.10: Securing ECG with Wavelet Decomposition and Partial Encryption

### Method 1: Discrete Wavelet based Anonymization

At level 3 we removed nodes  $(3, 0)$ ,  $(3, 1)$ . These nodes were encrypted with RSA Symmetric Cryptography. The remaining nodes  $(1, 1)$  and  $(2, 1)$  are compressed and transmitted to the ECG repository. The compression was performed with ZIP compression using IC-SharpCode.SharpZipLib (<http://www.icsharpcode.net>) library on .Net platform. Without the knowledge of nodes  $(3, 0)$  and  $(3, 1)$ , the newly constructed signal completely hides both P wave and T wave of the original ECG (Fig. 4.11).

Therefore, this method hides most of the features required to identify the patient [Biel et al., 2001]. However, this method does not provide complete obfuscation of the cardiovascular conditions, since the RR interval and certain types of arrhythmias are visible [Kusumoto, 2009; Bartolo et al., 2001] as obvious in fig. 4.12. The main strength of this method is the requirement of minimal selection of coefficient (approx. 25%) for encryption and key distribution. Figure 4.12 shows the selected coefficients. Therefore, this method is suitable when

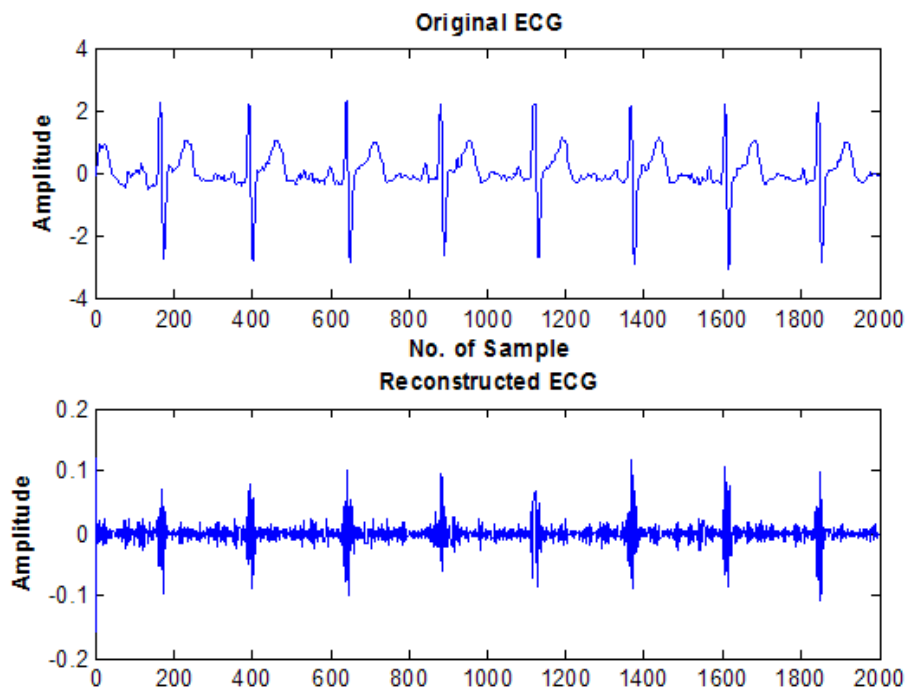


Figure 4.11: Original ECG Signal and Newly Constructed Trimmed ECG Signal with Node  $(3, 0)$  &  $(3, 1)$  Removed

faster distribution of key is priority and strong security is not deemed necessary.

## Method 2: Discrete Wavelet based Anonymization

During this configuration, nodes  $(3, 0)$ ,  $(3, 1)$  and  $(2, 1)$  are selected for encryption. Therefore, the remaining coefficients,  $(1, 1)$  is uploaded to the ECG repository. As seen from Fig. 4.13, the trimmed ECG from the coefficients of the repository completely obfuscates features related to cardiovascular condition and person identification as seen in Fig. 4.13.

This method provides increased security compromising larger key size (Approx. 50%) as in Fig. 4.14. It is clearly seen from Fig. 4.13 that trimmed ECG does not contain any ECG features, encrypting the ECG.

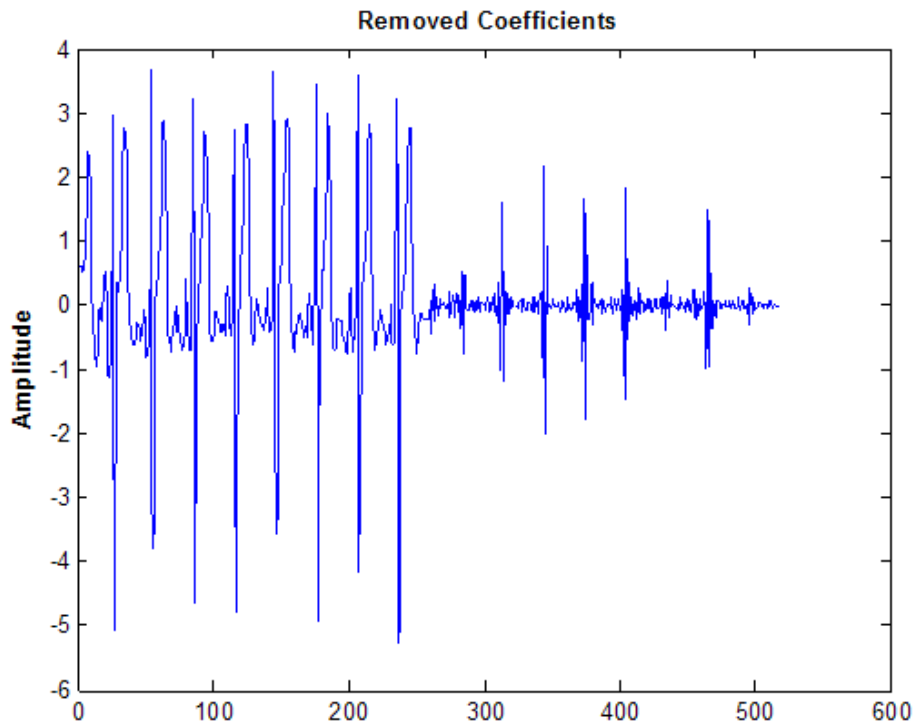


Figure 4.12: Removed (Selected for Encryption) Coefficients for Method 1

#### 4.4.3 Results and Discussion for Discrete Wavelet based Anonymization

The file size of the original ECG depicted in Fig. 4.11 and Fig. 4.13 is 21,150 bytes. In method 1 & 2, the selection of coefficients is different, as described earlier. Table 4.6 shows the overall file reduction during compression and encryption (of the selected coefficients) for both methods. Method 1 & 2 results in compression ratio of 2.75 and 2.81, respectively. Even though, method 2 possesses a higher key size of approximately 50% coefficients, the overall (both encrypted key and compressed public ECG) transmission is faster due to higher compression ratio. Moreover, method 2 provides complete obfuscation of the ECG, when downloaded from the ECG repository, without the key. With the key, the authorized medical professional can recover the original ECG without any loss of information.

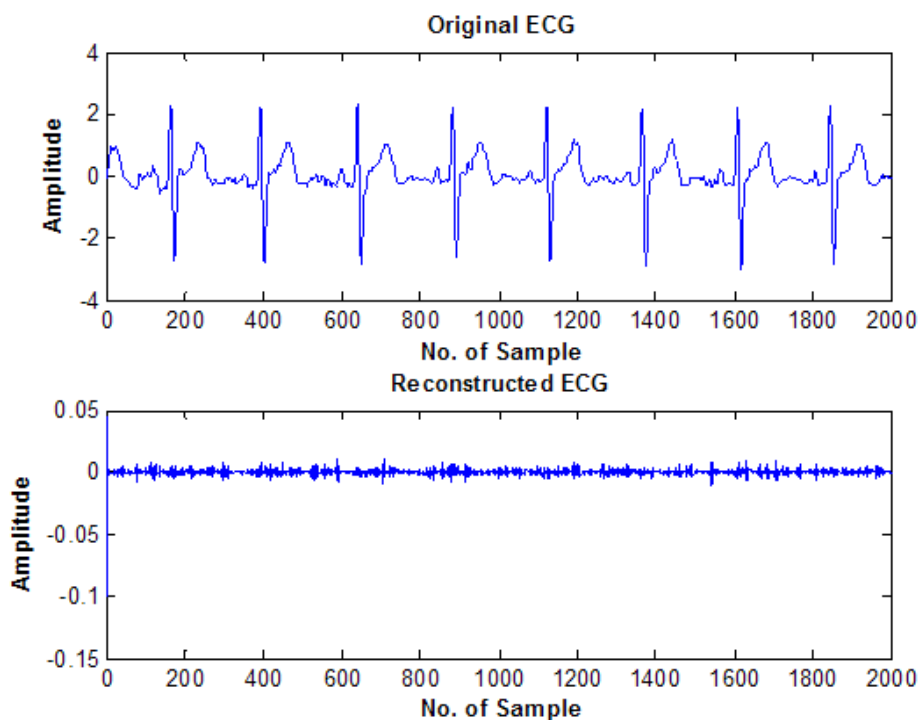


Figure 4.13: Original ECG Signal and Reconstructed ECG Signal with Node  $(3,0)$ ,  $(3,1)$  &  $(2,1)$  Removed

#### 4.4.4 Wavelet Packet based Anonymization

Discrete wavelet based anonymization produces a massive key size, which is about 25% to 50% of the original ECG. Distribution of this larger key entails delay in transmission. Therefore, we further conducted research in ECG anonymization, so that we can reduce the key size.

Then, we proposed an innovative technique for ECG anonymization by utilizing wavelet packet transformation [Sufi et al., 2008e]. First, the original ECG were decomposed to sub band coefficients or nodes from where the first node representing lowest frequency components were replaced with a distorted coefficient. Then, all the coefficients including the distorted coefficient were used to reconstruct (wavelet packet based technique) the anonymized ECG signal. Then, when this anonymized ECG is transmitted over the network, it is neither

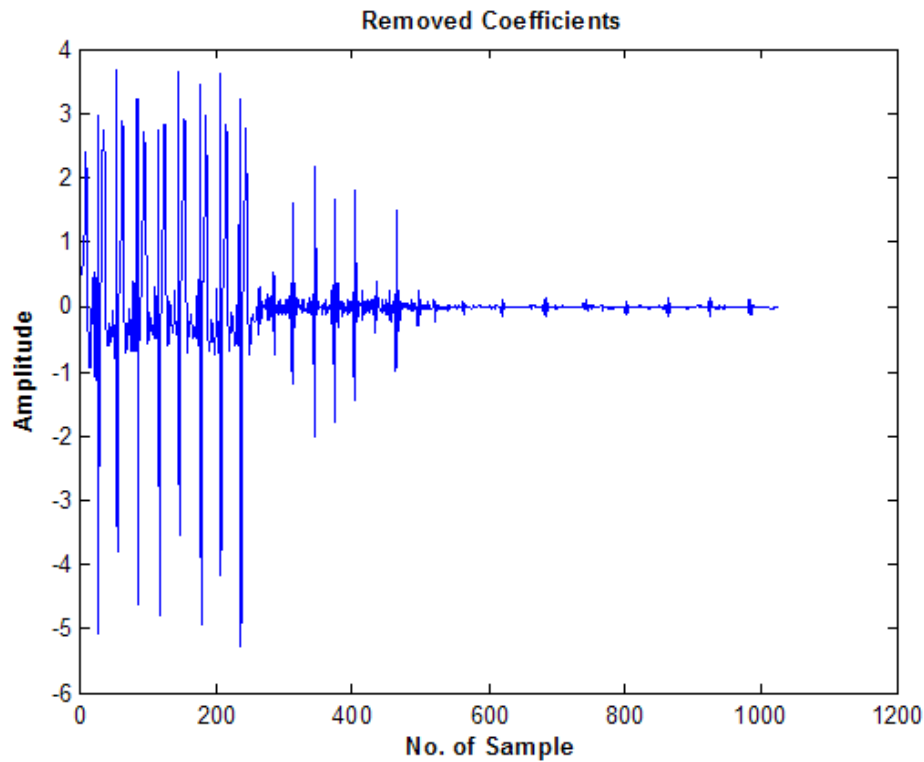


Figure 4.14: Removed (Selected for Encryption) Coefficients for Method 2

vulnerable to major security threat of possible replay attack by the spoofer, nor does it contain details of any cardiovascular conditions (as shown in Fig. 4.15).

The authorized personnel possessing a secret key will be able to reconstruct the original ECG. This key is nothing but the original coefficient (first) representing lower frequency band, which was distorted for the sake of ECG anonymization. Our experiments show that on an average the key is only 12.78% of the original ECG signal, which is small enough for efficient key distribution (transmission) and management (storage). This particular result of lower key size is a substantial improvement of a previous method [Sufi et al., 2008d], where the researchers used discrete wavelet transform that resulted in a key size of at least 25% of the original ECG. Hence, the proposed technique halves the required key size for original

ECG reconstruction. Moreover, the key was compressed and encrypted for further faster and secured transmission and resulted in a lower size of 5.8% on an average, when experiments were carried on 25 subjects. The most important contribution claimed by the proposed technique is all the 25 subjects remained unidentified with current ECG biometric system, providing security against replay attack and health privacy.

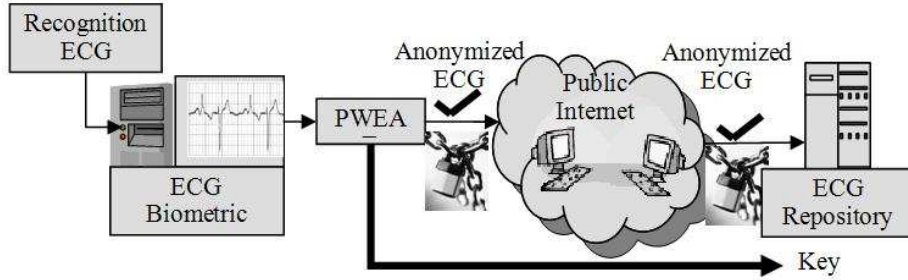


Figure 4.15: Anti Spoofing to Resist Illegal Capture of the Recognition ECG

### System Overview for Wavelet Packet based Anonymization

Wavelet Packet has long been used for ECG analysis. A wavelet packet function [Ogden, 1997] is defined as

$$\varphi_{l,k}^n(t) = 2^{\frac{l}{2}} \varphi^n(2^l t - k) \quad (4.15)$$

where  $l$  and  $k$  are the scale (frequency) and the translation (time) parameter, respectively; and  $n = 0, 1, 3, \dots$  is the oscillation parameter. The structure of wavelet packet (WP) decomposition is described as a binary tree structure  $E$ , each node is described as  $(l, n)$ , where  $l$  is a node's scale level and  $n$  is a node's number on the corresponded level. The root



node  $(0,0)$  of the WP tree corresponds to the entire frequency range of the ECG signal. Each internal node of the WP tree  $(l, n) \in E$  is called a parent node that is divided into two child nodes: the first and the second nodes are associated with low-pass  $h(k)$  and high-pass  $g(k)$  filters, which forms a quadrature mirror filter (QMF) pair [Wickerhauser, 1994].

The scaling function  $\omega(t)$  and the mother wavelet  $\psi(t)$  for the wavelet packet when  $n = 0, 1$  and  $l = k = 0$  are given by

$$\varphi^0(t) = \omega(t), \varphi^1(t) = \psi(t) \quad (4.16)$$

The other wavelet packet functions for  $n = 2, 3, \dots$  and  $l = 1$  are shown as follows

$$\varphi^{2n}(t) = \sum_k h(k) \varphi_{l,k}^n(t) \quad (4.17)$$

$$\varphi^{2n+1}(t) = \sum_k g(k) \varphi_{l,k}^n(t) \quad (4.18)$$

By substituting Eq. 4.15 into Eq. 4.17 and 4.18, we can get

$$\varphi^{2n}(t) = \sqrt{2} \sum_k h(k) \varphi^n(2t - k) \quad (4.19)$$

$$\varphi^{2n+1}(t) = \sqrt{2} \sum_k g(k) \varphi^n(2t - k) \quad (4.20)$$

where, the low pass filter  $h(k) = \frac{1}{\sqrt{2}} \langle \omega(t), \omega(2t - k) \rangle$ , and the high pass filter  $g(k) = \frac{1}{\sqrt{2}} \langle \psi(t), \psi(2t - k) \rangle = (-1)^k h(-k + 1)$ . The operator  $\langle \cdot, \cdot \rangle$  stands for the inner product.

Wavelet packet coefficients of the ECG signal  $x(t)$  is expressed as follows

$$Q_l^n(k) = \langle x, \psi_{l,k}^n \rangle = \int_{-\infty}^{\infty} x(t) \psi_{l,k}^n(t) dt \quad (4.21)$$

Each coefficient measures a specific sub-band frequency content, controlled by the scaling parameter  $l$  and the oscillation parameter  $n$ . The ECG signal  $x(t)$  can be decomposed into different time-frequency space with Eq. 4.20 and Eq. 4.21. By computing the full wavelet packet decomposition on the ECG signal, for the  $l$ th level of decomposition, we have  $2^l$  sets of sub-band coefficients of length  $\frac{N}{2^l}$ , where  $N$  is the ECG signal length [Scholl et al., 1998]. This is how wavelet packet decomposes the original ECG signal into 2 or more coefficients.

For our anonymization of the ECG signal, we performed level 3 wavelet decomposition ( $l = 3$ ). Therefore, the eight ( $2^3$ ) sub-band coefficients (nodes) creates the coefficient set,  $C$  that can be represented as in Eq. 4.22.

$$C = C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6 \cup C_7 \cup C_8 \quad (4.22)$$

Here, node  $C^1$  (and neighbouring coefficients) corresponds to the lowest frequency range,

which is sometimes referred as approximation coefficient. Node  $C^8$  corresponds to the highest frequency ranges, which is on the other hand referred as detail coefficients. Each of these nodes ( $C^1$  to  $C^8$ ) contains the coefficient values. Hence,

$$C_r = x_1^r, x_2^r, x_3^r, \dots, x_{M-1}^r, x_M^r \quad (4.23)$$

where,  $r$  is the number of nodes and highest value of  $r$  is  $2^l$  as stated earlier.  $M$  is the highest number of coefficients in a node, which depends on the number of samples within the ECG file. As seen in Table 3.1, value of  $M$  for subject 1 to 5 were, 196, 220, 193, 172 and 157. We know that ECG signal itself is a low frequency signal. Therefore, distorting the lower frequency component,  $C_1$  (node) will anonymize the whole ECG, when distorted  $C_1$  and the rest of the nodes are used for ECG reconstruction. Distorted  $C_1$  is referred as  $\bar{C}_1$  in the rest of the section. When primitive  $\varphi(\cdot)$  is the function that performs wavelet packet decomposition of level 3 and results in the eight coefficients, this wavelet packet decomposition process at level 3 can be shown as

$$\varphi(y_u) = C \quad (4.24)$$

where,  $y_u$  is the recognition ECG,  $u = 1, 2, 3, \dots, U$  and  $U = \text{length}(y_u)$ . From these coefficients, the original signal  $y_u$  can be reconstructed back by the wavelet packet reconstruction function,  $\varsigma(\cdot)$ .

$$\varsigma(C) = y_u \quad (4.25)$$

For the sake of simplicity and faster transmission with lower node size,  $C_1$  was distorted using Eq. 4.26. Equation 4.26 basically shows that all the coefficients within node  $C_1$  were replaced with zero.

$$\forall x \in C_1 : x_m^1 = 0 \quad (4.26)$$

where,  $1 \leq m \leq M$ . The corrupted coefficient set was acquired by Eq. 4.27.

$$\bar{C} = \bar{C}_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6 \cup C_7 \cup C_8 \quad (4.27)$$

Finally, ECG was anonymized with Eq. 4.28.

$$\kappa = O(\Delta(C_1)) \quad (4.28)$$

where,  $z_u$  is the anonymized ECG. The key is generated, by joint compression and encryption of node  $C_1$ . Joint compression and encryption mechanism has been explained in details, earlier in this Chapter. With the compression and encryption primitives represented by  $\Delta(\cdot)$  and  $O(\cdot)$ , the key,  $\kappa$  is generated as in Eq. 4.29.

$$\varsigma(\bar{C}) = z_u \quad (4.29)$$

This anonymized ECG signal appears totally dissimilar from the original ECG. The anonymized ECG can then be confidently transmitted over the public internet, since the anonymized ECG does not impose any threat over privacy. The separated node  $C_1$  is used as a key, without

which reconstruction of the original ECG from the anonymized ECG is impossible.

The authorized person, receives the key,  $\kappa$  and the anonymized ECG,  $z_u$ . When decryption and decompression is represented by functions  $\Theta(\cdot)$  and  $\Lambda(\cdot)$ , the lowest frequency coefficient  $C_1$  can be retrieved back with Eq. 4.30.

$$C_1 = \Lambda(\Theta(\kappa)) \quad (4.30)$$

Once, the original  $C_1$  is retrieved by the authorized user, he performs wavelet packet decomposition (Eq. 4.31) on the anonymized ECG,  $z_u$ . Thus,  $\bar{C}$  is obtained as follows:

$$\varphi(z_u) = \bar{C} \quad (4.31)$$

After, the retrieval of  $\bar{C}$ , the authorized personnel segregates the  $\bar{C}_1$  and replaces it with original  $C_1$ . Finally Eq. 4.25 is used to retrieve the original recognition ECG  $y_u$ .

### Implementation of Wavelet Packet based Anonymization

Figures 4.16 and Fig. 4.17 show our implementation of ECG anonymization by the sender and the ECG reconstruction by the authorized receiver respectively. The recognition ECGs for all the 30 subjects were used for decomposition of wavelet coefficients. Figure 4.18 shows the coefficients corresponding to subject one's ECG. The approximation coefficient (3,0) was removed (as seen in Fig. 4.16) and a set of keys for all the 65 subjects were generated. Then, distorted (3,0) was created by substituting all the low frequency coefficients with zeros. The distorted (3,0) is then positioned in the same location where the original (3,0) was previ-

ously located before segregation. Finally, all the coefficients along with distorted (3,0) were used for wavelet packet based signal reconstruction routine to achieve ECG anonymization. The anonymized ECGs for all the subjects appeared to be totally dissimilar from the original ECGs. Figure 4.19 shows the anonymized ECG signals for the first five subjects. To measure whether this dissimilarity is enough for keeping the subjects unidentified, those anonymized ECGs were fed to our ECG biometric system (as described in Section 4) for identification purposes. For all the cases, the subjects remained unidentified upholding the privacy requirement. Therefore, the wavelet packet based anonymization achieved 100% success for making all the subjects' unidentified protecting privacy of patients.

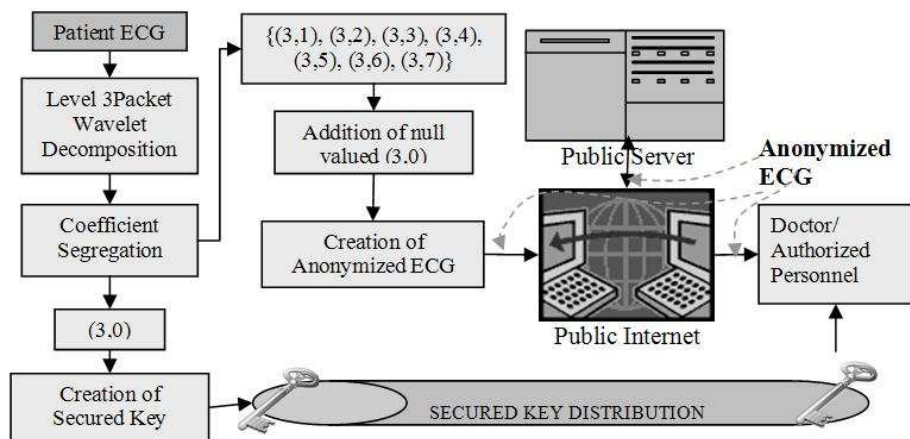


Figure 4.16: The Proposed Wavelet Packet based ECG Anonymization Mechanism

### Results for Wavelet Packet based Anonymization

The PRDs for all the 25 cases ranged from 21.987 to 46.592 with an average of 31.562. CC ranged from -0.012 to 0.0462 with an average of 0.009. For all the cases WDM values between 25 and 98.715 with an average of 87.315. Table 3.1 shows the result for the first five

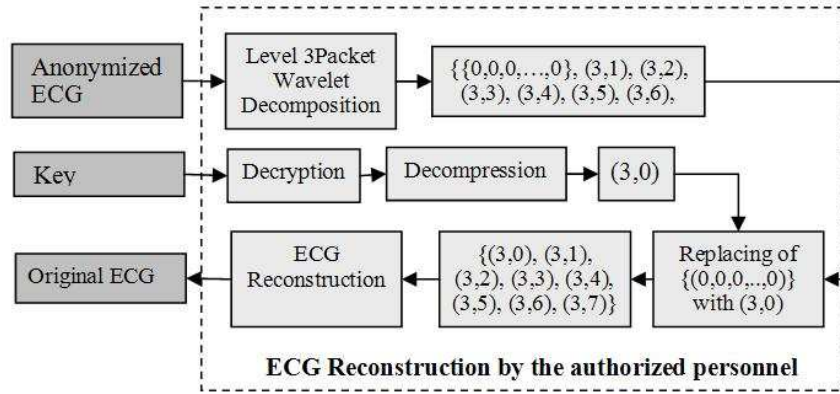


Figure 4.17: The Wavelet Packet Based ECG Reconstruction Mechanism Performed by Authorized Personnel

subjects. From the results, it becomes apparent that our previous empirical calculations of the thresholds for PRD, CC and WDM for successful identification were effective.

The size of the selected coefficient is only 12.78% of the original ECG signal without any compression and encryption. This is a substantial improvement compared to our previous research outcome on discrete wavelet based ECG obfuscation [Sufi et al., 2008d]. The previous method required at least 25% of whole ECG to be selected to achieve minimal level of obfuscation [Sufi et al., 2008d]. Therefore, the proposed ECG anonymization approach nearly halved the selected coefficient size for ECG anonymization. This substantial improvement results in faster distribution of the secured key.

It is evident from Table 4.7 that the key (node (3,0)) sizes gets reduced after the compression and encryption before secured distribution over the media. This particular ordering of compression followed by encryption was obtained by the promising results of our previous studies in [Sufi and Khalil, 2008b]. The overall compression ratio achieved after joint compression & encryption technique on the keys was 2.373 on an average.

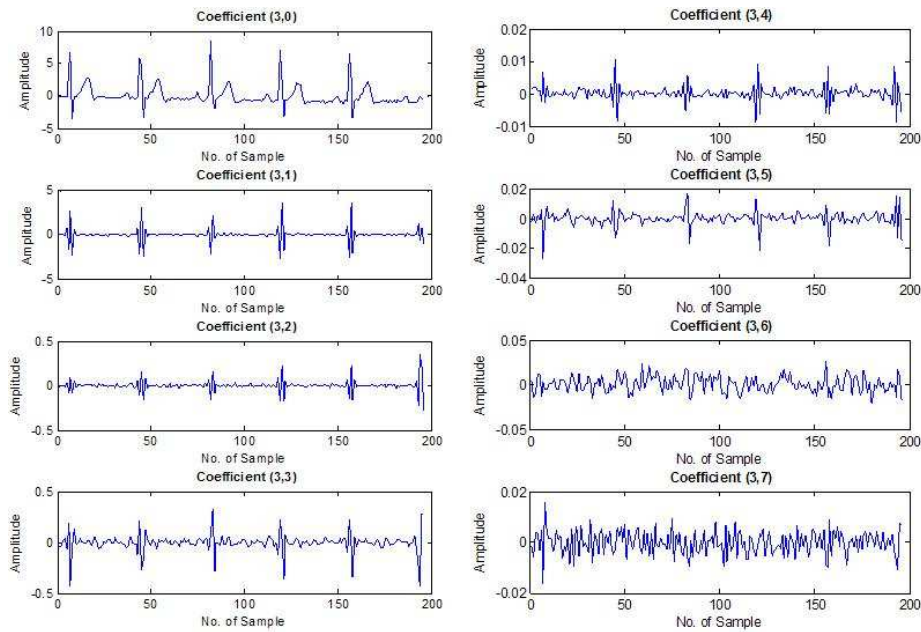


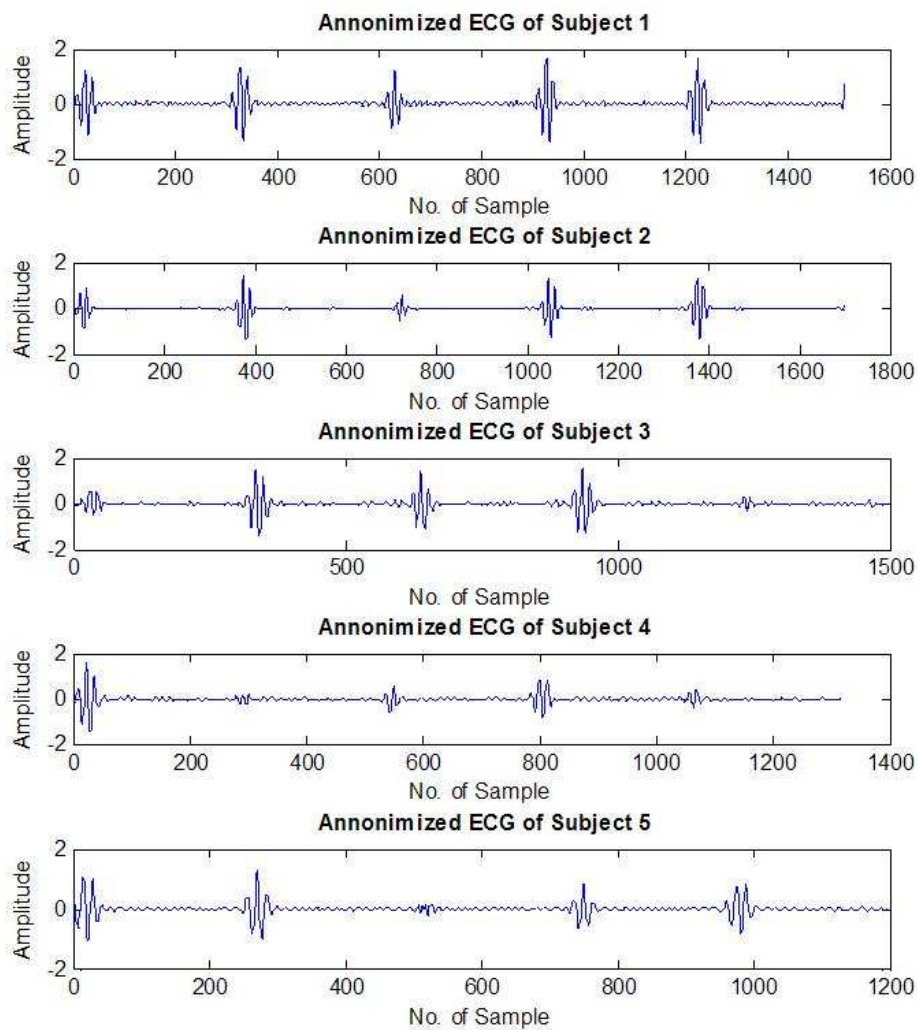
Figure 4.18: Wavelet Coefficients for Subject 1

On an average, the key is only 5.8 % of the recognition ECG size  $y_u$ , after performing compression and encryption of the key. Therefore, only a small portion of the recognition ECG needs secured transmission. Anonymized ECG does not require further encryption before transmission, since anonymization serves the purpose of encryption. However, compression on the anonymized ECG data will ensure faster data transmission.

#### 4.5 ECG Obfuscation with Noise

Wavelet packet based ECG anonymization produces a moderate key size (i.e. 5.8% of the original ECG). However, in Holter Monitoring scenario, ECG file size could be in Gigabyte range. A more efficient method that reduces the key size even further needs to be investigated. In addition, our previous methods of ECG encryptions / anonymizations represent the ECG in encrypted format, alluring the hackers in decrypting the encoded ECG. A new





*Figure 4.19: Anonimized ECG for the First Subjects*

anonymization technique that keeps the ECG packets appear to be original ECG while hiding the cardiovascular details and biometric features, is highly desired.

To achieve this, first of all, in this section, we present a new ECG feature detection mechanism, which was compared against existing cross correlation (CC) based template matching algorithms. Two types of CC methods were used for comparison. Compared to the CC based approaches, which had 40% and 53% misclassification rates, the proposed detection

algorithm did not perform any single misclassification. Secondly, a new ECG obfuscation method was designed and implemented on 25 subjects using added noises corresponding to each of the ECG features. This obfuscated ECG can be freely distributed over the internet without the necessity of encryption, since the original features needed to identify personal information of the patient remain concealed. Only authorized personnel possessing a secret key will be able to reconstruct the original ECG from the obfuscated ECG. Distribution of the key is extremely efficient and fast due to small size (only 0.04%-0.09% of the original ECG file). Moreover, if the obfuscated ECG reaches to the wrong hand (hacker), it would appear as regular ECG without encryption. Therefore, traditional decryption techniques including powerful brute force attack are useless against this obfuscation.

According to the literature, there are several methods of pattern matching algorithm that can be used for person identification. Cross correlation (CC) is a technique used in statistics to match the similarity of two vectors or signals [Last et al., 2004; Ifeachor and Jervis, 1993]. Different varieties of CC approaches have been successfully employed for template matching of the ECG signal [Last et al., 2004; Abboud and Sadeh, 1984; Govrin et al., 1985]. As reported by previous literatures, [Govrin et al., 1985] utilized both P and QRS template to locate successive P waves and QRS complexes for all cardiac cycles during their experimentation. More recently, [Last et al., 2004] utilized all ECG signature templates (P wave, QRS Complex and T wave) to perform multi-component CC approach to identify all three components from 3000 cardiac cycles or beats. We employed CC using both Eq. 4.32 and Eq. 4.33 as they were utilized by previous studies [Abboud and Sadeh, 1984; Govrin et al., 1985; Last et al., 2004; Ifeachor and Jervis, 1993], for the detection of P wave, QRS

complex and T wave. Moreover, a new pattern matching algorithm is proposed in this section for obfuscation of the ECG.

ECG obfuscation can be performed by the usage of existing encryption algorithms [Kartalopoulos, 2006]. Even though modern symmetric and asymmetric encryption algorithms are claimed and challenged to be unbreakable time to time, they are being broken by different groups [Kartalopoulos, 2006]. The encryption algorithm turns the plain text into redundancy free code words. Therefore, almost all of existing encrypted data appear as meaningless chunk of characters. Encrypted or encoded cipher texts allure expert hackers to employ powerful brute force attacks for decryption of the encoded text. However, if the encrypted text appears to be ordinary plain text, the hacker would think it to be unencrypted text and eventually he will not be tempted to decrypt the encoded text. Previous work in ECG encryption employed partial encryption to the ECG file [Miaou et al., 2002], which generates cipher text to attract hacker's attention. Also, more recent efforts of turning ECG text to chaotic representation will generate doubt among expert hackers [Lin and Chung, 2007]. Moreover, application of this method generates added error within the recovered ECG [Lin and Chung, 2007].

The proposed obfuscation method produces output signal (obfuscated ECG), which appears as regular ECG comprising typical feature waves like P waves, QRS complexes and T waves. Since the proposed ECG obfuscation deceives the hacker by pretending to be original ECG, the whole range of hacker's utilities become useless against the proposed method. Most importantly, the reconstructed signal is exactly same as the original ECG unlike the existing ECG scrambler [Lin and Chung, 2007].

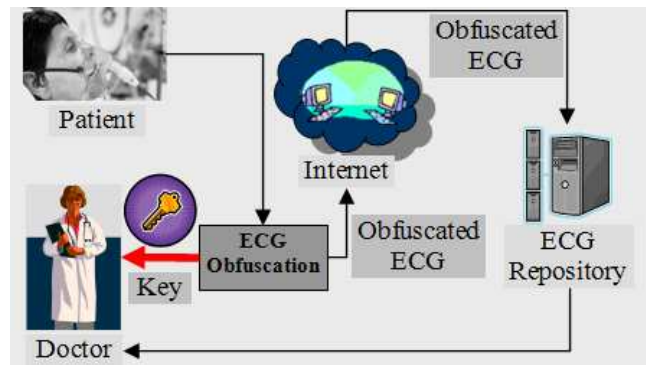


Figure 4.20: Key and Obfuscated ECG Distribution

#### 4.5.1 System & Method of ECG Obfuscation with Noise

The proposed ECG obfuscation model detects all three features, namely P wave, QRS complex and T wave from the ECG and replaces them with noised features. Therefore, to the unauthorized person, this noised ECG (obfuscated ECG) signal will appear as normal ECG signal, but certainly it will not disclose any person identification or cardiovascular details. The noised ECG preserves the original ECG hidden within it. Only authorized personnel (e.g., medical personnel, heart specialist etc.) are distributed with a key, using which the original ECG can be reconstructed (from the noised ECG). During the reconstruction of ECG from noised ECG (obfuscated), noised features are detected followed by noise deduction from the noised features. Thus, original ECG signal is reconstructed. Figure 4.21 demonstrates the simplified block diagram of ECG obfuscation and reconstruction process. As it is evident from Fig. 4.21, detection plays a major role before the actual process of obfuscation and reconstruction. Therefore, selection of an accurate feature detection algorithm (regular feature detection from ECG signal and noised feature detection from obfuscated ECG) is core to this research.

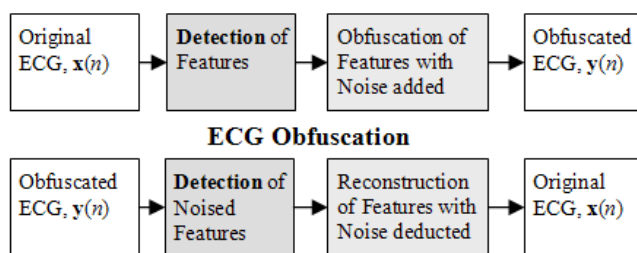


Figure 4.21: Block Diagram of ECG Obfuscation & Reconstruction Process

### Selection of Optimal Feature Detection Algorithm

Previous studies have successfully used CC method to detect ECG features [Abboud and Sadeh, 1984; Govrin et al., 1985; Last et al., 2004; Ifeachor and Jervis, 1993]. For this research we evaluated two types of CC approaches for the detection of P waves, QRS complexes and T waves from the input ECG,  $x(n)$ . Then, we introduced our own algorithm for the same purpose of detection of ECG features. All three methods of template matching based ECG feature detection were tested against ECG samples from 25 subjects captured with the acquisition device developed by Biopac Systems Inc. ([www.biopac.com](http://www.biopac.com)). The possibility of variation in heart rate increases with longer acquisition time for the patients. If the change in heart rate is drastic during a single ECG session, then the templates that were chosen at the beginning of the session might provide poor detection at the end of the session.

Therefore, 10 minutes acquisition time was optimally appointed for each of the subject to evade wider variation in heart rates during the experimentation session. Moreover, the subjects were allowed to take 15 minutes rest before the start of the ECG session. Thus, steadier heart rate was assured. Lead II configuration and 360 Hz sampling frequency was set for all the acquisitions. The acquisition was performed under resting condition for all the sessions to avoid the possibility of baseline drifts and noises, since these might impede

against good CC results. The three template matching algorithms are described as follows:

1) *Cross Correlation Method 1:*

We used Eq. 4.32 to obtain the similarity between the subset of original ECG and the template (P template, QRS template and T template). The highest values of CC vector,  $r_{cc}$  reveal possible locations of a feature.

$$r_{cc}(j) = \frac{1}{M} \sum_{m=1}^M x(m+j) \times f(m) \quad (4.32)$$

where,  $m = 1, 2, 3, \dots, M$  and  $M$  is the length of feature template  $f(n)$ . By sliding the feature template with respect to the ECG  $x(n)$ , vector  $r(j)$  is created as in Eq. 4.33. During this sliding process only the value of  $j$  is incremented and therefore,  $j = 1, 2, 3, \dots, (N - M)$

$$r_{cc}(j) = r(1), r(2), r(3), \dots, r(N - M) \quad (4.33)$$

This procedure was followed for the detection of P wave, QRS complex and T wave. To detect P wave, QRS complex and T wave from the original ECG, P templates, QRS templates and T templates are used respectively. During the P wave classification, this method misclassified both T waves and QRS complexes apart from successfully identifying P waves. Therefore, the total misclassification rate was found to be 40% for this method. Figure 4.22, shows a subset of original ECG signal for subject 3. Figure 4.23 shows the templates for P wave, QRS complex and T wave. These templates were basically chosen from the

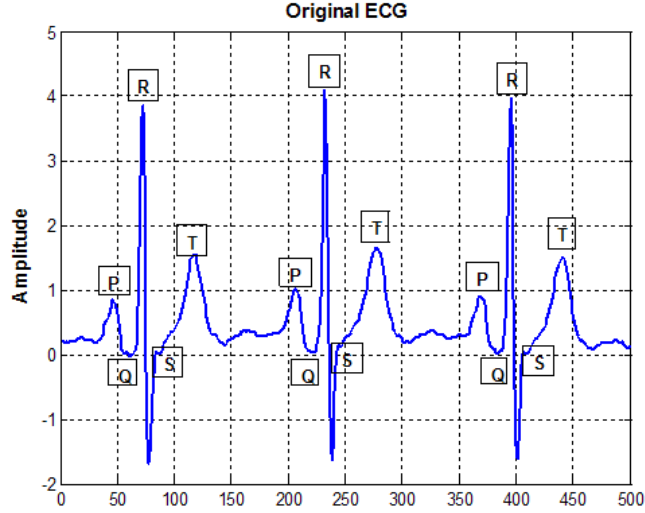


Figure 4.22: Original ECG Signal

first occurrences of corresponding features from Fig. 4.21. Finally, Fig. 4.24 (a) plots the  $r_{cc}$  showing 9 positively classified P features, out of which only 3 are correct. However, this method successfully detected all the QRS complexes and T waves as seen in Fig. 4.24 (b) and Fig. 4.24 (c) without misclassifications. Because of lower accuracy arising from misclassified P waves, this method was not selected for the proposed ECG obfuscation method.

*Cross Correlation Method 2:* In this method, we used Eq. 4.34 to calculate the CC vector,  $r_{mcc}$  to detect P wave, QRS complex and T wave. This equation was formerly used by previous research [Last et al., 2004] in multi-component based CC for detection of P, QRS and T. During our experimentation the misclassification rate observed for this method was 54%, which is even greater than that of CC method 1 (Fig. 4.25).

$$r_{mcc}(j) = \frac{\sum_{m=1}^M [x(m+j) - \bar{x}] \times [f(m) - \bar{f}]}{\sqrt{\sum_{m=1}^M [x(m+j) - \bar{x}]^2 [f(m) - \bar{f}]^2}} \quad (4.34)$$

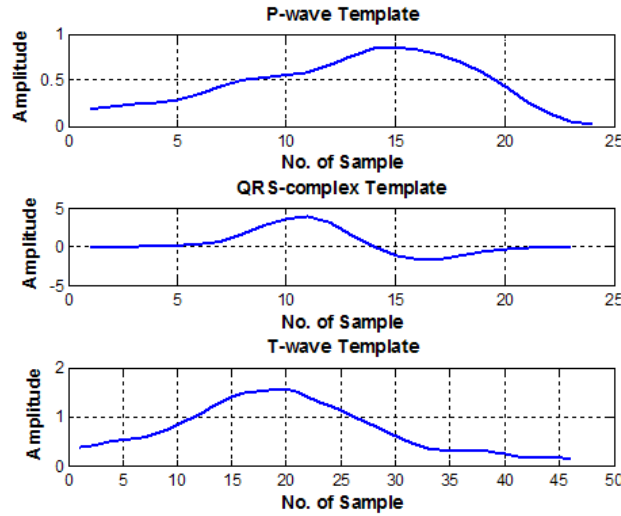


Figure 4.23: Feature Template to be used for Feature Extraction

Figure 4.25 (a) shows that out of 8 candidates of possible P onset only 3 were true. Figure 4.25 (b) shows all 3 candidates for QRS complex were misclassified. However, Fig. 4.25 (c) correctly detected the three T waves. The Proposed Feature Detection Method Because of high misclassification rates for both CC method 1 and method 2, a better method of ECG feature detection was sought. Percent of Root-Mean-square Difference (PRD) is widely used to measure the quality of reconstructed ECG after lossy ECG compression [Zigel et al., 2000b].

Basically, PRD provides a measurement of dissimilarity between two signals as in Eq. 4.35. Therefore, to obtain the similarity between two waves Eq. 4.36 can be utilized. The vector,  $r_s$  provides the highest percentage value (over 92%) when the template wave is matched within the original ECG as seen in Fig. 4.26.

The proposed similarity matching technique, using Eq. 4.36, which was inspired by the PRD measurement, did not incur any single misclassification. Therefore, this new technique



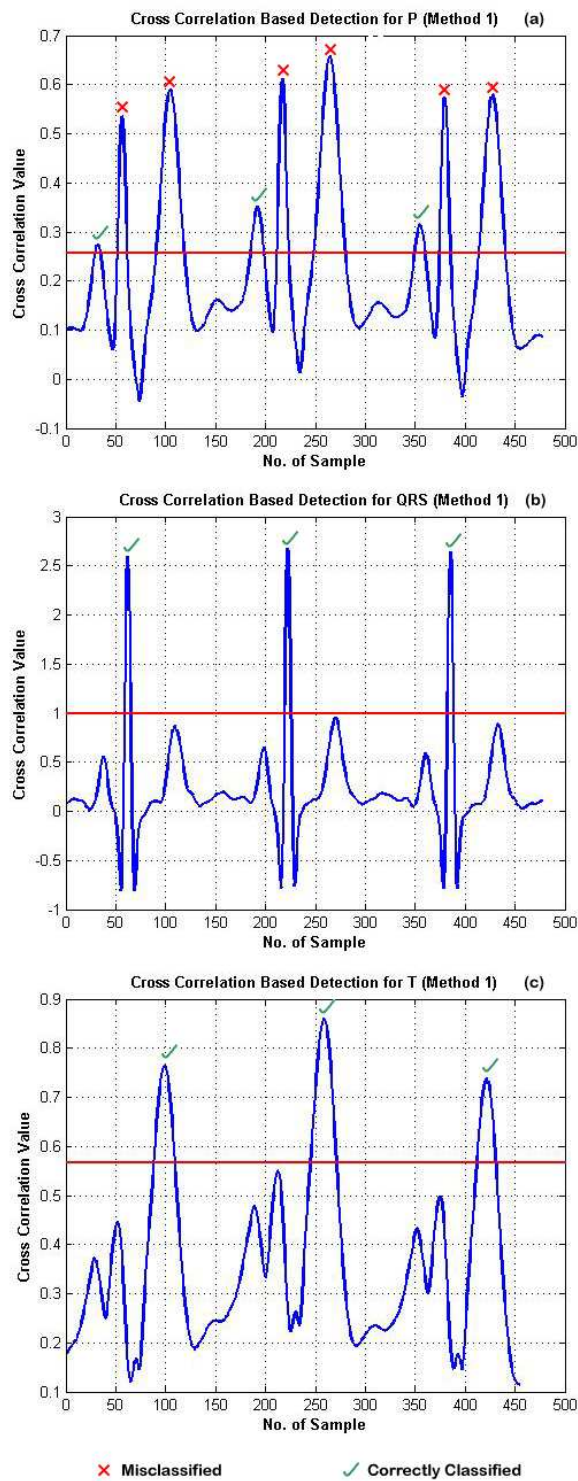


Figure 4.24: Measurement of Cross Correlation ( $r_{cc}$ ) for Detection of P wave, QRS Complex and T Wave using CC Method 1

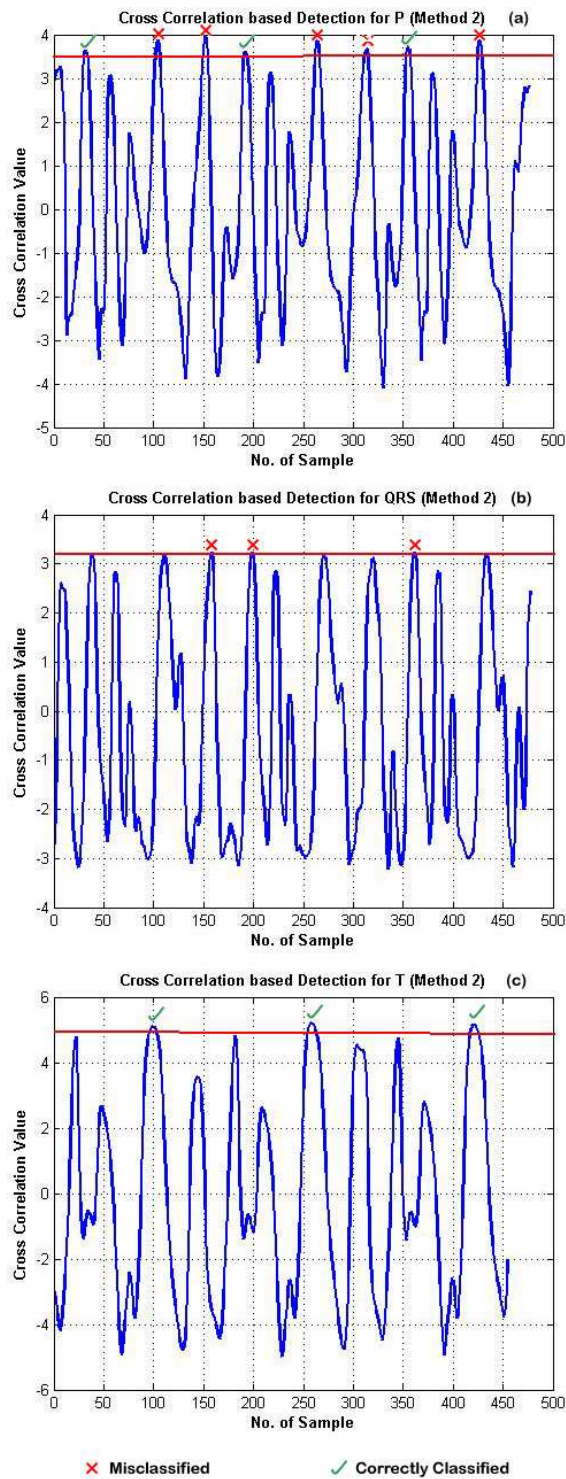


Figure 4.25: Measurement of Cross Correlation ( $r_{cc}$ ) for Detection of P wave, QRS Complex and T Wave using CC Method2

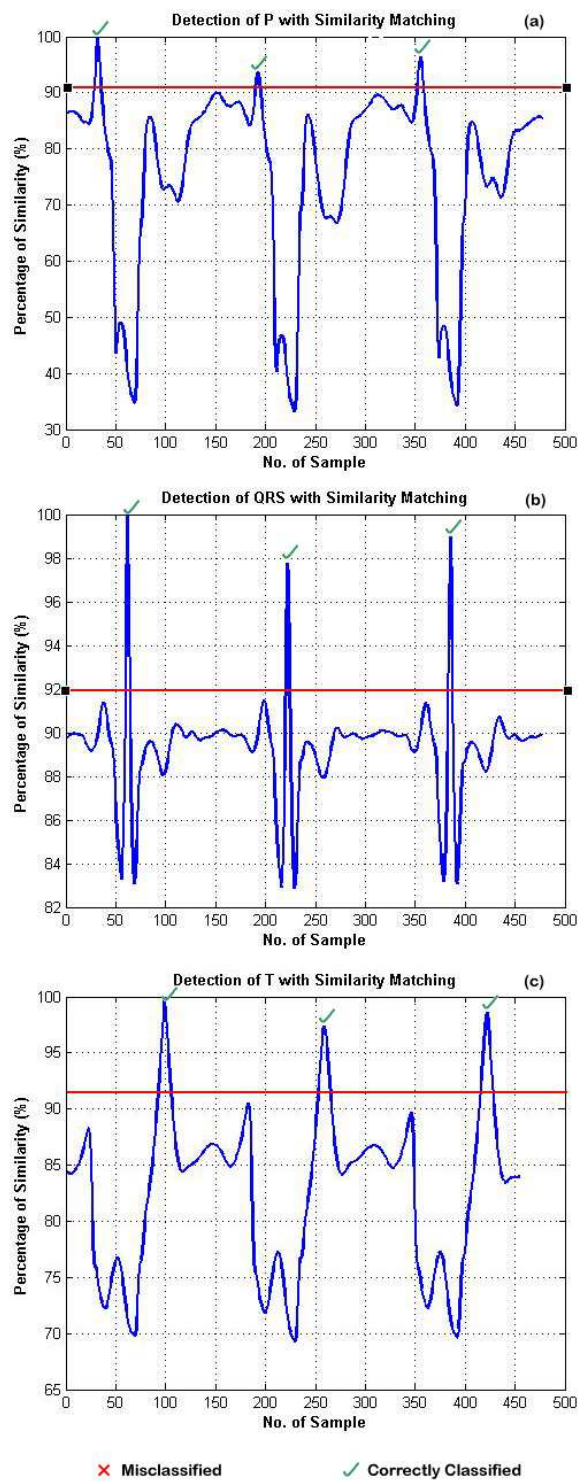


Figure 4.26: Detection of P wave, QRS Complex and T wave with Percentage of Similarity

was found to be more suitable whenever higher detection accuracy is of paramount importance and finally this method was used for the noised based obfuscation and reconstruction procedure.

$$PRD = \sqrt{\frac{\sum_{m=1}^M [x(m+j) - f(m)]^2}{\sum_{m=1}^M [x(m+j) - \bar{x}]^2}} \times 100 \quad (4.35)$$

$$r_s(j) = (1 - \sqrt{\frac{\sum_{m=1}^M [x(m+j) - f(m)]^2}{\sum_{m=1}^M [x(m+j) - \bar{x}]^2}}) \times 100 \quad (4.36)$$

$$r_s(j) = 100 - PRD(j) \quad (4.37)$$

The Detection Function,  $\Lambda(x(n), f(m))$  detects the onset and offset of particular feature waves from ECG ( $x(n)$ ) by sliding the Eq. 4.36 and performing template matching with the particular features,  $f(m)$ . This detection function receives two parameters: the original signal  $x(n)$  (from where the features are needed to be detected) and the feature template, where,  $1 = m = M$  and  $M = length(f(m))$ . In short,  $\Lambda(\cdot)$  is utilized to reveal any of the features (similar pattern like  $f(m)$ ) of  $x(n)$  by template matching with  $f(m)$ . The mathematical symbols are further defined in Table 4.8.

### 4.5.2 Key used in ECG Obfuscation & Reconstruction

Both the patients and the doctor share the same key,  $K$  for obfuscation and reconstruction. The key contains the feature template  $\Gamma$  and noise template  $C$ . Feature template,  $\Gamma$  contains three templates for P wave, QRS complex and T wave. Therefore,

$$\Gamma = \Gamma_P(o) \cup \Gamma_{QRS}(l) \cup \Gamma_T(v) \quad (4.38)$$

The noise template contains individual noises for P wave, QRS complex and T wave. Hence,

$$C = C_P(o) \cup C_{QRS}(l) \cup C_T(v) \quad (4.39)$$

Thus, the key,

$$K = \Gamma \cup C \quad (4.40)$$

Figure 4.27 depicts the key composition, which is central to the proposed ECG obfuscation and reconstruction process. Therefore, the templates and the noises are carefully selected. The selection of the templates can be performed during the training phase as in earlier research [Last et al., 2004]. Noises pertaining to each of the features (P wave, QRS complex

and T wave) can be represented by either of the followings:

- As a signal vector (e.g.  $q = 6, 7.5, 3.9, 8.1, 2.3, \dots$ )
- As an equation (e.g.  $q(x) = e^{4.5 \times x}$ )

However, in both the cases there are trillions of possible noise permutations, making the proposed ECG obfuscation process highly secured. Unlike the obfuscated ECG, the key requires secured distribution to the authorized personnel, who are allowed to view the ECG. Key distribution techniques for this obfuscation method are out of the scope for this section, since it is separate research by itself [Lee and Lee, 2008].

### 4.5.3 ECG Obfuscation Process

The obfuscation method is a two-step process where individual feature of the ECG (P waves, QRS complexes and T waves) are detected followed by the addition of different noises to those detected features (Fig. 4.21). Obfuscation is performed by obfuscation function, which takes the original ECG signal  $x(n)$  and produces the obfuscated ECG signal  $y(n)$  using key  $K$ . Figure 4.28 details the ECG obfuscation process.

**Step 1-Feature Detection:** Detection function,  $\Lambda(x(n), \Gamma)$  detects all the features,  $F$  from  $x(n)$  using feature templates,  $\Gamma$ . Therefore, the feature set contains all the P waves, QRS complexes and T waves from the original ECG.

This feature revelation process can be shows as follows:

$$F = P \cup QRS \cup T \quad (4.41)$$

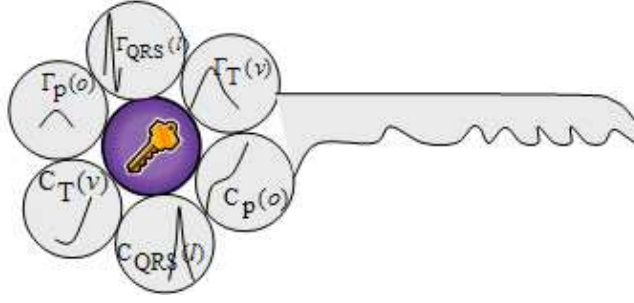


Figure 4.27: Key Composition for ECG obfuscation & Reconstruction

$$\Lambda(.) : x(1), x(2), \dots, x(n) \longrightarrow x(1), x(2), \dots, P_1(o), \dots, QRS_1(l), \dots, T_1(v), \dots, P_2(o), \dots, x(N)$$

**Step 2-Noise Addition:** After the features are detected from the original raw ECG data, various types of relevant noises are added on the detected features for feature obfuscation as follows:

$$\forall P, \hat{P}_u(o) = P_u(o) + C_P(o) \quad (4.42)$$

$$\forall QRS, \hat{QRS}_w(l) = QRS_w(l) + C_{QRS}(l) \quad (4.43)$$

$$\forall T, \hat{T}_z(v) = T_z(v) + C_T(v) \quad (4.44)$$

An example of this noise addition is presented in Eq. 4.45, which shows how individual

noises are added to corresponding features.

$$y(n) = x(1), x(2), \dots, (P_1(o) + C_P(o)), \dots, (QRS_1(l) + C_{QRS}(l)), \dots, x(N) \quad (4.45)$$

Or,

$$y(n) = y(1), y(2), y(3), \dots, \hat{P}_1(o), \dots, Q\hat{R}S_1(l), \dots, \hat{T}_1(v), \dots, \hat{P}_2(o), \dots, y(N) \quad (4.46)$$

Following conditions should be noted during this observation:

An example of this noise addition is presented in Eq. 4.45, which shows how individual noises are added to corresponding features.

$$y(n) = x(n) \text{ where } x(n) \in \bar{F} \quad (4.47)$$

$$y(n) = x(n) + \xi \text{ where } x(n) \in \bar{F} \quad (4.48)$$

where,  $\xi$  is the feature specific noise for that particular ECG sample point  $x(n)$ . Equation 4.47 and 4.48 basically mean that noises are only added to the features (not to the featureless portion).



#### 4.5.4 ECG Reconstruction Process

During the Reconstruction process obfuscated or noised features are detected from the obfuscated ECG, followed by the noise deduction from those detected noised features (Fig. 4.20). This process involves the usage of reconstruction function,  $\Xi = (y(n), K)$  which reconstructs the original ECG  $x(n)$  from the noised signal  $y(n)$  using the key,  $K$ . Figure 4.29 shows the details of ECG reconstruction method. Table 4.9 contains the mathematical symbol definitions for ECG reconstruction.

**Step 1-Noised Feature Detection:** The detection function,  $\Lambda(y(n), \hat{\Gamma})$  detects all the noised features,  $\hat{F}$  from  $y(n)$  using the corrupted template,  $\hat{\Gamma}$ .

$$\hat{F} = \hat{P} \cup Q\hat{R}S \cup \hat{T} \quad (4.49)$$

$$\hat{\Gamma} = \hat{\Gamma}_P(o) \cup \hat{\Gamma}_{QRS}(l) \cup \Gamma_T(v) \quad (4.50)$$

These noised templates for P wave, QRS complex and T wave can be obtained by adding noises to the corresponding templates as in Eq. 4.51 - 4.53:

$$\hat{\Gamma}_P(o) = \Gamma_P(o) + C_P(o) \quad (4.51)$$

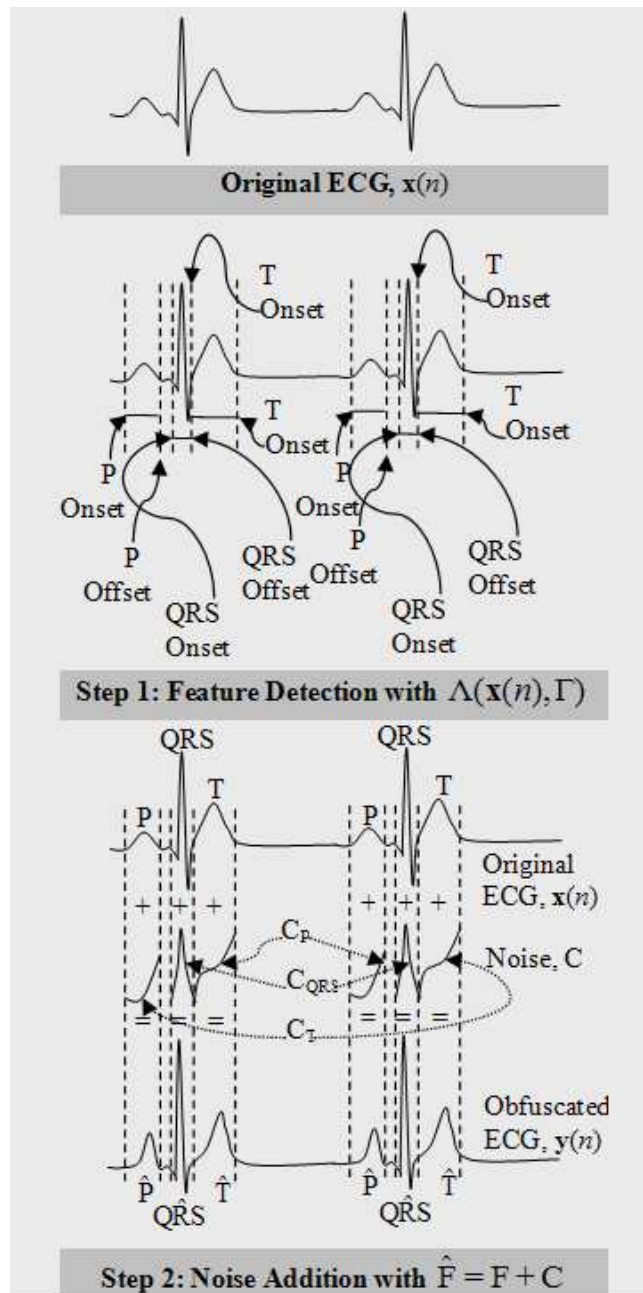


Figure 4.28: Details of Obfuscating ECG

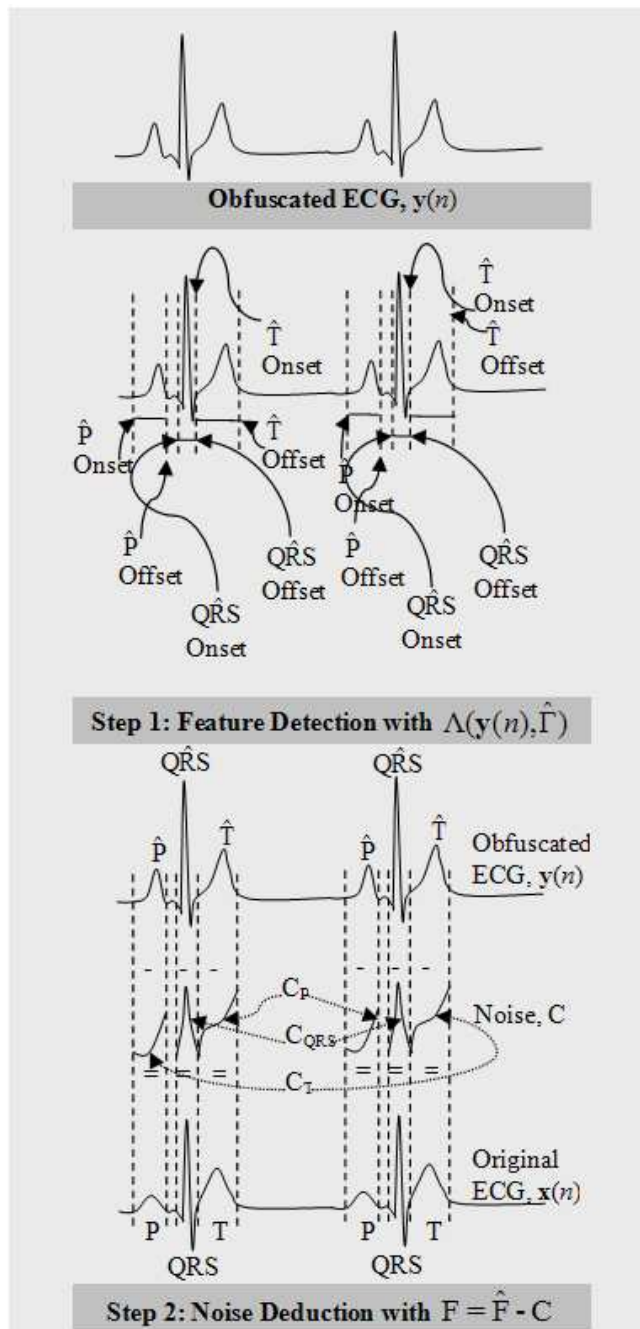


Figure 4.29: Details of Reconstructing ECG

$$\hat{\Gamma}_{QRS}(l) = \Gamma_{QRS}(l) + C_{QRS}(l) \quad (4.52)$$

$$\hat{\Gamma}_T(v) = \Gamma_T(v) + C_T(v) \quad (4.53)$$

Therefore, the noised features are detected as follows:  $\Gamma(\cdot) : y(1), y(2), y(3), \dots, y(n) \longrightarrow y(1), y(2), y(3), \dots, \hat{P}_1(o), \dots, Q\hat{R}S_1(l), \dots, \hat{T}_1(v), \dots, \hat{P}_2(o), \dots, y(N)$

Step 2-Noise Deduction: Corresponding feature noises from C (set of noises for P wave, QRS complexes and T wave) are deducted from the individual corrupted features,  $\hat{F}$  (which was detected earlier in step 1) to reconstruct the original features. These feature reconstruction operations can be expressed as follows:

$$\forall \hat{P}, P_u(o) = \hat{P}_u(o) - C_P(o) \quad (4.54)$$

$$\forall Q\hat{R}S, QRS_w(l) = Q\hat{R}S(l) - C_{QRS}(L) \quad (4.55)$$

$$\forall \hat{T}, T_z(v) = \hat{T}_z(v) - C_T(v) \quad (4.56)$$

Therefore, as an example the reconstruction process is completed by following (where the noises are deducted from corresponding noised features):

$$x(n) = y(1), y(2), y(3), \dots, (\hat{P}_1(o) - C_P(o)), \dots, (Q\hat{R}S_1(l) - C_{QRS}(l)), \dots, (\hat{T}_1(v) - C_T(v)), \dots, (\hat{P}_2(o) - C_P(o)), \dots, y(N)$$

$$x(n) = x(1), x(2), x(3), \dots, P_1(o), \dots, QRS_1(l), \dots, T_1(v), \dots, P_2(o), \dots, x(N)$$

#### 4.5.5 Experimental Results for ECG Obfuscation

As noted earlier, this obfuscation method was tested on ECG measurements collected from 25 subjects using the same procedures, as explained earlier. After successful ECG obfuscation, keys were generated for all the 25 sessions. The key size ranged from only 0.04-0.09% of the original ECG file. When noise equation was used to represent the noises, minimal key size was obtained.

Key sizes can be further reduced by representing the feature templates by equations. Existing research in synthetic ECG shows that the ECG can be represented by mathematical equations 4.52. Lower key size results in faster key distribution to the authorized personnel.

Figure 4.30 represents the corresponding noises for P waves, QRS complexes and T waves for subject 3, which can be expressed as follows:

$$C_P(o) = 0.5 \times e^{\frac{-|t|}{a}} \quad (4.57)$$

where,  $a$  is width of the wave and  $t$  is time (since, ECG signal is in time domain).

$$C_{QRS}(l) = \Pi 2a(t) \quad (4.58)$$

$$C_T(v) = e^{\frac{-t^2}{a}} \quad (4.59)$$

The original ECG and the selected template for P wave, QRS complex and T wave was already shown in Fig. 4.22 and Fig. 4.23. Using these templates and noises (key), the ECG can be successfully obfuscated by the proposed technique as in Fig. 12. This figure reflects only a fraction (1.39 s) of total acquisition time. Figure 4.31 clearly depicts that the all P waves, QRS complexes and T waves appears totally different than the original ECG signal. If features are hidden as it is done by the proposed technique, then both cardiovascular details and person identification are impossible to detect without the knowledge of Eqs. 4.57-4.59 and templates in Fig. 4.23. After obfuscation, the PRD was measured using Eq. 4.60 and it was found to be 2.9750 for subject 3.

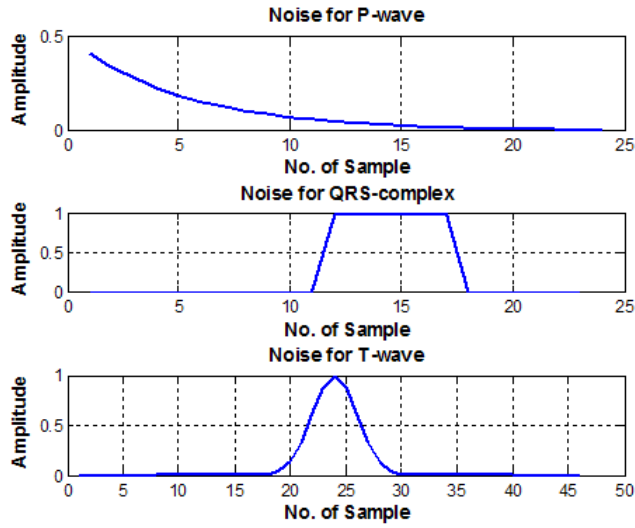


Figure 4.30: Noise for P wave, QRS complex and T wave

$$PRD = \sqrt{\frac{\sum_{i=1}^N [x(i) - f(i)]^2}{\sum_{i=1}^N [x(i)]^2}} \times 100 \quad (4.60)$$

The key for subject 3 was only 936 bytes in size. However, the total file size for the original ECG recording of subject 3 (which is partially presented in Fig. 4.22) was 2433492 bytes. Therefore, the key is less than 0.04 % of the original ECG. This small piece of information is so crucial that without it reconstruction of the noised ECG is not possible. Moreover, this minute information can be very easily transferred to the authorized personnel in secured fashion.

Similarly, the PRDs for the rest of the subjects were measured to be  $5.3450 \pm 2.37$ . For all the sessions, obfuscated ECGs were recovered using their own keys with 100% accuracy, since PRDs for the reconstructed and original ECGs were 0 for all the cases. During this process

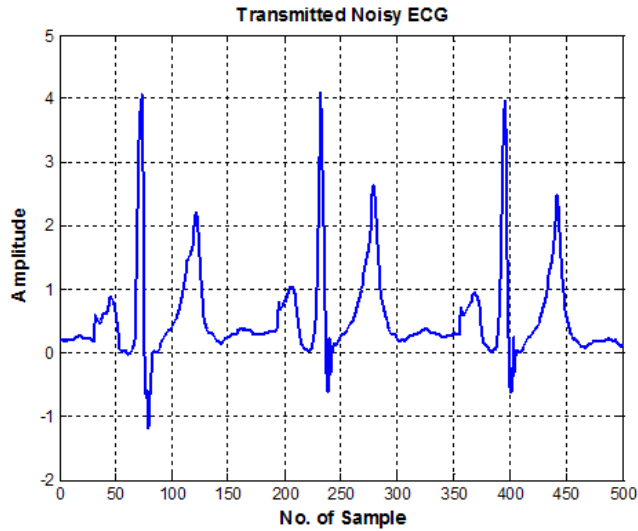


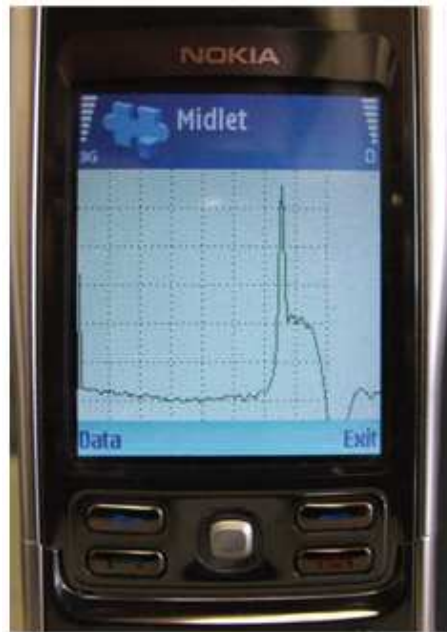
Figure 4.31: Noised ECG signal

random noises were chosen from the noise bank containing 50 noises (25 noise equation and 25 noise vector). All these noises were controlled noises specifically generated in way that adding them with the original ECG does not make the PRD of the original and the obfuscated ECG more than 10

However, we would like to mention that although the proposed feature detection mechanism (Eq. 4.36) provides higher accuracy as compared to both CC method 1 (Eq. 4.32) and CC method 2 (Eq. 4.34), it is computationally expensive compared to CC method 1. Therefore, higher accuracy is purchased with the cost of computational complexity, which is apparent from Eq. 4.36.

A Java MIDlet [Sufi, 2007], which is a miniature program capable of being executed in java supported mobile phones, was programmed to perform ECG feature detection and obfuscation. Figure 4.32 demonstrates the Java MIDlet being executed in Nokia N95 mobile phone.





*Figure 4.32: Implementation of detection and obfuscation on mobile phone*

#### 4.6 Conclusion

To prevent spoofing attacks and refrain malicious users from gaining access to the biometric systems (with the help of captured recognition ECG), the plain-text ECG was encrypted and anonymized in this chapter.

We first showed that 3 Phase Encoding-Compression-Encryption mechanism, which not only secures end-to-end data transfer from the acquisition device to the medical server but also significantly reduces the file size of ECG with a compression ratio of up to 20.06. Therefore, by adding compression and encryption steps along with our encoding method (shown in Chapter 2), we have increased the compression ratio. By encoding (with permutation cipher) the ECG and concealing which compression method and which encryption method to use, the proposed 3 phase ECE mechanism can provide massive security strength (approximately

$4.666 \times 10^{970}$  years as shown in Section 4.3.7.

Then, for the first time, we successfully employed two methods of discrete wavelet based ECG anonymization technique [Sufi et al., 2008d;e]. When the proposed anonymization techniques are applied to a patient centric architecture like Fig. 4.10, patients' privacy is protected. Moreover, faster transmission is achieved due to the benefit of higher compression ratio of up to 2.81.

Next, Packet Wavelet based Anonymization technique was presented. During creation of the anonymized ECG, a secret key was also generated from a feature rich subset of the original recognition ECG. This unique key is only 5.8% of the size of the actual recognition ECG. Therefore, because of the smaller size of the key, key management (e.g. storage) and distribution (e.g. transmission) is comparatively convenient compared to previous studies performed with discrete wavelet transformation.

Lastly, we proposed a new technique for ECG feature detection, which performed classification of P waves, QRS complexes and T waves from several subjects with 1.67 and 2.17 times accuracy compared to two existing CC based approaches. This feature detection method was implemented on the subjects to detect ECG feature for a new noise based ECG obfuscation technique. The proposed ECG obfuscation technique not only conceals the details necessary for person identification, but also hides some of the major cardiovascular details. The keys, which were found to be only 0.04-0.09% of the original ECG file sizes, were generated for all the subjects. The key size of noise based ECG anonymization method was approximately 64.44 times smaller in size than our wavelet based ECG anonymization technique. Therefore, key distribution for this noise based ECG anonymization techniques is even more efficient.

The benefit of using the proposed obfuscation over regular encryption mechanisms including wavelet based ECG anonymization is that the corrupted ECG appears as regular ECG without encryption (unlike existing ECG encryption techniques ([Miaou et al., 2002; Lin and Chung, 2007])). Therefore, to the eavesdropper the process of standard decryption method is useless. Moreover, noise can be represented in enormous number of combinations establishing unmatched security for the proposed ECG obfuscation technique.

Table 4.3: Results for Securing ECG with 3 Phase Encoding-Compression-Encryption Mechanism

MIT_BIH No.	$S_o$	Encoding		Compression		Encryption		$CR_t$	$T_e$	$T_c$	$T_s$	$T_t$
		$S_e$	$CR_{oe}$	$S_c$	$CR_{ec}$	$S_s$	$CR_{es}$					
100	172197	45152	3.82	16355	2.76	8584	1.91	20.06	125	93	15	233
102	171033	44632	3.83	16341	2.73	8672	1.88	19.72	125	62	10	197
105	170912	47952	3.56	17306	2.77	9208	1.88	18.56	140	46	10	196
111	169280	46644	3.63	17330	2.69	9072	1.91	18.66	140	46	10	196
114	171214	44608	3.84	16526	2.70	8880	1.86	19.28	140	62	10	212
201	171367	46163	3.71	16030	2.88	8504	1.88	20.15	140	93	10	243
210	170549	46454	3.67	16694	2.78	8896	1.88	19.17	156	78	10	244
213	168640	51573	3.27	19850	2.60	10568	1.88	15.96	125	62	15	202
222	170355	44296	3.84	16581	2.67	8656	1.92	19.68	125	92	10	227
228	168208	46228	3.64	18075	2.56	9376	1.93	17.94	140	62	10	212
231	169048	46358	3.65	17004	2.73	9072	1.87	18.63	125	62	10	197
234	170184	46478	3.66	16799	2.77	8760	1.92	19.43	125	62	10	197

Table 4.4: Results of Performance Comparison among Three Joint Compression Encryption Mechanisms

Different Cases of arrangements	Average Compression Ratio, $Avg(CR_t)$	Average Total Time $Avg(T_t)$ in ms	Time required to raise one unit of compression ratio, $T_{CR}$ , in ms
2 Phase Encryption-Compression Mechanism	0.99	55.33	55.40
2 Phase Compression-Encryption Mechanism	14.44	571.58	39.58
3 Phase Encoding-Compression-Encryption Mechanism	18.94	213.00	11.25

Table 4.5: Notations for Security Strength of the Scheme

Notation	Definition
$\Delta_1$	For ECG acquisition alone we used three different acquisition devices (GE MAC 5500, Alive Heart Monitor [Ali, Accessed 2009], In-house Developed ECG Monitor) during experimentation. Apart from these, MIT BIH Arrhythmia database entries were also being evaluated. Therefore, the total number of ECG sources was 4.
$\Delta_2$	This is the number of all ASCII permutations for sign encoding, which is $256!$
$\Delta_3$	This is the number of all ASCII permutations for value encoding, which is also $256!$ .
$\Delta_4$	This is the number of supported compression algorithm. Eventually, only one compression algorithm is selected from 4
$\Delta_5$	This is the number of supported encryption algorithms. During our experimentation one encryption is selected from 18 encryption mechanisms

Table 4.6: Reduction of ECG File Size for Method 1 & 2. M1 and M2 Denotes Method 1 and Method 2.

Coefficient Selection	Encrypted Coefficient (M1)	Transmitted Coefficient (M1)	Encrypted Coefficient (M2)	Transmitted Coefficient (M2)
Original Size (bytes)	4,987	17,261	10,513	11,735
Compressed Size (bytes)	2,052	5,712	3,935	3,812
Encrypted Size (bytes)	1,968	-	3,728	-

Table 4.7: Performance Metrics for the Proposed ECG Anonymization Mechanism. Cf. Size, Comp. Cf. Size and Encr. Cf. Size are in Bytes.

Subject	PRD	CC	WDM	CL	Cf. Len	Cf. Size	Comp. Cf. Size	Encr. Cf. Size
1	25.202	0.0415	37.356	51.059	196	1845	837	792
2	25.47	0.004	97.352	20.0565	220	2079	921	880
3	39.112	-0.012	92.425	18.7095	193	1719	801	768
4	33.949	0.006	38.206	47.55975	172	1641	768	728
5	31.407	0.012	28.264	53.31625	157	1505	703	672

Table 4.8: Definition of Mathematical Symbols for ECG Obfuscation

Notation	Description
$x(n)$	Original ECG Signal
$y(n)$	Obfuscated ECG Signal
$\Lambda(.)$	Detection Function
$K$	Key for obfuscation or reconstruction
$\Gamma$	Feature template containing P template, QRS template and T template of the ECG
$C$	Noise template containing P noise, QRS noise and T noise
$\Gamma_P(o)$	Set of ECG samples representing P Template, and $1 = o = O$ , where $O = \text{length}(P\text{template})$
$\Gamma_{QRS}(l)$	Set of ECG samples representing QRS Template, and $1 = l = L$ , where $L = \text{length}(QRS\text{template})$
$\Gamma_T(v)$	Set of ECG samples representing T Template, and $1 = v = V$ , where $V = \text{length}(T\text{template})$
$C_P(o)$	Set of values representing Noise for P and $1 = o = O$ , where $O = \text{length}(P\text{template})$
$C_{QRS}(l)$	Set of values representing Noise for QRS and $1 = l = L$ , where $L = \text{length}(QRS\text{template})$
$C_T(v)$	Set of values representing Noise for T and $1 = v = V$ , where $V = \text{length}(T\text{template})$
$F$	Feature set containing all the P, QRS and T from original ECG, $x(n)$
$P$	P feature set containing all the $P_u(o)$ within the original ECG, $x(n)$ , where $P \subset F$ and $u = 1, 2, 3$ ,
$QRS$	QRS feature set containing all the $QRS_w(l)$ within the original ECG, $x(n)$ , where $QRS \subset F$ and $w = 1, 2, 3$ ,
$T$	T feature set containing all the $T_z(v)$ within the original ECG, $x(n)$ , where $T \subset F$ and $z = 1, 2, 3$ ,
$\bar{F}$	Set of ECG samples without containing any ECG Feature like P wave QRS complex or T wave

Table 4.9: Definition of Mathematical Symbols for ECG Reconstruction

Notation	Description
$\Xi$	Reconstruction Function, $\Xi : y(n) \longrightarrow x(n)$
$\hat{F}$	Obfuscated Feature Set containing all the Obfuscated P, Obfuscated QRS and Obfuscated T
$\hat{P}$	Obfuscated P feature set containing all the $\hat{P}_u(o)$ within the original ECG, $x(n)$ , where $\hat{P} \subset \hat{F}$ and $u = 1, 2, 3, \dots$
$Q\hat{R}S$	Obfuscated QRS feature set containing all the $Q\hat{R}S_w(l)$ within the original ECG, $x(n)$ , where $Q\hat{R}S \subset \hat{F}$ and $w = 1, 2, 3, \dots$
$\hat{T}$	Obfuscated T feature set containing all the $\hat{T}_z(v)$ within the original ECG, $x(n)$ , where $\hat{T} \subset \hat{F}$ and $z = 1, 2, 3, \dots$
$\hat{\Gamma}$	Obfuscated or noised template containing noised P template, noised QRS template and noised T template
$\hat{\Gamma}_P(o)$	Noised P template created by adding P noise with P template
$\hat{\Gamma}_{QRS}(l)$	Noised QRS template created by adding QRS noise with QRS template
$\hat{\Gamma}_T(v)$	Noised T template created by adding T noise with T template

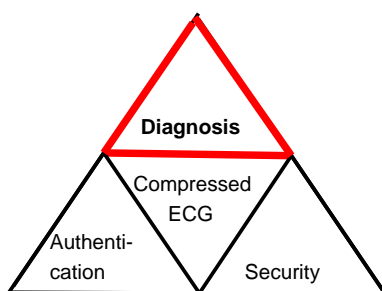


## Chapter 5

# Efficient Cardiovascular Diagnosis

ECG has been intensively used by cardiac specialists to efficiently diagnose Cardiovascular Diseases (CVD) for the last seven decades [Hamilton and Tompkins, 1986; Friesen et al., 1990; Clifford et al., 2006; Bartolo et al., 2001; Kusumoto, 2009]. Apart from diagnosing CVD, ECG is also used for monitoring breathing pattern, mental stress and condition of autonomous nervous system [Kumar et al., 2007]. ECG can also reveal the identity of a person using ECG based biometric techniques as we have learnt in Chapter 3.

For wireless telecardiology, limited bandwidth is one of the major bottlenecks of faster diagnosis. Many of the recent telemonitoring platforms suggest using innovative compression technologies, so that the massive amount of ECG data (e.g. ECG from 12 leads) can be accommodated with today's bandwidth constrained mobile Internet (as described in Chapter 2). However, since ECG packets are kept in compressed format by these efficient tele-cardiology platforms, the packets need to be decompressed before using any existing diagnosis algorithms [Lee et al., 2007; Hung and Zhang, 2003; Jasemian and Arendt-Nielsen, 2005; Hamilton and



*Figure 5.1: Cardiovascular Diagnosis on Mobile Phone*

[Tompkins, 1986; Friesen et al., 1990; Clifford et al., 2006; Bartolo et al., 2001]. This extra step of decompression before performing diagnosis entails delay in diagnosis, which can be a killer. After having a cardiac arrest, the cardiac cell damage may start, which is an irrecoverable process. The dead cardiac cells will never revive. That is why every seconds count, when a patient is having the symptom of a cardiac arrest [Luca et al., 2004; Bradley et al., 2006].

The key to faster diagnosis is to perform diagnosis directly from the compressed ECG as opposed to decompress the compressed ECG and then perform diagnosis on the plain ECG. Our recent research in wireless telecardiology shows that cardiovascular diagnosis from compressed ECG is faster than decompression followed by diagnosis. This chapter answers our last research question of faster CVD diagnosis from ECG. To reduce the delay in treatment and diagnosis, in previous chapters we focused on faster ECG transmission via mobile telephony network and faster (and secured) authentication mechanism. Cardiac abnormality detection directly from the compressed ECG will be the main focus of this chapter (Fig. 5.1).

## 5.1 ECG Diagnosis from plain ECG

The diagnosis of cardiovascular diseases with ECG signal has been well researched and well established for the last few decades. However, almost all these algorithms were designed for the plain (uncompressed) ECG. Within the last 5 years, research on mobile phone based cardiovascular monitoring is progressing well, since cardiovascular diseases is the number one killer of modern era. Existing ECG diagnosis algorithms can be classified into three different categories as follows:

- Direct Approach
- Transformational Approach
- Intelligent Approach

### 5.1.1 Direct Approach

Direct methods encompass diagnosis algorithms that are of relatively lower complexity. They tend to apply some simple mathematical operations on the original ECG to extract the feature waves. Amplitude based method, First Derivative based method and Second Derivative based methods are some examples of direct-methods to locate the QRS complex of ECG [Hamilton and Tompkins, 1986; Friesen et al., 1990]. Because of lower complexity, they are suitable for mobile and embedded devices with lower computational capacity. we have implemented few of the direct methods to locate QRS complex and calculate RR interval in mobile platform, as seen in figures 5.2 and 5.3.

These 3 existing methods have been used in various applications and their implementa-

tions vary across different literatures. The details of our implementation for these existing ECG beat recognition methods are briefly described here.

The *Amplitude based Technique* (ABT) performs simple and primitive comparisons where the ranges of sample ECG points falling beyond an amplitude threshold are determined to be a possible QRS complex candidate. Within Table 5.3, the column "Th." shows varying thresholds for different MIT BIH entries (first 60 seconds of ECG data).

For *First Derivative based Technique* (FDBT), first derivatives of the original ECG signal are obtained before performing any other calculations. To measure the performance of FDBTs on mobile phone, a modified version of [Hamilton and Tompkins, 1986] was adopted. A QRS complex candidate is suspected whenever three consecutive first derivative values are greater than a positive slope threshold (0.1375), followed within next ten samples by two consecutive first derivative values less than a negative slope threshold (-0.2). The following 3 conditions describes this process.

*Condition 1:*  $y_i, y_{i+1}, y_{i+2} > 0.1375$

*Condition 2:*  $y_j, y_{j+1} < -0.2$

*Condition 3:*  $j - i < 10$

In Table 5.3, the column *On Set* and *Off Set* reflect these two parameters.

The *Second Derivative based Technique* (SDBT) relies on similar mechanism used in QRS detection algorithms based on Second Derivatives. For performance comparison, a modified version of [Balda, 1977] was adopted. At first, Eq. 5.1 - 5.2 was used to evaluate  $y_0$  and  $y_1$ .

$$y_0 = ABS(x_{n+1} - x_{n-1}) \quad (5.1)$$

$$y1_s = ABS(y0_{d+2} - 2y0_d + y0_{d-2}) \quad (5.2)$$

where,  $s = 1, 2, 3, 4, \dots, N - 3$

A scaling value,  $y2$  is calculated from  $y2_s = 1.3y0_d - 1.1y1_s$ . All values higher than a threshold value, are determined to be the beginning of a QRS candidate ( $y2_s \geq 0.9$ ). In Table 5.3, this parameter  $y2_s$  is referred as "Const".

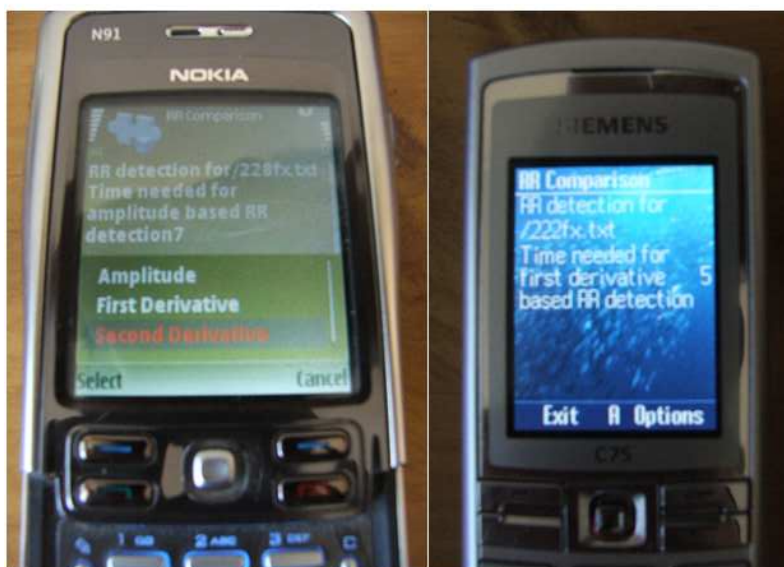
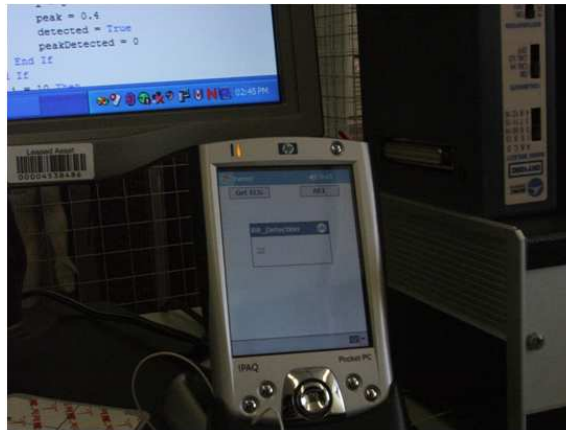


Figure 5.2: Implementation of Direct Methods for Diagnosing ECG on J2ME Supported Mobile Phones

### 5.1.2 Transformational Approach

These methods include application of transformations like wavelet transform, Fourier transform, cosine transforms etc. [Dokur et al., 1999; Lemire et al., 2000]. They require higher computational power compared to most of the direct methods. Often, these methods transform the ECG from time domain to some other domains like frequency domain.



*Figure 5.3: Implementation of Direct Methods for Diagnosing ECG on .Net Supported PDAs / Smart Phones*

### 5.1.3 Intelligent Approach

These methods employ various intelligent techniques like Neural Network, Clustering, Support Vector Machine, Attribute Selection, Hermite Polynomial etc. [Gang et al., 2000]. They consume the highest level of processing power and almost unsuitable for processing by the mobile or embedded devices.

## 5.2 ECG Diagnosis from compressed ECG

With the advent of modern mobile phone based telecardiology applications, the ECG packets are being transmitted in compressed format to suit the limited bandwidth of mobile telephone network. The ability to perform diagnosis straight from the compressed ECG packets has been proven to be faster than applying existing ECG diagnosis on the compressed ECG, after decompression.

Once the ECG data is compressed and secured, faster and efficient transmission is guaranteed. The encoded ECG segments from several patients are transmitted to the medical

server over the wireless network. The medical server continues to perform background detection on these stored ECGs. When an abnormality is detected by the background monitoring agent of the medical server, the doctor is notified via SMS and MMS messages. This type of communication from the medical server to the doctor is called *Server Push Abnormality Notification* (SPAN). On the other hand, a doctor might want to view the status of his patients on his mobile phone, and may request the data from the Medical Server. This type of communication is defined as *Doctor Pull Wellness Monitoring* (DPWM). With both the cases, the doctor's mobile is flooded with ECG segments from several patients. Under these circumstances, the urgent and more serious ECG segments must be dealt first with higher priority. Therefore, a fast HR estimation algorithm (Algorithm 1) is required to screen out more serious patients requiring immediate attention. The proposed HR estimation algorithm can estimate the HR very fast with a high degree of accuracy. The crucial reason for this algorithm to be faster than any other existing HR detection methods is simple: the proposed HR estimation algorithm does not require to read the compressed ECG data.

Once the HR is estimated, so that the more serious patients are remotely attended by the doctor, the estimation results are required to be confirmed. This should be done with some detailed HR calculation methods. However, if existing HR calculation methods are used, then the compressed and secured ECG data must be decompressed by the doctor's mobile phone, since existing HR calculation methods are unable to work with compressed ECG segments [Friesen et al., 1990; Hamilton and Tompkins, 1986; Balda, 1977]. Decompressing these multiple ECG segments produced by several patient's that a doctor is assigned, consumes enormous time and processing power on the doctor's mobile phone. Apart from introducing

delay in diagnosis while performing both decompression and analysis of ECG signals, the decompression task also poses a new threat of patient's privacy being compromised. If the doctor's mobile phone decodes or decompresses the ECG signal on his mobile phone, the uncompressed ECG might be captured by an impostor leading to health privacy vulnerability. Obviously, it should be a better choice if the compressed / encoded ECG segments are maintained as it is and the entire ranges of estimation or detection tasks are performed directly on the compressed ECG packets. It should be noted that during the earlier phase, the proposed HR estimation method does not even read the content of the compressed ECG packets. At this stage, the proposed HR calculation method, which is described in algorithm 2, reads the compressed ECG and without further decompressing or decoding it, can reconfirm the estimated HR with confidence.

Figure 5.4 shows the workflow of the proposed cardiac diagnosis system based on compressed ECG for the wireless telecardiology application. Once a compressed ECG packet arrives via MMS, SMS, HTTP or Socket connection to the doctor's mobile phone, the size of the compressed ECG is obtained. Then, HR estimation algorithm (Algorithm 1) performs a preliminary estimation of the HR. As it is seen from algorithm 1, after receiving a packet, the payload size (containing compressed ECG) is obtained. Then, the heart rate ( $HR_{est}$ ) is estimated. Based on the estimated HR, further action is taken. If the HR is lower or higher than a normal person's HR, then the proposed HR calculation algorithm (Algorithm 2) performs calculation on the compressed ECG to confirm particular heart abnormalities like bradycardia or tachycardia. Additionally, the irregularity of the beats are checked for determination of arrhythmia (using Algorithm 3), where beat intervals are irregular [Bar-



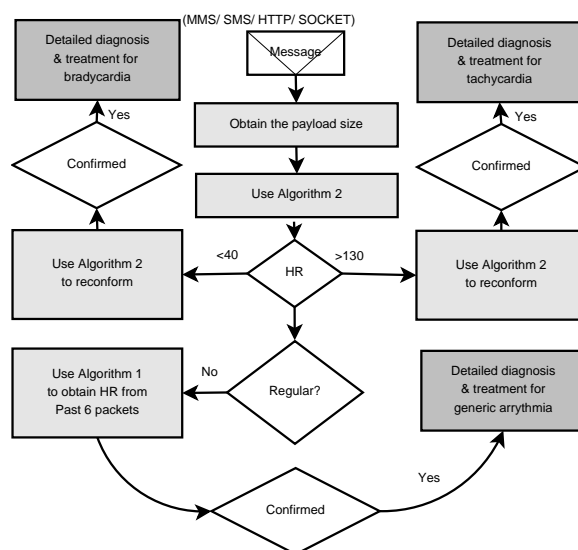


Figure 5.4: The Proposed Cardiac Diagnosis System

tolo et al., 2001]. Moreover, Algorithm 4 determines instances of wide QRS, which provides indication of several heart disturbances.

Our previous research works suggest that ECG diagnosis from the compressed ECG can be performed by the following three ways.

- Instant Detection Approach
- Direct Approach
- Intelligent Approach

### 5.2.1 Instant Detection Approach

The heart rate estimation algorithm does not require reading the compressed ECG. It only checks the payload size within a particular ECG packet (containing compressed ECG). Therefore, these algorithms provides the fastest diagnosis (since there is no decompression or even

Table 5.1: The Relationship between CR and Encoding Types

MIT_BIH Entry No.	Heart Rate	Sub Set U Encoding	Sub Set V Encoding	CR
114	54	10155	645	4.03
231	63	9737	1063	3.87
111	68	9695	1105	3.86
102	73	10081	719	4.01
228	73	9781	1019	3.86
100	74	10131	669	4.05
222	75	10271	529	4.05
105	83	9505	1295	3.85
201	90	9913	887	3.97
210	91	9836	964	3.93
234	92	9870	930	3.93
213	111	8529	2271	3.56

reading of compressed character involved) decision with the cost of accuracy. Therefore, they are suitable for preliminary diagnosis (not for final diagnosis).

We earlier explained in Chapter 2 that each  $U$  character represents 2 entries of Differenced Normalized ECG without sign. Therefore, higher compression is achieved ( $2 \times \log_{10} M_o$ ) when the compressed ECG segments contain large number of  $U$  characters. Whereas, in multiple character encoding, single entry of Differenced Normalized ECG without sign is represented by a single  $V$  character. Eventually, compressed ECG containing larger area of  $V$  character subset (compared to  $U$  character subset), result in lesser compression. Table 5.1 shows the compression ratio achieved with our proposed algorithm. Clearly, the ratio is linearly dependant ( $\gamma = 0.983$ ) on the number of single character encoding with  $U$  and inversely dependant ( $\gamma = -0.983$ ) on the number of multiple character encoding with  $V$ .

Curve fitting techniques reveal this in Eq. 5.3 and 5.4

$$CR = 0.0003 \times N_{Uenc} + 1.0549 \quad (5.3)$$

$$CR = -0.0003 \times N_{Venc} + 4.2085 \quad (5.4)$$

where,  $N_{Uenc}$  = Number of  $U$  character subset Encoding,  $N_{Venc}$  = Number of  $V$  character subset Encoding and  $CR$  = Compression Ratio.

**Observation 1:** Equation 5.4 basically shows that higher  $V$  elements within the ECG subset results in lower CR (or lower  $V$  elements translates to higher CR). Therefore, Fact 1 is established.

$$\mathbf{Fact\ 1:} \quad N_{Venc} \propto \frac{1}{CR}$$

Even though, the relationships among  $CR$ ,  $N_{Uenc}$  and  $N_{Venc}$  are evident from Table 5.1, the relationship between CR and HR is not seemingly apparent. Therefore, to understand this relationship, knowledge of QRS morphology is required. The duration of QRS complex is from 0.06 to 0.1 sec. for normal case. However, for abnormal cases, where conduction is impaired within the ventricles, duration of QRS is over 0.1 sec. (Wide QRS) [Kusumoto, 2009]. The MIT\_BIH database contains many of the serious heart abnormality cases, with wider and shorter QRS durations. Therefore, comparing HRs of different patients from MIT\_BIH database with respect to same  $CR$ , might result in wider variance in HR values.

However, for a particular individual, the morphology of QRS complex remains unchanged [Wubbeler et al., 2007]. Utilizing this phenomenon, recent researches show that human identification is possible (as shown in Chapter 3). Hence, if we select a particular subject and measure his ECG for different HRs and then compress those ECG segments (of different HRs), we will see that there is a clear linear relationship between the HR and CR. The mathematical logic behind this phenomenon will be further explained at a later stage in this section after the establishment of few facts. Figure 5.6 shows this linearity for a particular patient with heart abnormality. For this patient ECGs were taken at different HRs. Those ECG segments collected for different HRs were compressed. CRs were calculated for all of those ECG segments. This relationship for that particular patient can be expressed by following:

$$HR = -238.79 \times CR + 957.6 \quad (5.5)$$

Equation 5.5 basically tells that when CR is known for a particular patient, HR can be estimated. For each person being monitored, equations like this is easy to calculate with curve fitting tools. The generic form of this equation is as follows:

$$HR = a \times CR + b \quad (5.6)$$

For each individual, the values of  $a$  and  $b$  are different within Eq. 5.6. This is because,

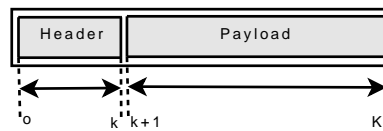


Figure 5.5: Compressed ECG Packet

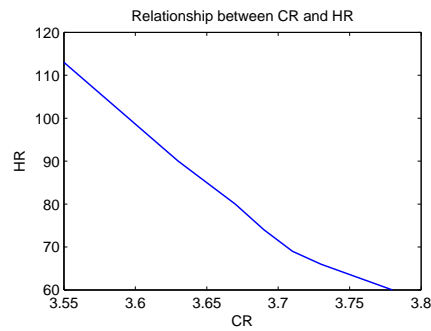


Figure 5.6: The Relationship between Heart Rate and Compression Ratio

HR pattern differs from person to person according to ECG based biometric research (please refer to Chapter 3). According to the literature, this intrinsic relationship between HR and CR was never researched before. This particular relationship can be highly useful for wireless telecardiology application. When the doctor or the medical server receives the compressed ECG packets, the payload size can be obtained even without decompressing it. From the payload size, CR can be derived from Eq. (5.7).

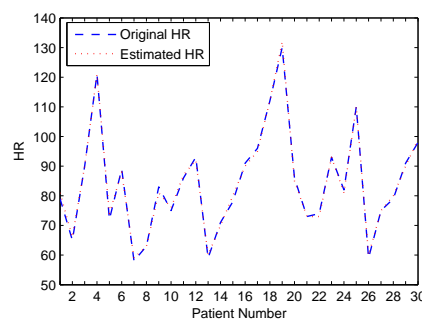


Figure 5.7: The Distance between the Estimated HR and Original HR

---

 Algorithm 1: The Proposed Estimation of Heart Rate (HR)
 

---

**on receipt of message**
**obtain the payload size,  $S_c = K - (k + 1)$** 
**estimate  $HR = a \times \frac{S_o}{S_c} + b$** 


---

$$CR = \frac{S_o}{S_c} \quad (5.7)$$

Here,  $S_o$  is original ECG packet size, which can be set fixed for a particular telecardiology application.  $S_c$  is the payload size of the packet containing compressed ECG. Hence, HR for a particular patient can be successfully estimated with the following simple equation:

$$HR_{est} = a \times \frac{S_o}{S_c} + b \quad (5.8)$$

This estimation of heart rate is by far the fastest and simplest algorithm (containing three basic operations  $\times$ ,  $\div$  and  $+/-$ ) as far as HR calculation is concerned. Unlike any other method of HR calculation, this innovative method does not even need to read the payload data containing compressed ECG. The size of the payload can be retrieved from the header of compressed ECG packet. As shown in Fig. 5.5, the payload size is  $(K - k - 1)$ , where  $K$  is the total message length and  $k$  is the length of the message header.

When experimented on 30 MIT BIH entries (21600 samples segmented from each entries), the difference between the predicted (i.e. estimated) and original HR was measured to be 1.14 in terms of Root Mean Square Error (RMSE) (Eq. 5.9) Figure 5.7 shows that for those

30 ECG segments (collected from randomly selected MITBIH entries) the estimated HR ( $HR_{est}$ ) and original HR coincided, upholding high accuracy of this HR estimation method.

$$RMSE = \left[ \frac{1}{N_{sub}} \sum (HR_{est} - HR_{orig})^2 \right]^{1/2} \quad (5.9)$$

Here,  $N_{sub}$  is the number of Subjects. This experimentation results suggest that HR can be estimated with good confidence level within shortest possible time, drastically minimizing the delay faced by the existing wireless telecardiology applications. Apart from this, the dependency of  $CR$  and  $HR$  ensures that the ECG data pertaining to more serious patients is transmitted first. Whenever, a patient is lively or performing any strenuous activities, he or she will be experiencing higher heart rates (except for different cases of tachyarrhythmia). The heart of a dying patient with the symptoms of Assystols, when the electrical activity of the heart is desperately seeking pause, creates tremendously lesser amount of beats. This extremely lower HR results in higher CR. Higher CR results in faster data transmission of minimal ECG data (compressed).

This technique provides the likelihood of a particular compressed ECG packet containing abnormality. The heart rate estimation method is an example of instant detection technique based on compressed ECG. It was found that an ECG signal containing more heart beats will have lower compression ratio when compared with an ECG packet with less heart beat, under the following two constraints:

1. If the person is same

2. If the numbers of ECG samples are same for the packets

### 5.2.2 Direct Approach

While the HR estimation method provides approximate HR values within the shortest possible time, to confirm the estimated values a detailed and more accurate HR calculation method is necessary. As it is already mentioned (in Section III - c) that the compression algorithm encodes the ECG with two different character sets ( $U$  and  $V$ ).  $U$  characters sets encode the low sloped ECG segments. However, the QRS portion of the ECG segment contains high sloped values. This high sloped ECG is encoded with  $V$  character set. The proposed HR calculation method only needs to identify  $V$  character set locations, to identify QRS complexes. In this section, we first introduce the system detail of this innovative HR calculation method.

#### Method Description

As depicted in Fig. 5.8, the compressed ECG stream  $S$  is read from one direction to another direction inside a buffer. Therefore, the buffer is moved forward in a window sliding fashion until the end of the compressed ECG stream is reached. During this sliding procedure, the content of the buffer is updated. This buffer content for a particular instant is expressed as  $B$ , where  $B \subseteq S$ .

Hence for a particular instance of the buffer position,  $B = \{b_1, b_2, b_3, \dots\}$  can contain  $\Phi$  (where,  $\Phi \subset U$ ),  $\Psi$  (where,  $\Psi \subset V$ ) or mixed elements from both  $U$  and  $V$ . From these three different possibilities of the character contents for  $B$ , beats can be detected by the conditions



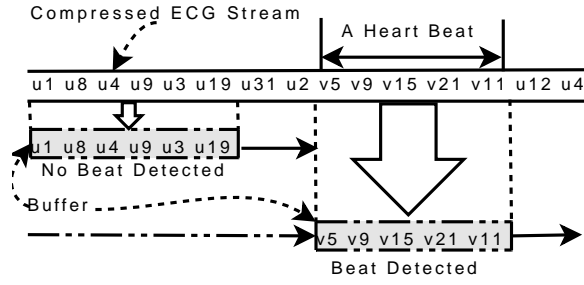


Figure 5.8: Heart Beat Detection from Compressed ECG

stated in Eqs. 5.10 - 5.11:

$$\forall b_i : B \subset V \quad (5.10)$$

$$\forall b_i \exists \Psi_i : |B| - |\Psi| < th \quad (5.11)$$

In Eq. 5.11, it is required that majority of the content of  $B$  be elements from  $V$ . The threshold  $th$  was determined to be 2, during our experimentation. To reduce the computational complexities, after a successful beat detection a mandatory stall is initiated, since it is a medical fact that minimum distance between two consecutive heart beats is 0.2 second. Depending on the acquisition frequency, the minimum number of stalled ECG samples is calculated as,  $Stalled\_Sample = 0.2 \times F$ , where,  $F$  is the sampling frequency of ECG acquisition device.

Hence, for our experimentation with a sampling frequency of 360 the stall period is

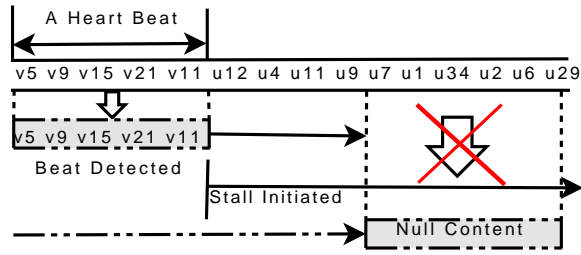


Figure 5.9: Initiation of Stall after Successful Beat Detection

72 ECG samples. This means that we can skip reading 72 characters (approx) following a successful beat detection, since it is highly unlikely that a high pitched value will be observed immediately after beat detection. During this stall phase, reading operations in the buffer to update  $B$  is prohibited as seen in Fig. 5.9. The reading operations are resumed only after the stalled period is over. This increases the performance of the algorithm. It is understood that the positive predictivity and the specificity of the algorithm revolves around the following three parameters: Buffer Size (window size), Threshold,  $th$  (of Eq. 5.11) and Stall period.

This HR calculation was implemented with Algorithm 2, which detects all the high pitched values represented with  $V$  elements. As seen from Fig. 5.10, the locations of the QRS complexes remain hidden within the compressed ECG stream, from where it is picked up by Algorithm 2. Within Fig. 5.10, the  $V$  character sets are represented by the numeric characters (0-9), upper case characters (A-Z), a small subset of lower case characters (m, n, o, p, q, r, s, t, u, v, w, x, y, z) and double quote character ("). When, this  $V$  character set is known, location of the QRS complexes can be identified. This algorithm 2, basically reads the compressed ECG and if high pitched ( $V$  character set) values are found, then variable  $Slope\_Count$  is incremented. When the value of the  $Slope\_Count$  gets higher then the threshold ( $Buffer\_Size$ ), a beat is detected. After detecting a beat, a mandatory stall

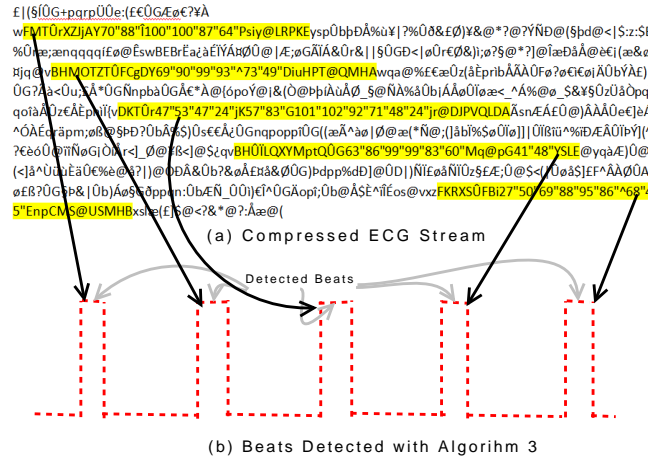


Figure 5.10: Beats Hidden within Compressed ECG. The Shaded Segments Represented by  $V$  Character Set, Where Each Segment Indicates Width of a Whole QRS Complex.

is initiated. During the stalled period, only the value of  $Stall\_Count$  is decremented.

**Observation 2:** Figure 5.10 clearly shows that QRS width is equivalent to the number of  $V$  characters,  $N_v$  within a block (where each block represents a QRS complex). Moreover, since each QRS complex is represented with powerful ventricular activity, HR is equivalent to number of  $V$  character blocks,  $N_b$  (within a minute). Therefore, Fact 2 and Fact 3 are established.

**Fact 2:**  $QRS\ Width = N_v$

**Fact 3:**  $N_b = HR$

At this point, it is also clear that the total number of  $V$  characters within an ECG segment,  $N_{Venc}$  is  $(N_v \times N_b)$ . Therefore, Fact 4 and 5 are deduced.

**Fact 4:**  $N_v \propto N_{Venc}$ , when,  $N_b$  is constant

---

```

Algorithm 2: Heart Rate Calculation From Compressed ECG
Stall_Count = 0 // Manage stall after beat detection
Slope_Count = 0 // Counts occurrences of the V set
Loop (Until the end of compressed ECG)
  Read one compressed character
  if ((both current and previous character are
    members of V) AND (Stall_Count = 0))
    Slope_Count = Slope_Count + 1
    if (Slope_Count > Buffer_Size)
      Beat Detected
      //Initiate Stall
      Stall_Count = (Stall Value)
    endif // When the character member of set
  elseif (Stall_Count <> 0)
    Stall_Count = Stall_Count - 1
  endif
End Loop

```

---

**Fact 5:**  $N_b \propto N_{V_{enc}}$ , when,  $N_v$  is constant

Finally, from fact 1, 2, 3 and 5, it can be logically deduced that  $HR \propto \frac{1}{CR}$ , for a particular human being, since for a particular individual the QRS morphology (e.g. QRS width) remains unchanged as demonstrated in earlier researches [Wubbeler et al., 2007]. This proof (by deduction logic) explains our earlier results (of experimentation) showing the inverse relationship between HR and CR (demonstrated by Fig. 5.6 and Eq. 5.5).

### Cardiovascular Abnormality Detection

Apart from the manual annotations and inspections of ECGs by the expert cardiologists, automated algorithms have also demonstrated their abilities to efficiently detect different cardiovascular abnormalities. However, according to the literature, there exists no single

Table 5.2: Disease Detection with Algorithms

Disease Detection	Algorithms Used	Description
Tachycardia	Algorithm 1, Algorithm 2	when $HR_{est} > 120$ (refer to Eq.5.7)
Bradycardia	Algorithm 1, Algorithm 2	when $HR_{est} < 30$ (refer to Eq.5.7)
Arrhythmia	Algorithm 1, Algorithm 2, Algorithm 3	when $\frac{(HR(n)_{est}-HR(n+1)_{est})}{HR(n)_{est}} > 15\%$ (refer to Eq.5.7) or $\frac{RR(n)-RR(n+1)}{RR(n)} > 15\%$ for 3 consecutive RRs
WPS, RBBB, LBBB, Ven- tricular Conduction Problems	Algorithm 4	when QRS width is more than 0.12 seconds or approx. 44 samples (when the sampling frequency is 360)

algorithm that can detect all possible abnormalities [Chiu and Kao, 2001; Seydnejad and Kitney, 1997; Kumar et al., 2007; Akselrod et al., 2007; Hamilton and Tompkins, 1986; Bartolo et al., 2001]. While most of the existing algorithms execute on uncompressed ECG, our attempt of ECG abnormality detection from compressed ECG has many advantages like faster execution, ensuring patient's privacy etc. Faster execution is possible because number of characters to be analysed is reduced in compressed ECG. Table 5.2 provides a glimpse of different cardiovascular abnormalities efficiently recognised by our proposed mobile phone based wireless telecardiology system.

In Fig. 5.11, RR, which is the time difference between two consecutive occurrences of heart beats (specifically QRS complex), has been calculated by an existing method and our proposed HR calculation method. Amplitude based Technique (ABT) is used here as an

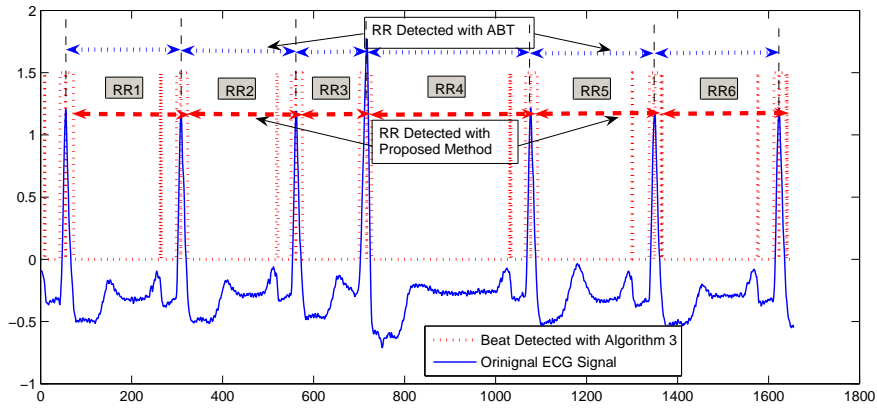


Figure 5.11: RR Interval for an MITBIH Entry. The RR Intervals Values Calculated by both the Methods are Almost Similar. However, the Proposed Method is a Bit Time Shifted from the RRs Calculated by ABT. Most Importantly, in Terms of Accuracy, this Lagging does not have any Adverse Affect, since the Time Shifted Delay (almost constant) is Added to Each of the RR Intervals.

existing QRS detection mechanism and RR was calculated based on that. It is evident from Fig. 5.11 that our implementation is able to determine the RR interval with high level of accuracy.

This RR detection algorithm is implemented with Algorithm 3, which relies on Algorithm 2 for beat detection (by detecting  $N_b$  as in Fact 3). Once HR is detected with algorithm 2, index of the current sample is recorded ( $rr\_previous$ ). On the detection of the next beat current sample is again recorded ( $rr\_current$ ). Next, the difference between the two consecutive beats are obtained (in terms of number of samples,  $int\_rr$ ). At the end, the counted number of samples (difference between two beats) are converted to time to obtain RR interval ( $rr\_interval$ ). As seen in Fig. 5.11, execution of this algorithm on a sampled ECG having irregular RR intervals correctly identifies any irregularity within RR intervals (which is important for Arrhythmia detection). As clearly seen, the interval RR3 is the

---

Algorithm 3: RR Interval Calculation From Compressed ECG

---

```

rr_interval = 0 // Count the number of samples between successive Rs
int_rr = 0 // Count the number of samples between successive Rs
Loop (Until the end of compressed ECG)
  if (beat detected)
    rr_current=(get the index of current sample)
    int_rr = rr_current - rr_previous
    rr_previous = rr_current
    rr_interval =  $\frac{int\_rr}{f}$ 
  endif
End Loop

```

---

shortest and RR4 is longest (Fig. 5.11).

After retrieval of RR signal, it is possible to deduce Heart Rate Variability (HRV), which is basically the rate of change of consecutive RR values [Akselrod et al., 2007; Seydnejad and Kitney, 1997; Ruha et al., 1997]. HRV provides detailed understanding of Cardiovascular Autonomic Control and activities of the Autonomous Nervous System [Chiu and Kao, 2001]. The importance of HRV started to be appreciated in the late 1980s, when it was confirmed that HRV is a strong predictor of mortality after an acute myocardial infarction [Malik et al., 1989]. Moreover, recent research shows that HRV also provides indications for mental stress and respiratory functions of an individual [Kumar et al., 2007; Meste et al., 2005].

Apart from detection of RR interval and HRV from the compressed ECG, it is also possible to detect Wide QRS, which indicates many cardiovascular abnormalities like Wolff-Parkinson-White syndrome (WPS), Left Bundle Branch Block (LBBB), Right Bundle Branch Block (RBBB) etc. [Kusumoto, 2009]. Figure 5.12 shows that using Algorithm 4, it is possible to detect occurrences of wide QRS. Algorithm 4, continues searching for more  $V$  elements just after detection of a beat by Algorithm 2. If greater number of  $V$  elements are located adjacent to a detected beat, wide QRS is confirmed by Algorithm 4. Within algorithm 4, the

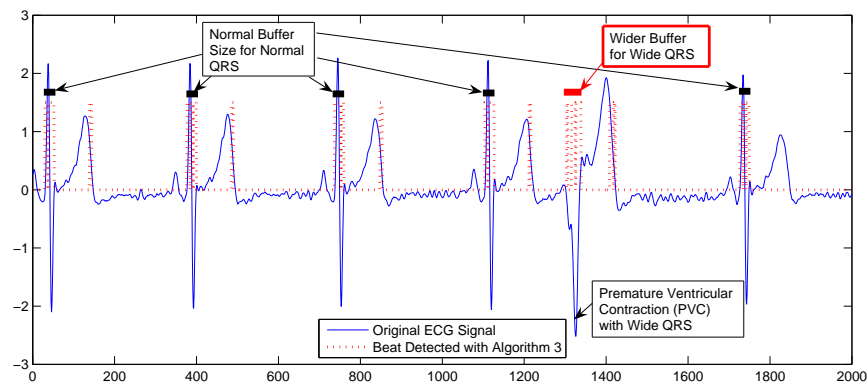


Figure 5.12: Wide QRS Detected with Wider Buffer Size (Higher Values of  $N_v$  as per Fact 2)

number of  $V$  characters are calculated and kept in variable  $QRS\_Len$ . When,  $QRS\_Len$  is greater than the normal beat threshold (normal beat width in terms of  $V$  characters), wide QRS is Identified. This is aligned with Fact 2, where it is stated that wide QRS is identified with higher values of  $N_v$ .

It should be noted that within algorithm 4, two compressed characters are read at a time. If both of the characters are  $U$  elements then it is not a beat. However, if at least one of the characters are  $V$  element then this indicates that the algorithm is still reading the beat. In this case (one  $V$  element and one  $U$  element), the  $U$  element can be the sign information and  $V$  element can be the high slope of the QRS. In the most obvious case, both the characters are  $V$  elements carrying high sloped QRS values (still reading beats) and  $QRS\_Len$  is incremented. Direct methods check the frequency of some particular compressed characters (or encoded characters) and apply a threshold for diagnosis decision.



---

Algorithm 4: Detection of Wide QRS

---

```

QRS_Len = 0 // Holds the QRS length
WideQRS = false
Loop (all the detected beats  $H_i$ )
  Beat Detection with Algorithm 2 (Equation 11 or 12 is fulfilled)
  Loop (if any character of the next two character read  $\in V$ )
    QRS_Len = QRS_Len + 2
  End Loop
  if ( $QRS\_Len > threshold$ )
    WideQRS = True
  endif
End Loop

```

---

### Comparison Result

Table 5.3 provides the comparison results of various methods. It is clearly seen that the proposed HR calculation method performs well by accurately calculating the number of beats (from compressed ECG) with minimal changes of the algorithm parameters. These algorithm parameters are used to control the positive predictivity and specificity. During this comparison, different ECG recordings from the MIT BIH database were used. MIT BIH database entries were previously used by many researchers for performance comparisons of their algorithms [Jalaleddine et al., 1990].

Finally, to obtain a critical understanding of delay minimizing effort performed for telecardiology applications with our research, Table 5.4 is presented. This table provides a rapid glimpse of our efforts in reducing the delay when compared to existing telecardiology applications. In this table two scenarios, as depicted in Fig. 5.13, are compared with our proposed solution. Clearly, the proposed solution makes better use of the limited network bandwidth to transfer ECG data with minimal delay.

In scenario 1, ECG segments (files) from randomly selected MIT-BIH entries are trans-

Table 5.3: Comparison of the proposed HR detection method with ABT, SDBT and FDBT.

MIT BIH	Proposed			SDBT		ABT		FDBT			HR Count
	Slope	Stall	HR	Const	HR	Th.	HR	On Set	Off Set	HR	
100	13	75	74	1.0	74	0.4	74	0.1375	-0.2	74	74
102	13	75	73	1.0	73	0.35	73	0.12	-0.2	73	73
105	13	75	83	0.6/0.7	111/23	0.4	83	0.18	-0.2	83	83
111	13	75	68	0.4/0.5	112/42	0.37	68	0.1375	-0.11	68	68
114	13	75	54	0.6	54	-	53	0.1375	-0.2	54	54
						0.0195					
117	10	75	50	0.7	50	-0.16	49	0.1375	-0.2	50	50
207	10	80/81	66/67	0.4	61	0.42	67	0.1375	-0.2	66	66/67
210	4/5	75	92/91	0.6	85	0.4	85	0.1375	-0.2	91	90/92
213	13	75	111	1.4	112	0.4	111	0.1375	-0.2	111	111
219	13	75	74	1.3	72	0.4	74	0.18	-0.2	74	74
222	5	75	75	0.5	90	0.2	75	0.18	-0.2	75	75
228	7	75	73	0.6	72	0.33	75	0.1375	-0.2	73	73
231	13	75	63	1.4	63	0.44	63	0.12	-0.2	63	63
234	13	75	92	1.0	89	0.4	92	0.1375	-0.2	92	92

mitted from the patient (sender) to the doctor/medical server (receiver) without using any compression algorithms. At present, this mode of transmission is performed by existing telecardiology applications [Lee et al., 2007]. It is evident from Table 5.4,  $t_{orig}$ , the time required for ECG file transmission, is significantly high, when uncompressed ECG files  $L_{orig}$  are transmitted on a bandwidth,  $B$  of 256 kbps. Here,  $t_{orig} = L_{orig}/B$ .

ECG HR detection was performed on HP iPAQ h6365 Smart Phone with Amplitude based technique (ABT), which is faster than most of the existing HR detection method. Hence, we used ABT to determine  $t_{HR}$ , the time to calculate HR (i.e. beats). Obviously, the total time for diagnosis  $T_{orig}$  is the total time of transmission  $t_{orig}$  and HR detection ( $t_{HR}$ ).

In scenario 1, since uncompressed ECG transmission leads to longer transmission time, it is obvious to use ECG compression algorithms. Therefore, to reduce the transmission time,

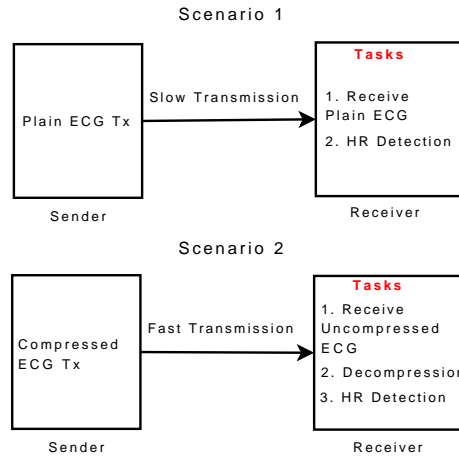


Figure 5.13: Two Different Scenarios of a Mobile Phone based Wireless Telecardiology System

ECG files are compressed (lossless) with encoding schemes and then transmitted. As seen from Table 1, scenario 2, this action minimized the transmission delay,  $T_{comp}$ .

In scenario 2, transmission time,  $t_{comp} = L_{comp}/B$ , where  $L_{comp}$  is the size of the compressed ECG. Even though the compressed ECG transmission time ( $t_{comp}$ ) is minimal, the receiver node (doctor's mobile phone or medical server) requires decompressing the data, before performing HR detection tasks. This added delay of decompression time,  $t_{decomp}$  measured on same HP iPAQ h6365 Smart Phone platform increases the overall total delay,  $T_{comp}$ . Despite this, scenario 2 is a better choice than scenario 1, because ECG compression has other serious advantages like allowing more ECG data transmission on limited telecommunication bandwidth, and larger storage of ECG signals on medical repositories (within medical server) [Kim et al., 2006].

With our implementation on the same platform, HR calculation times  $t_{pHR}$  were slightly higher than the times taken by ABT based HR calculation. The total times  $T_{HRest}$  needed for transmission as well as the HR estimation (0.005 sec. on an average) by algorithm 1

were substantially lesser than  $T_{orig}$  in scenario 1 (6.72 times) and  $T_{comp}$  in scenario 2 (15.311 times). This faster transmission is possible because algorithm 1 does not need to read the compressed ECG, as explained earlier. Similarly,  $T_{HRcal}$ , which denotes the combined time for compressed ECG transmission ( $t_{comp}$ ) and HR calculation by algorithm 2 was also less than  $T_{orig}$  in scenario 1 (1.249 times approx.) and  $T_{comp}$  in scenario 2 (2.845 times approx.). It should be noted that for this simulated experimentation, we have chosen HTTP on mobile platform for the sake of consistency in transmission time, which is not guaranteed on SMS and MMS based text messaging system. However, the beauty of the system lies in the fact that ECG analysis can be performed even without decompression of the compressed ECG segments. As we have seen that the decompression time on a doctor's mobile phone could be significant, our proposed direct-method on compressed ECG will be highly advantageous in patient wellness monitoring system where a doctor has to read and diagnose from compressed ECG signals of several patients allocated to him.

### 5.2.3 Intelligent Approach

Intelligent methods involve usage of subset selection, clustering (e.g. K-Means, Expectation Maximization etc.), principal component analysis (PCA), neural network etc. on compressed ECG [Sufi and Khalil, 2009a; Ibaida et al., 2009].

In [Sufi and Khalil, 2009a], the frequency of the different characters used for encoding (compressing) the ECG was counted first. Since there were about 157 characters (including the numbers), using all these characters as attributes for clustering will result in misclassification. Therefore, an attribute selection was performed, before clustering. The attribute

Table 5.4: Delay Involved in Different Telecardiology Scenarios. All the values of times are in seconds. The ECG Segments collected are for the duration of 1 minute (21600 samples/ECG segment).

ECG Segment	Scenario 1				Scenario 2				Proposed Methods		
	$L_{orig}$	$t_{orig}$	$t_{HR}$	$T_{orig}$	$L_{comp}$	$t_{comp}$	$t_{decomp}$	$T_{comp}$	$t_{pHR}$	$T_{HRest}$	$T_{HRcal}$
1	172197	5.255	5	10.26	45152	1.378	16	22.378	7	1.383	8.378
2	171033	5.219	4	9.219	44632	1.362	15	20.362	6	1.367	7.362
3	170912	5.215	4	9.215	45203	1.379	16	21.379	5	1.384	6.379
4	169280	5.166	4	9.166	43644	1.332	15	20.332	5	1.337	6.332
5	171214	5.225	4	9.225	44608	1.361	16	21.361	6	1.366	7.361
6	171367	5.229	4	9.229	46163	1.408	16	21.409	8	1.413	9.409
7	170549	5.204	4	9.204	46454	1.417	16	21.418	8	1.422	9.417
8	168640	5.146	4	9.146	44973	1.372	15	20.372	5	1.377	6.372
9	170355	5.198	4	9.198	43804	1.337	15	20.337	5	1.342	6.337
10	168208	5.133	3	8.133	44628	1.362	16	20.362	5	1.367	6.362
11	169048	5.158	4	9.158	44358	1.353	16	21.354	6	1.358	7.354
12	170184	5.193	4	9.193	42478	1.296	15	20.296	6	1.301	7.296

selection mechanism identifies few key attributes (or encoding character) responsible for distinguishing a normal ECG segment (compressed) from an abnormal ECG segment (compressed). Expectation Maximization (EM) is our favourite (over K-Means clustering) for identifying abnormal ECG packets in compressed form. However, K-Means algorithms are easier to be implemented on mobile platform.

In [Ibaida et al., 2009], PCA was used first to identify the principal components from the 157 frequency counts for all the encoded characters (i.e. characters used for compressing / encoding the ECG). Then, using the few principal components a linear neural network (NN) was trained. When the trained neural network was tested with a test set, the trained system could correctly identify abnormality directly from compressed ECG, without decompressing them. Implementing this system on mobile and embedded devices, require proper

optimization of coding, since both PCA and NN are computational intensive.

Compressed Electrocardiography (ECG) is being used in modern telecardiology applications for faster and efficient transmission. However, conventional ECG diagnosis algorithms require the compressed ECG to be decompressed before diagnosis can be applied. This added step of decompression before performing diagnosis for every ECG packets introduces undesirable delays, which can have severe impact on the longevity of the patient. In this section, we first used an attribute selection method that selects only a few features from the compressed ECG. Then we used Expected Maximization (EM) clustering techniques to create normal and abnormal ECG clusters. 20 different segments (13 normal and 7 abnormal) of compressed ECG were tested with 100 % success on our model. Apart from automatic clustering of normal and abnormal compressed ECG segments, this section presents an algorithm to identify initiation of abnormality. Therefore, emergency personnel can be contacted for rescue mission, within the earliest possible time. This innovative technique based on data mining of compressed ECGs attributes, enables faster identification of cardiac abnormalities resulting in an efficient telecardiology diagnosis system.

CVD being the number one killer of the modern era, researchers are providing wireless cardiovascular monitoring facility to save lives [Lee et al., 2007; Hung and Zhang, 2003; Blount et. al., 2007]. As ECG signal are enormous in size [Sufi et al., 2008c], usage of compression technology makes the whole tele-cardiology faster and efficient [Kim et al., 2006; Alesanco et al., 2006; Istepanian and Petrosian, 2000]. A faster solution is of crucial importance for diagnosis and treatment of CVD, as delay of every second counts towards a patient's mortality [Luca et al., 2004; Bradley et al., 2006; Otsuka et al., 2009; Sillesen et al.,

2008; Ortolani et al., 2007]. Even though ECG compression enables faster transmission, it introduces a slight delay as the compressed ECG needs to be decompressed before performing any diagnosis. To mitigate this delay, direct methods on compressed ECG have successfully detected few CVD anomalies directly from the compressed ECG (i.e. without decompressing them). Therefore, a completely new direction of research in CVD diagnosis from compressed ECG is established, that establishes the basis for a fast, secure and efficient telecardiology solution.

However, the mechanisms of detecting cardiac abnormality from compressed ECG presented in "direct method on compressed ECG" employ a rule based algorithm for detection of a particular disease. In order to identify all the cardiac abnormalities, direct method on compressed ECG, requires hundreds of complex algorithms to be integrated under one computationally hungry system. Maintaining and updating such a system for every new abnormality is intrinsically complex.

This introduces the problem of finding a simple and fast solution towards heart abnormality detection from compressed ECG that raises alert to the cardiac specialist as soon as a cardiac abnormality is detected.

In this section, we present a simple but efficient Data Mining based solution that detects an abnormality from the compressed ECG. This technique can be placed within a wireless monitoring facility to alert the emergency personnel in an event of cardiac abnormality of a subscribed patient.

As seen from Fig. 5.14, patient is attached with a portable ECG acquisition device, which collects ECG signal from the patient's body and transmits ECG packets to the mobile

phone via Bluetooth, Wifi, Near Field Communication (NFC) or Zigbee protocol. Mobile phone then compresses and encrypts the ECG packets and forwards them to the hospital or monitoring services via HTTP or MMS. The monitoring services executes a background monitoring agent implementing Data Mining techniques.

However, for this section we are adding a data mining module (situated in the hospital) for identification of diseases from compressed ECG sent by the patient, using clustering techniques. These data mining techniques use the knowledge of what is normal and what is abnormal from the monitored patient's ECG. The input and output to the mining agent are the compressed ECG and a boolean type denoting abnormality, respectively. Therefore, for this telemonitoring solution, if the compressed ECG is derived from a normal ECG, output of the data mining agent would be negative. In case of abnormal ECG signal from the patient, the agent will output positive detection, signalling abnormality and alert mechanism would be activated in such a case.

### **Architecture of the Proposed Disease Identification System**

In remote telemonitoring, massive amount of ECG data is transferred [Sufi et al., 2008c], and therefore, adoption of specialized compression technology (as demonstrated in Chapter 2) is often required. Our ECG compression technique uses the encoding function  $\epsilon(\cdot)$  that transforms the ECG signal,  $X_n$  to a compressed ECG,  $C_r$  (Eq. 5.12). The lossless nature of our ECG compression technique ensures that ECG features set,  $F$  (a subset of ECG signal  $X_n$  as shown in Eq. 5.13) also exists within the encoded (or compressed) ECG  $C_r$  (Eq. 5.14). New algorithm can be designed to reveal these encoded ECG feature set for CVD diagnosis



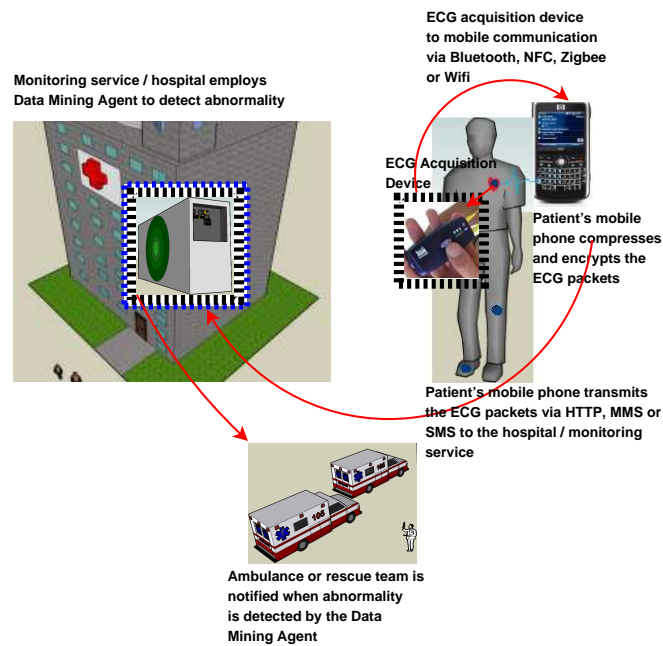


Figure 5.14: Architecture of the Data Mining based Compressed ECG Diagnosis System

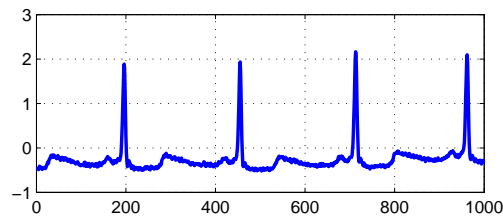


Figure 5.15: A normal ECG Segment of a Patient (a Random CU1 Entry of MIT BiH CU Ventricular Tachyarrythmia Database)

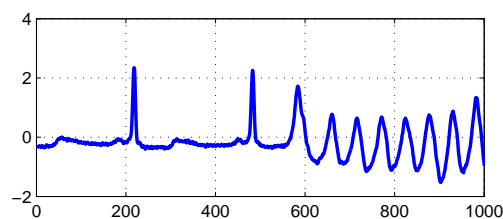


Figure 5.16: Initiation of Abnormality (Ventricular Tachyarrythmia) with the ECG Segment for CU1)

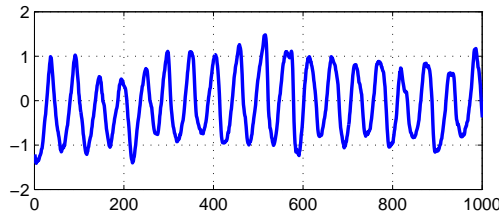


Figure 5.17: An Abnormal (Ventricular Tachycardia) ECG Segment of a Patient (CU1)



Figure 5.18: Compressed ECG for Fig. 5.15 (Normal ECG), Fig. 5.16 (Normal and Abnormal) and 5.17 (Abnormal ECG)

directly from the compressed ECG.

As an example, Figure 5.15 shows a normal ECG segment for Entry ID CU1 of CU Ventricular Tachyarrhythmia database [Phy, Accessed 2009]. Figure 5.16 demonstrates the initiation of abnormality (i.e. Ventricular Tachyarrhythmia) for that particular patient. Lastly, Figure 5.17 depicts a complete episode of Ventricular Tachyarrhythmia for the same patient. Figure 5.18 shows the compressed ECG (i.e. compressed using our specialised ECG compression algorithm) of Fig. 5.15 - 5.17. Equation 5.12 represents the fact that Fig. 5.18 preserve the ECG features of Fig. 5.15 - 5.17. Within this section, our proposed idea is to harness data mining routines for efficient detection of CVD anomalies (i.e. Cardiac Abnormality) directly from compressed ECG (e.g. the compressed ECG shown in Fig. 5.18).

$$\epsilon(X_n) = C_r \quad (5.12)$$

$$F \subset X_n \quad (5.13)$$

$$F \subset C_r \quad (5.14)$$

During the compression process, 148 characters and numeric values (0 - 9) are used to encode the plain text ECG signal, as seen in Fig. 5.19 (ECG compression is performed inside patient's mobile phone). The data mining agent (DMA) of the hospital (Fig. 5.14) needs to be trained with normal and abnormal ECG (from compressed ECG) of patients. After being

trained, the DMA can be tested for irregularities (abnormal ECG). Our proposed algorithm (Algorithm 5), instantly identifies abnormal ECG segments (directly from the compressed ECG).

### 5.2.4 Training of the Proposed Model

During this training phase, the proposed model learns what is normal ECG and what is abnormal ECG. Figure 5.20 shows the main stages of this learning process from compressed ECG.

**Characters**

```
@f$¥èéùìòçøðÀà_^{}[-~]|€£æßÉ
!#%&()*+,-./:;<?i$zãõñuàAAA
AAÈÈÈIIIIÏÐÑÒÓÔÕÖÙÚÛÜÝÞþáâãçê
éíîïðóôõúýabcdefghijklmnopq
rstuvwxyzABCDEFGHIJKLMNOPS
TUVWXYZ\
```

**Numeric Sub Groups**

```
0-50
50-100
100-150
150-200
200-250
250-300
300-350
350-400
400-500
```

*Figure 5.19: 157 Characters and Numeric Sub Groups (Attributes) used for Generating Compressed ECG (from Plian ECG Signal). Details of this Character Substitution based Compression Techniques have been Described in Chapter 2*

### Character Frequency Calculation

As shown in Fig. 5.20, from the compressed ECG, the frequency of each encoded characters is computed first. There are about 148 characters and 9 numeric subgroups for which the

frequencies are generated (Fig. 5.19). The frequency of these 157 character (and numeric sub groups) are utilized as the attributes for clustering. However, 157 attributes are too many for generating clusters (normal and abnormal ECG). Therefore, the attribute subset selection process is necessary. Using proven techniques, we first select characters from the compressed ECG that are mainly responsible for identifying diseases. Then, based on the selected characters (or attributes) classification of abnormality and normality is possible.

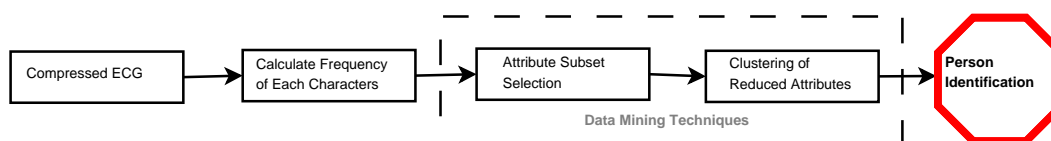


Figure 5.20: Step by step procedure of the proposed cardiac abnormality detection technique

### Attribute subset selection

Data pre-processing using attribute selection is an important step in data mining, since a large number of attributes often lead to poor learning due to untenably large combinatorial search space for the solution [Han and Kamber, 2006]. The goal of feature subset selection is to (a) reduce the dimensionality of the data to be analysed, (b) to speed up execution of learning algorithms, (c) improve performance of data mining techniques including learning time and predictive accuracy, (d) improve the comprehensibility of the output. Recent studies have shown that attribute subset selection helps improve the performance of clustering algorithms with reduced attributes [Talavera, 1999a;b; Sufi and Khalil, 2009c]. In this section, we have adapted for use with continuous ECG signals, a correlation based feature subset selection technique [Hall, 1999; Sufi and Khalil, 2009c], which outperforms other feature selection algorithms, such as ReliefF [Kira and Rendell, 1992] and RReliefF [Robnik-Sikonja

and Kononenko, 1997]. The attribute selection is based on an attribute's relative utility with regards to the predicted class as well as taking into consideration its correlation with other attributes in the subset. The utility of an attribute can be represented using the Pearson's co-efficient for correlation, where the variables are standardized as in Eqs. 5.15 and 5.16.

$$\overline{r_{xy}} = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{(n - 1)\sigma_x\sigma_y} \quad (5.15)$$

$$U_S = \frac{C\overline{r_{ap}}}{(C + C(C - 1)\overline{r_{aa}})^{\frac{1}{2}}} \quad (5.16)$$

where  $x_i$  and  $y_i$  are sample mean calculated from the data,  $\sigma_x$  and  $\sigma_y$  are the standard deviations,  $a, \acute{a} \in S, C \leftarrow |S|, \overline{r_{xy}} \leftarrow \text{Average correlation}$  between features  $x$  and  $y$ . For a subset  $S$  of  $C$  features, the utility function calculates how much the features  $(a, \acute{a})$  are related  $\overline{r_{ap}}$  to the predicted class  $p$ , while being less related to each other  $\overline{r_{aa}}$ . The utility function reduces the effect of irrelevant attributes as they are less correlated with the predicted class. It also discards redundant attributes as they are highly correlated with each other.

We used a greedy best first algorithm to search through the candidate subsets for a locally optimal solution. The algorithm initiates with an empty subset, adding one attribute at a time and estimating the utility function, to determine the correlation of the subset with the predicted class. The next attribute is added as long as the utility value does not decline for the best subset. If there is a decrease then the algorithm selects the next best subset and commences adding attributes to it. In some datasets where there are groups of features that are locally predictive to the predicted class, we investigate the attributes that were

initially discarded while building the best subset. In this case, after the best subset has been generated, the algorithm investigates the rejected list of attributes one-by-one and evaluates its correlation to the predicted class against the average correlation to the subset. If its correlation to the class is greater than its correlation with the attribute subset, signalling a stronger attraction to the class than the subset, then the attribute is incorporated in the subset.

### **Automatic learning of normal and abnormal patterns using clustering of compressed ECG features**

Using the smaller subset of attributes we can now produce a cluster from the normal compressed ECG patterns. This cluster of normal patterns would serve as the benchmark test against future ECG sent from the observed client. Under normal circumstances any incoming ECG would closely match the stored cluster. However, if there is any abnormality then the clustering algorithm would create a different cluster from the abnormal ECG. This will generate an alarm and require urgent attention of a physician or a cardiologist. It should be noted that the procedure given in this section works solely on the compressed ECG character frequency, and does not even require decompression, which would take valuable extra time from a patient's life.

The aim of clustering is to group a given set of objects so that similar objects (also known as cases, instances or patterns) are grouped together and dissimilar objects are kept apart. Although there are many different techniques to build multi-dimensional clusters [Mahmood et al., 2008], we have chosen a statistical clustering technique called Expectation

Maximization (EM) [Han and Kamber, 2006] to cluster compressed ECG data, since it can be used to find the correct number of clusters automatically. Assuming two clusters A and B, representing normal and abnormal class of ECG, we describe the steps for EM clustering for two clusters:

1. Choose model parameters mean  $\mu$ , standard deviation  $\sigma$  and probability of clusters  $p$  arbitrarily for Clusters A and B
2. For each iteration  $j$ , calculate the probability that instance  $I$  belongs to clusters  $A$  and  $B$ :

$$P(A|I) = \frac{p_A^j P^j(I|A)}{P^j(I)}, P(B|I) = \frac{p_B^j P^j(I|B)}{P^j(I)} \quad (5.17)$$

The probability of  $P(I|A)$  can be modelled using any distribution function. For the commonly used Gaussian distribution that we have adopted in this section, it can be given by

$$P(I|A) = \frac{1}{\sqrt{(2\pi)\sigma_A}} \exp \frac{-(I-\mu_A)^2}{2\sigma^2} \quad (5.18)$$



3. Update the mixture parameters on the basis of the new estimates:

$$P_B^{j+1} = \frac{\sum_I P(A|I)}{n}, P_B^{j+1} = \frac{\sum_I P(B|I)}{n} \quad (5.19)$$

$$\mu_A^{j+1} = \frac{\sum_I I \times P(A|I)}{\sum_I P(A|I)}, \mu_B^{j+1} = \frac{\sum_I I \times P(B|I)}{\sum_I P(B|I)} \quad (5.20)$$

$$\sigma_A^{j+1} = \frac{\sum_I P(A|I)(I - \mu_A^{j+1})^2}{\sum_I P(A|I)}, \quad (5.21)$$

$$\sigma_B^{j+1} = \frac{\sum_I P(B|I)(I - \mu_B^{j+1})^2}{\sum_I P(B|I)} \quad (5.22)$$

4. Calculate the log likelihood value  $E_j = \sum_I \log(P^j(I))$ . Consider a fixed stopping criterion  $\epsilon$ , then if  $|E_j E_{j+i}| \leq \epsilon$ , then stop; else set  $j = j + 1$ .

EM can decide how many clusters to create by cross validation (as is the case in the present study), or it may be specified apriori (normal and abnormal clusters). In the scenario of Fig. 5.14, the patient continuously sends the compressed ECG information to the hospital, which clusters the new information and checks to see if there are two clearly segregated clusters. In cases where the compressed ECG falls under abnormal cluster (or inclines towards abnormal cluster), as shown in Fig. 5.24, abnormality is detected. If such an abnormality is observed then an immediate alarm is raised, since the ECG pattern has been found to be significantly different from normal patterns. In our experiments, the EM algorithm has been successful in isolating the normal and abnormal compressed ECG with remarkable accuracy (100%) using the 20 ECG segment dataset.

### 5.2.5 Instant Abnormality Detection from Compressed ECG

Once the proposed model is trained, we know the cluster centers (or means) for all the selected attributes (for the classes). With this knowledge, whenever a new compressed ECG is sent by the patient, the DMA calculates the frequency of selected characters (selected attribute in training stage). These inputs (attribute values of the instance) are fed along with the cluster centers to Algorithm 5, which determines initialization of abnormality.

During an initialization of abnormality, we expect the compressed ECG packet to contain both normal and abnormal ECG. Therefore, for these initialization of abnormality packets, distances from normal cluster centers (for the selected attributes) will start to increase. Abnormality can be signalled, once the distance between the instance (initialization ECG packet) and normal cluster mean goes beyond a threshold value. After the detection of abnormality initialization, the emergency personnel can be contacted for the rescue of the patient (Fig. 5.14).

## 5.3 Results and Discussion

Figure 5.21 shows 20 different segments of ECG for CU1 entry of CU Ventricular Arrhythmia database ([Phy, Accessed 2009]) in a matrix format. Sub-figures 1 to 3 ([1,1], [1,2] and [1,3]) of Fig. 5.21 are normal ECG segments. Sub-figure 4 or [1,4] shows initiation of ventricular arrhythmia. Sub figures 5 to 10 represent continual cardiac abnormality (ventricular tachyarrhythmia episode). The rest of the sub figures of Fig. 5.21 show normal ECG segments for patient CU1. It should be noted that for our proposed architecture (in Fig. 5.14), plain ECG (as in Fig. 5.21) is not viewed anywhere. Figure 5.21 only serves the purpose of

---

Algorithm 5: Detection of the Abnormality Initialization

---

//Notation Description:

//Input: Attribute values for all the instances

//Input: Cluster means of the 2 clusters for all the attributes

//Output: The most equidistant instance

---

### Step 1

Create distance vector,  $A_j$  and  $B_j$  for

Cluster 1 and 2, where  $j$  is the number of instances

$$A_j = \sqrt{\sum_{i=1}^I (f_i^j - C_i^1)^2}$$

$$B_j = \sqrt{\sum_{i=1}^I (f_i^j - C_i^2)^2}$$

here,  $f_i$  is the attribute value vector for all I

attributes and  $C_i^1$  and  $C_i^2$  are the centroid

vectors of cluster means 1 and 2 (normal & abnormal)

and  $i = 1, 2, 3, \dots, I$  is the number of attributes

### Step 2

Symmetry metric is generated by normalizing the  
difference in distance vectors for the 2 clusters

$$S_j = \frac{|A_j - B_j|}{\text{Max}(A_j, B_j)}$$

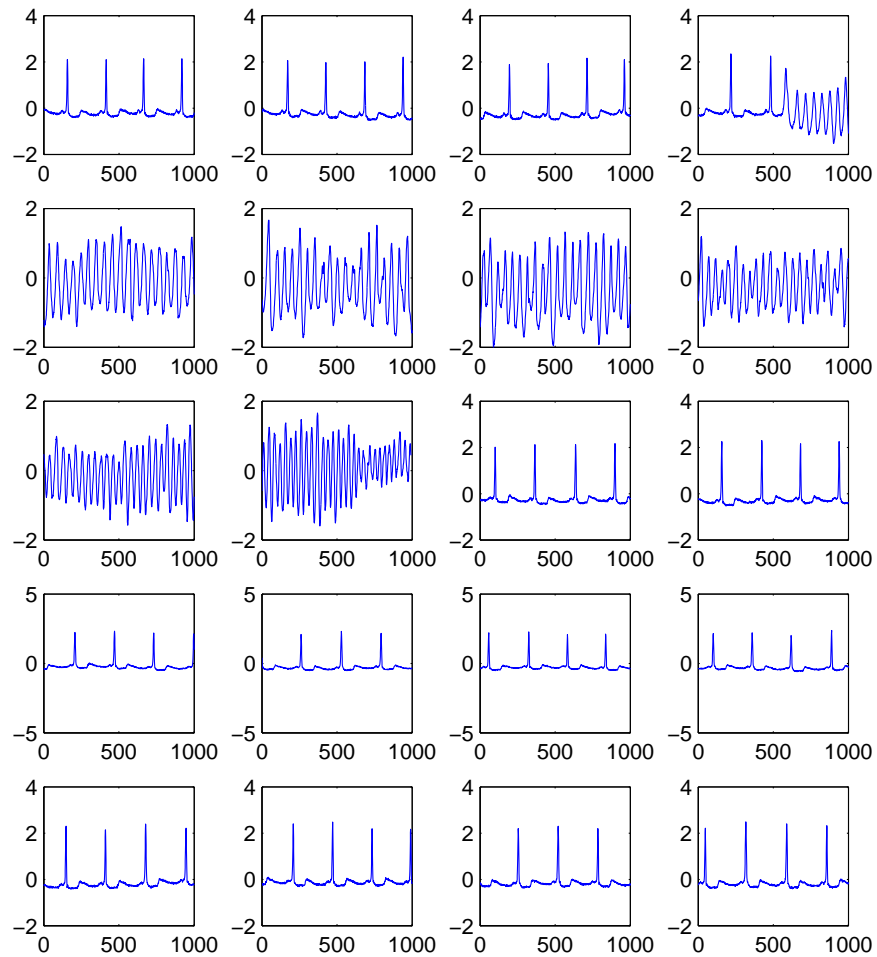
### Step 3

The most equidistant instance,  $R$  has the lowest value of  $S_j$

$$S_R = \text{Min}(S_j)$$


---

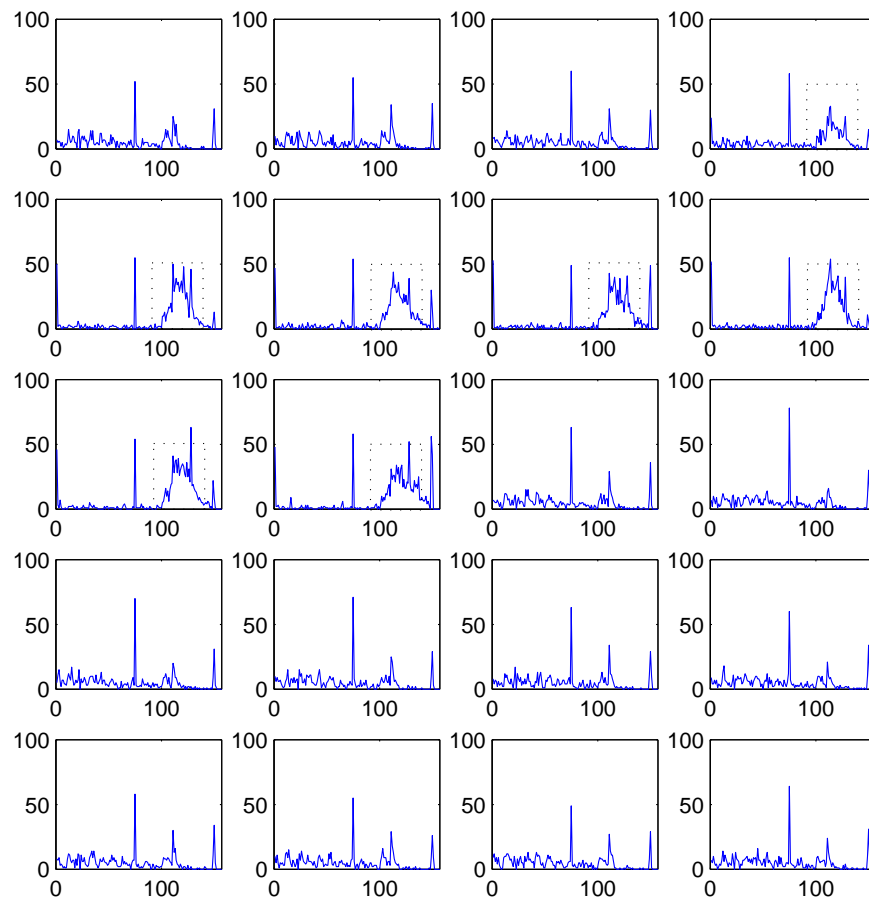
understanding the concept behind this section.



*Figure 5.21: 20 Randomly Selected ECG Segments for CU1 Entry (from CU Ventricular Tachyarrhythmia - MIT BIH)*

As shown in Fig. 5.20, we only receive compressed ECG from which the frequencies for all attributes (Fig. 5.19) are calculated. After calculating frequencies of the 157 attributes from the compressed ECGs of Fig. 5.21, we can observe that certain group of characters

have different frequency bands for normal and abnormal ECGs. Figure 5.22 illustrates the fact that sub figures 3 to 10 have notably higher frequencies for attributes 115 to 131 (for character set  $\{[t-z], [A-J]\}$ ). However, these sub figures (3 to 10) actually correspond to abnormal ECG. Therefore, Fig. 5.22 represents the fact that certain compressed character frequencies behave differently for abnormal ECG.



*Figure 5.22: Frequency Distribution of the 20 Randomly Selected ECG Segments for CU1 Entry (of Fig. 5.21). Boxed Region Shows high Frequencies of Attribute 115 to 131 Denoting Abnormality from the Compressed ECG.*

However, rather than manual inspection of the characters responsible to signal abnormality, an accurate and automated attribute selection procedure is highly desirable. Our attribute selection process on 20 different instances provides us 48 key characters or attributes that are shown in the left column of Table 5.5, Table 5.6, Table 5.7 and Table 5.8. Based on these 48 attributes, we generated cluster with previously described EM methodology. EM generates 2 clusters with 100% accuracy when the clusters are compared (or cross-validated) to the known class (abnormal ECG segment and normal ECG segment). It is worth mentioning that EM was not informed about the number of clusters (i.e. 2). The log likelihood measured by EM, after creation of 2 clusters based on the 48 selected attributes, is -100.27906. Table 5.5 and 5.6 show the frequency of these characters on the 13 different instances for normal ECG. On the other hand, Table 5.7 and Table 5.8 show 7 instances of abnormalities. For all the tables, cluster means or centers (right most columns for Table 5.5, 5.6, 5.7 and 5.8) are distant. Also, for normal and abnormal cases, the respective attributes show affinity towards their corresponding class means. Figure 5.23 shows the difference in normal and abnormal ECGs for the selected 48 attributes. Unlike Fig. 5.22, where 16 characters show visual distinction (from 115 to 131), Fig. 5.23 shows clear distinction of 48 automatically selected attributes.

This study was the first demonstrated in [Sufi and Khalil, 2009c] and enhanced in [Sufi and Khalil, 2011b; Sufi et al., 2011] to show the feasibility of an automated alert mechanism. This alert mechanism was based on data mining techniques and compressed ECG, designed to save lives of monitored CVD patients.

Now that we can observe two distinct clusters for normal and abnormal compressed ECG

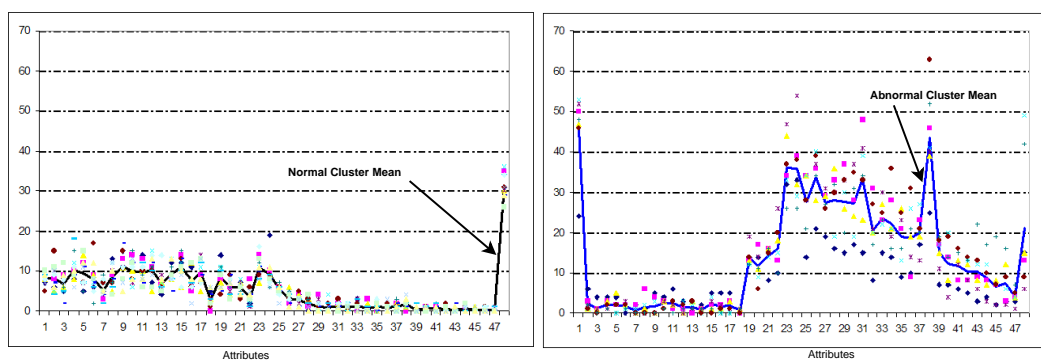


Figure 5.23: Normal and abnormal cluster means

segments, the question of belonging arises for the compressed ECG segments that contain half normal ECG and half abnormal ECG. For example, this situation can be observed for the case of 4th sub figure of Fig. 5.21 (row 1, column 4). This initialization of abnormality is also depicted in Fig. 5.16. It should be mentioned again that for the sake of clarity of this chapter, original ECG segments are shown in Figs. 5.16 and 5.21. However, in real monitoring scenario, only compressed ECGs are dealt by the patient and the DM agent (in Fig. 5.14). For this initialization of abnormality case (Fig. 5.16), we logically expect it to be equidistant from the two clusters, as this particular segment contains both normal and abnormal ECG. To represent this fact, in a two dimensional coordinate is not straight forward, as we are dealing with 48 attributes and each attribute provides individual decision of belonging towards a particular cluster.

To represent the fact that compressed ECG packets containing both normal and abnormal ECG are nearly equidistant from both the clusters, in two dimensional coordinate, we define the concept of symmetricity of instances in a bi-class clustering. An instance is said to be symmetric with respect to a bi-class clustering, when the location of the instance is nearly

Table 5.5: Selected Characters (First Half Attributes) and their Respective Frequencies in Compressed ECGs (Normal) for 13 Different Instances

At.	N1	N2	N3	N4	N5	N6	N7	N8	N9	N10	N11	N12	N13	CCtr
@	7	10	8	7	7	5	10	8	9	8	10	9	7	8.0769
\$	6	8	5	5	10	15	9	7	4	9	11	6	10	8.0769
Ø	5	9	6	5	8	8	6	2	5	8	12	9	7	6.9231
Å	8	10	8	12	9	9	15	9	18	11	9	10	6	10.3077
å	5	12	14	11	7	7	5	11	7	7	15	12	11	9.5385
-	6	9	9	7	8	17	2	7	6	5	8	12	8	8
[	5	3	5	7	4	7	9	4	2	8	5	5	4	5.2308
]	13	9	5	8	10	7	7	8	6	12	4	10	12	8.5385
	15	13	11	11	11	15	8	17	11	11	8	5	7	11
Æ	8	14	10	6	7	8	15	12	8	11	12	8	13	10.1538
&	14	13	10	10	8	10	9	7	12	11	6	8	8	9.6923
(	7	11	5	15	11	10	11	12	10	14	6	13	9	10.3077
*	4	7	7	7	9	6	5	6	6	14	5	8	6	6.9231
:	12	8	8	13	8	8	11	5	8	8	9	13	8	9.1538
;	12	14	6	12	10	13	15	13	10	6	11	10	9	10.8462
ü	11	5	12	7	7	6	8	6	7	6	12	8	2	7.4615
Á	9	9	5	11	14	7	8	9	12	7	13	8	13	9.6154
Ë	5	0	3	3	3	1	2	4	3	2	2	6	6	3.0769
k	14	8	7	11	9	4	11	5	10	9	9	6	6	8.3846
l	9	6	4	4	5	9	6	9	4	8	3	7	7	6.2308
m	7	6	7	8	7	3	5	4	4	6	6	4	7	5.6923
o	2	8	4	2	1	6	3	4	1	3	3	4	5	3.5385
r	10	14	7	11	9	9	12	11	8	16	13	11	8	10.6923
s	19	10	9	9	9	9	6	8	9	7	8	11	6	9.2308

equidistant from both the cluster centroids.

Algorithm 5 basically determines the instance, which is equidistant from both the classes.

In first step, algorithm 5 calculates the cluster distances for all the 20 instances of the example case (i.e. distance from normal cluster,  $A_j$  and distance from abnormal cluster,  $B_j$ ). For this



Table 5.6: Selected Characters (Last Half Attributes) and their Respective Frequencies in Compressed ECGs (Normal) for 13 Different Instances

At.	N1	N2	N3	N4	N5	N6	N7	N8	N9	N10	N11	N12	N13	CCtr
t	6	6	6	5	6	6	7	5	6	4	5	6	2	5.3846
u	3	2	6	3	1	3	5	2	4	3	4	1	5	3.2308
v	4	4	4	1	2	5	3	1	3	1	3	1	3	2.6923
w	0	1	3	1	2	3	3	2	2	4	4	0	1	2
x	0	4	2	0	3	1	0	1	0	2	0	0	2	1.1538
y	2	0	0	4	0	2	0	1	2	0	0	0	1	0.9231
z	0	2	2	1	1	3	0	1	2	2	0	1	1	1.2308
A	0	1	1	2	0	0	1	2	0	2	1	0	1	0.8462
B	3	0	2	2	3	2	0	1	3	1	1	0	0	1.3846
C	1	3	2	0	0	0	0	0	1	0	0	0	0	0.5385
D	1	0	0	2	2	2	0	0	1	3	2	1	0	1.0769
E	0	1	2	0	0	2	0	1	1	0	1	0	3	0.8462
F	1	2	2	0	1	1	3	2	1	0	0	1	0	1.0769
G	1	0	1	1	2	2	2	1	2	2	2	3	4	1.7692
H	0	0	0	0	0	0	0	0	2	0	0	1	0	0.2308
I	0	1	0	1	0	1	0	1	1	0	0	1	1	0.5385
J	0	1	0	0	0	0	2	1	2	0	0	1	0	0.5385
K	0	1	1	0	0	2	0	0	0	0	1	0	0	0.3846
L	0	0	0	0	0	0	0	2	0	0	0	1	0	0.2308
M	0	1	0	1	0	1	2	0	0	1	2	0	1	0.6923
N	0	0	1	0	0	0	0	0	0	0	0	0	1	0.1538
O	0	0	0	0	0	1	0	0	1	1	0	0	0	0.2308
R	0	0	0	1	1	0	0	0	1	0	0	0	1	0.3077
50-100	31	35	30	36	30	31	29	29	34	34	26	29	31	31.1538

examples case, cardinality of  $A_j$  and  $B_j$  is 20 ( $|A_j| = |B_j| = 20$ ).

Using step 2 of Algorithm 5, we can also ascertain our proposed symmetricity metric,  $S_j$  for the 20 instances of our example case (as seen from Table 5.9). We can clearly see that the most equidistant case,  $R$  is the 4th (4th subplot of Fig. 5.21 or Fig. 5.16) case. Therefore,

Table 5.7: Selected Characters (First Half Attributes) and their Respective Frequencies in Compressed ECGs (abnormal) for 7 Different Instances

Att.	An1	An2	An3	An 4	An5	An6	An7	CCtr
@	24	50	47	53	52	46	48	45.7143
\$	6	3	1	1	2	1	2	2.2857
Ø	4	1	1	1	1	0	0	1.1429
Å	4	3	3	1	1	2	1	2.1429
å	4	2	5	0	2	2	0	2.1429
-	0	2	2	1	3	2	1	1.5714
[	2	2	0	1	0	0	0	0.7143
]	1	6	1	2	0	0	0	1.4286
	5	4	0	3	0	0	0	1.7143
Æ	4	3	3	3	3	1	1	2.5714
&	6	1	2	3	2	3	0	2.4286
(	3	1	0	3	0	2	1	1.4286
*	0	0	3	2	1	3	1	1.4286
:	2	1	1	0	1	0	1	0.8571
;	5	2	1	4	3	0	1	2.2857
ü	5	2	1	0	2	1	0	1.5714
Á	5	3	3	0	1	1	0	1.8571
Ë	0	0	1	1	1	0	1	0.5714
k	14	13	13	12	19	14	12	13.8571
l	14	17	11	9	14	6	11	11.7143
m	8	16	16	14	15	15	16	14.2857
o	10	13	18	15	26	20	10	16
r	32	34	44	33	47	37	26	36.1429
s	33	39	32	29	54	38	26	35.8571

$R = 4$  as  $S_4 = \text{Min}(S_j)$ , where,  $j = 1, 2, 3, \dots, 20$ .

Algorithm 5 can clearly identify the initialization of abnormality, and as soon as the algorithm detects shifts from normal cluster, it can notify the emergency personnel for assistance of the monitored patient. This section serves as a proof of concept to show that

Table 5.8: Selected Characters (Last Half Attributes) and their Respective Frequencies in Compressed ECGs (abnormal) for 7 Different Instances

Att.	An1	An2	An3	An 4	An5	An6	An7	Cctr
t	14	34	34	34	28	28	21	27.5714
u	21	36	28	40	37	39	34	33.5714
v	19	29	29	31	31	26	27	27.4286
w	16	33	36	19	30	30	32	28
x	15	37	26	30	33	33	20	27.7143
y	17	28	24	19	37	35	31	27.2857
z	15	48	23	39	41	33	34	33.2857
A	8	31	20	20	21	27	17	20.5714
B	15	23	27	22	30	25	23	23.5714
C	14	28	21	21	19	36	16	22.1429
D	9	21	26	13	23	25	16	19
E	10	9	19	26	14	31	21	18.5714
F	17	23	19	27	13	21	20	20
G	25	46	39	41	40	63	52	43.7143
H	7	17	15	17	11	18	19	14.8571
I	7	14	8	20	4	19	14	12.2857
J	6	8	13	12	12	16	15	11.7143
K	5	8	12	13	8	14	13	10.4286
L	3	9	8	12	6	13	22	10.4286
M	4	8	7	12	3	10	17	8.7143
N	2	7	8	2	2	7	19	6.7143
O	3	3	12	6	2	9	16	7.2857
R	3	4	4	4	1	5	7	4
50-100	15	13	15	49	6	9	42	21.2857

cardiac abnormality can be detected directly from the compressed ECG with the application of data mining technique like EM.

Figure 5.24 shows the fact that sub figure 4 of Fig. 5.21 (or Fig. 5.16) is equidistant (being more closer to abnormal cluster) from the 2 clusters (according to Algorithm 1), even

Table 5.9:  $A_j$ ,  $B_j$  and  $S_j$  values for the 20 ECG segments

$$A_j = \{17.30530722, 12.36044732, 13.77612638, \\ 72.26985027, 134.7904569, 120.5433543, \\ 125.0978411, 137.5469333, 144.1012035, \\ 123.8610014, 12.08989901, 9.406054328, \\ 16.00034556, 14.48650607, 12.22903341, \\ 13.18553215, 14.27789403, 15.17882927, \\ 12.32616964, 13.55373225\}$$

$$B_j = \{118.8628916, 118.3491715, 117.4859846, \\ 54.51042274, 29.27631103, 23.41155244, \\ 38.1514297, 37.79026049, 35.32039337, \\ 38.08583448, 121.1030833, 120.3706758, \\ 119.8604513, 119.2606355, 120.2970672, \\ 118.8009722, 119.3707786, 118.8893224, \\ 120.5503405, 120.1616153\}$$

$$S_j = \{0.854409505, 0.895559494, 0.882742385, \\ \mathbf{0.24573771}, 0.782801307, 0.805783134, \\ 0.695027273, 0.725255521, 0.754891753, \\ 0.692511492, 0.900168529, 0.921857593, \\ 0.866508549, 0.878530699, 0.898343046, \\ 0.88901158, 0.880390375, 0.87232807, \\ 0.897750852, 0.887204144\}$$

though it belongs to Abnormal cluster according to EM. Other instances (or compressed ECG segments) are clearly identified as a member of normal or abnormal clusters.

In a conventional wireless telecardiology, compressed ECG is transmitted by the patient and for detection of cardiovascular abnormality and the compressed ECG is decompressed first before applying existing ECG abnormality detection algorithms. The delay generated by *decompression before detection* may cost the longevity of the patient, as cardiac cell damage after an abnormality symptom is irrecoverable [Luca et al., 2004]. Within this chapter, we present an innovative algorithm that detects cardiovascular abnormality directly from the compressed ECG without any delay.

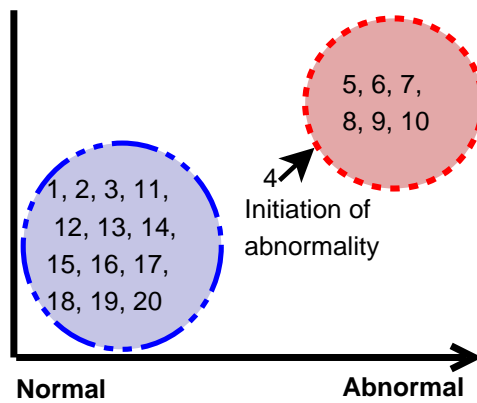


Figure 5.24: Segregation of normal and abnormal ECG (in two different clusters)

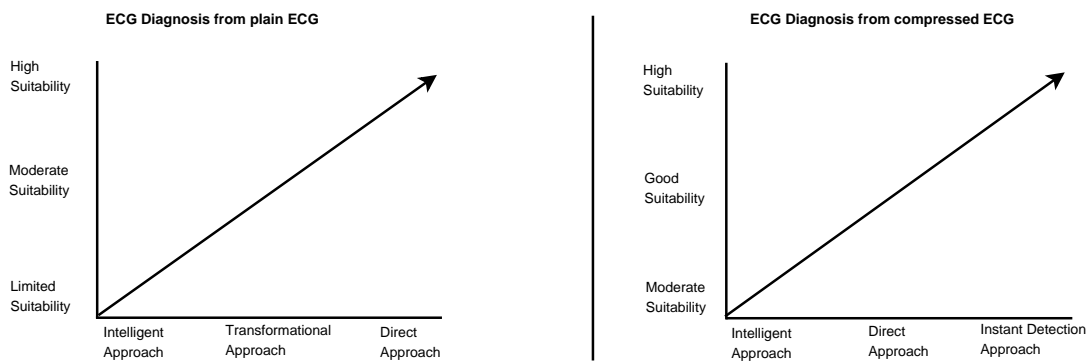


Figure 5.25: Suitability of different algorithms in mobile platform

The abnormality detection algorithm presented in this section is based on an existing attribute selection process and a clustering algorithm (EM). The presented techniques achieved 100% accuracy in identifying cardiac abnormality from compressed ECG, when experimented on CU Ventricular Tachyarrhythmia database [Phy, Accessed 2009]. Finally, figure 5.25 shows the suitability of different detection methods on mobile platform, described within this chapter.

## 5.4 Conclusion

In this chapter, the focus was on mobile phone based faster cardiovascular diagnosis. Faster diagnosis is possible if the ECG file (from where diagnosis is to be performed) lengths are smaller by harnessing specialized ECG compression technology (as compared to larger plain ECG). Since a lossless compression (such as the one in Chapter 2) transforms a larger file into a smaller one, if diagnosis is performed from the smaller compressed file (containing same information in different form), there will be less file input/output operations.

HR estimation algorithm (i.e. instant detection algorithm) was 6.72 times faster than existing algorithms when experimented on our compressed ECG based tele-monitoring system. On the other hand, HR Calculation method (i.e. direct approach on compressed ECG) was 1.249 times faster than existing methods. It should be mentioned that while instant detection algorithm and direct approach on compressed ECG served the purpose of initial assessment and feasibility study, detailed experimentation on detection accuracy was performed after improvement was made with data mining technique. Our experimentation with data mining technique showed that different CVD could be detected with 100% accuracy.

In the next chapter, we will explore another technique of CVD diagnosis that has the potential of executing as fast as diagnosis from compressed ECG (described in this chapter) but suitable for graphical display and visualization on mobile devices. The techniques described in our next chapter can easily be adopted by existing systems not running our ECG compression algorithms.

## Chapter 6

# Cardiod based Diagnosis and Person Identification

In our previous four chapters, we have already answered all the research questions that we posed to ourselves during the beginning of our research. However, the most urgent objective is to identify a patient and provide the patient with healthcare support in case of urgency (such as a heart attack) while reducing any associated delays. The previous chapter on diagnosis from ECG signal was mainly based on compressed ECG, which doesnt have any visual appeal. However, despite all the automations in the area of cardiac anomaly diagnosis, doctors and cardiologists still heavily rely on manual inspection with ECG paper strip. Viewing minutes worth of ECG on limited screen size of mobile phone may take hundreds of clicks for browsing forward (or backward).

While most of ECG diagnosis algorithms ([Hamilton and Tompkins, 1986; Akselrod et al., 2007; Bartolo et al., 2001; Kumar et al., 2007; Clifford et al., 2006; Kusumoto, 2009]) being

designed and tested primarily on PC based environment, mobile phone based cardiovascular abnormality detection algorithm is a very recent area of research [Lee et al., 2007; Hung and Zhang, 2003]. Within this chapter, we present the novel idea of cardioid based ECG abnormality detection and patient authentication mechanism on mobile, handheld and server platform. This cardioid based technique provides fast visualization of several minutes ECG on a single screen of mobile phone. Therefore, the doctors or cardiologists hardly require more than one click to browse through the ECG. Apart from providing faster display on limited screen size, the Cardioid based technique provides very fast diagnosis and authentication with our proposed set of algorithms. Our experimentation results suggest that Cardioid based abnormality detection and patient authentication substantially minimize the delay associated with the treatment of cardiovascular patient.

First, we present the concept of centre of cardioid followed by its application in person identification/authentication. Then, we demonstrate its applicability in faster diagnosis. Both authentication and diagnosis components are the integral part of a Mission Critical Cardiovascular Abnormality Alerting (MCCAA) mechanism designed to provide faster patient care and save precious life. According to our experimentations, the authentication time can be reduced from 30.64 sec. (manual authentication in novice mobile user) to 0.4398 sec. (automated authentication). Our ECG based patient authentication mechanism is several times faster than conventional biometrics like face recognition. The diagnosis time could be improved from several minutes to less than 0.5 sec. (cardioid display on a single screen). Therefore, with our presented mission critical alerting mechanism on wireless devices, minutes worth of tasks can be reduced to seconds, without compromising the accuracy



of authentication and quality of diagnosis.

## 6.1 Motivation

This section provides a general understanding of the medical significance for faster cardiovascular care, which is driving our research in mobile phone based alert mechanism. To delve into the understanding of faster cardiovascular patient care, the concept of Door to Ballooning Time (D2B) and Symptom-Onset-to-Balloon Time can be reviewed.

Door to ballooning refers to the measurement of time for the treatment of ST segment elevation myocardial infraction (STEMI) or acute Myocardial Infraction (MI) [Bradley et al., 2006; Otsuka et al., 2009; Sillesen et al., 2008; Ortolani et al., 2007; Luca et al., 2004]. This is the time between a patient's arrival in the Emergency Department (ED) and balloon angioplasty (or Balloon inflation). Delay in balloon inflation and subsequent insertion of mesh wire to enable free blood flow with the heart, effectively creates an environment where blood gets coagulated and forms blood clot. Formation of blood clot leads to irreversible cardiac cell damages. ACC/AHA guidelines recommend the D2B time less than 90 minutes.

Symptom-Onset-to-Balloon time refers to the time interval between the patient feeling discomfort (cardiac symptom) and catheter guide wire crossing the culprit lesion in the cardiac cathlab. When the patient initially feels a cardiac discomfort identifying possible incident of MI, he/she calls the ambulance. The ambulance then brings the suspected MI affected patient in the ED. The ED personnel then undergo a detailed ECG acquisition of the patient and decide the procedure to be taken. Based on their decision with cardiovascular experts, the patient may be taken to the cathlab. This lengthy process is susceptible to

deteriorate patient's cardiovascular health. To minimize the detrimental effect of this delay, many ambulances are equipped with ECG equipments. Therefore, ECG can be obtained from the patient, while the patient is being transported to the ED. The acquired ECG can then be sent to the ED / Cardiovascular experts within the hospital, prior to patient's encounter to the hospital. Thus, the hospital can take early diagnosis and treatment decision. The hospital can instruct the ambulance personnel, where to take the patient. This process can bypass the patient's admittance in ED and enable urgent patients be directly endured surgery in cathlab. This ambulance to hospital communication can be performed by Fax, Email, MMS, HTTP etc.

The usefulness of this type process is very recently drawn in [Otsuka et al., 2009]. The researchers in [Otsuka et al., 2009] transmitted real-time ECG, vital signs (Blood pressure, heart rate and oxygen saturation) and live video directly from the ambulance to the on duty cardiologist in the hospital. After viewing the ECG trace and diagnosing the possible STEMI, the cardiologist in [Otsuka et al., 2009] can activate the catheterization laboratory. The ambulance to hospital transmission delay was within 10 seconds. The crucial importance of pre-hospital diagnosis is also reported in recent literature [Ortolani et al., 2007].

Researchers in [Luca et al., 2004] have plotted the relationship between ischemic time and 1 year mortality. They have showed that each 30 minutes of delay was associated with a relative risk for 1-year mortality of 1.075 (95% CI 1.008 to 1.15; P=0.041). The conclusion drawn by them [Luca et al., 2004] was simple; all efforts should be made to reduce the total ischemic time.

For the research presented in [Otsuka et al., 2009], a mobile phone connected with an

in-ambulance server was deployed for enabling data transmission between the ambulance and the server. In [Sillesen et al., 2008], usage of mobile phone in diagnosis of heart attack minimized delay in treatment from 94 to 22 minutes. The study in [Sillesen et al., 2008], transmitted 12 lead ECG data to the attending cardiologist's mobile phone. This study [Sillesen et al., 2008], not only make it evident that usage of mobile phone in cardiovascular monitoring provides faster patient care but also it shows that important diagnosis decisions can be made based on the ECG plot drawn on mobile phone's screen.

In fact, taking ECG before the patient's admittance to the hospital significantly reduces the Symptom-Onset-to-Balloon time. Any efforts in minimizing delays associated with patient care impacts in saving patients life [Otsuka et al., 2009; Luca et al., 2004; Sillesen et al., 2008; Ortolani et al., 2007]. However, this process demands significant improvement in terms of minimizing end-to-end delay.

According Chapter 2, the delay associated with ECG data transmission has been reduced drastically with the usage of specialized lossless compression techniques (designed for ECG). Therefore, our recent research activities as demonstrated in Chapter 2 have successfully minimized the delay associated with ECG data transmission. However, existing mobile phone based remote monitoring systems [Blount et. al., 2007] with username and password based authentication mechanism takes 12 ~35 seconds of time, according to our experimentation. As the patient requires manual input of the username and password, these types of solutions (in [Blount et. al., 2007]) are not fruitful for patients having cardiac attacks which subsequently triggers anomaly in regular finger movement. As a result, we came up with an automated solution with ECG based biometric with polynomial distance measurements

(described earlier in Chapter 3). However, generation of polynomial coefficients in mobile devices takes significant amount of time (around 12 seconds).

On the other hand, reducing the delay associated with ECG based authentication is a challenging issue for faster patient care. Existing ECG diagnosis algorithms are mainly based on PC and Servers [Hamilton and Tompkins, 1986; Friesen et al., 1990; Clifford et al., 2006; Bartolo et al., 2001; Kusumoto, 2009; Kumar et al., 2007; Akselrod et al., 2007] and can be classified in three broader categories in terms of complexities.

- Fiducial Technique (e.g. Detection of Wave onset, offset, amplitude, duration, slope etc.) [Hamilton and Tompkins, 1991; Friesen et al., 1990]
- Transformational Techniques (e.g. Wavelet transform, Fourier Transform, Cosine Transform etc.) [Kim et al., 2006; Miaou and Lin, 2002]
- Intelligent Techniques (e.g. Support Vector Machines, Fuzzy logic, Neural Network and Other classifiers) [Kumar et al., 2007]

Fiducial Point based technique generally being the fastest method of ECG diagnosis, includes multiple steps. These steps start with the detection QRS Complex. Then, onset and offset of QRS is detected. Next amplitude and duration of QRS is detected. Then, other parameters such as slope of QRS are detected. Similarly, onsets, offsets, amplitudes, durations are calculated of P wave and T waves. Detection of all these parameters for all the feature waves within the ECG trace entails significant delay in mobile environment. Transformational and Intelligent techniques are generally more complex than fiducial point based techniques, making them unsuitable for resource constraint mobile devices (described earlier

in Chapter 2). On the contrary, the proposed Cardioid based technique does not employ multiple steps nor adopt any complex technique for patient identification and detection purpose. Therefore, the proposed techniques reduce delay in "Door to Ballooning Time" or "Symptom-Onset-to-Balloon time".

## 6.2 Architecture & System Design

The proposed architecture of our mission critical cardiovascular abnormality alert system monitors the patient's ECG in real-time. In the event of cardiovascular abnormality, the proposed alerting mechanism notifies the hospital personnel. The hospital can come to a quick decision by undergoing rapid diagnosis. The hospital personnel then initiate life saving protocols by sending emergency rescue team, ambulance etc. With the proposed framework, faster life saving effort is established with both faster authentication and faster diagnosis. The underlying technology of both authentication and diagnosis is focused on a computationally inexpensive, yet effective method called center of cardioid.

In the MCCA architecture presented in Figure 6.1, when the ECG trace of a subscribed patient is normal, the major task established by the system is to obtain back-up of the current data (referred as previous data). The saved data is used to create the biometric template for authentication purposes in the case of heart abnormality. Therefore, the routine task for the scenario when the patient's ECG signal remains normal is to acquire ECG data from the acquisition device, calculate the center of the cardioid, save the current ECG data (provided that ECG data is normal as center of centroid lies within a preset range). This range is dependent on the monitored person, the monitoring device and the sensor placement

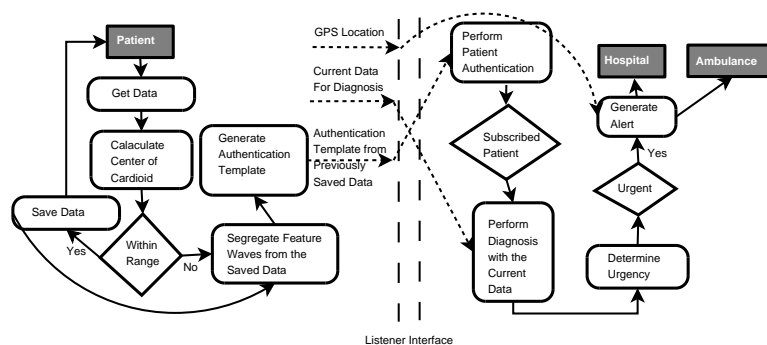


Figure 6.1: Architecture of Mission Critical Cardiovascular Abnormality Alerting System

configuration (Lead I, II, III, V1-V6 etc.).

On an event of cardiovascular abnormality, the centroid location will be shifted from the normal range. Since authentication must be carried out to ensure that this event of abnormality reaches to the hospital, previously saved data is engaged in authentication procedure. As the abnormal data (current ECG data) hardly inherit any biometric trait for the patient, it cannot be used for biometric feature extraction. Therefore, the previously saved normal ECG trace (without the occurrence of the abnormal trait) is fetched and segregated to extract P wave, QRS complex and T wave. From the individual feature waves biometric recognition data is prepared.

In the next phase, listener (of the patient's mobile) is turned on and a message containing the biometric features (for patient authentication) is created and sent to the hospital. The listener handles communication protocol with the hospital. On arrival of the biometric template message, the hospital's biometric server performs one to many matching against its entire subscribers' list. If the hospital's authentication mechanism recognizes the biometric template as a valid subscriber, then in the next step, it obtains the abnormal ECG data (current data containing the ECG abnormalities) through the listener (already turned

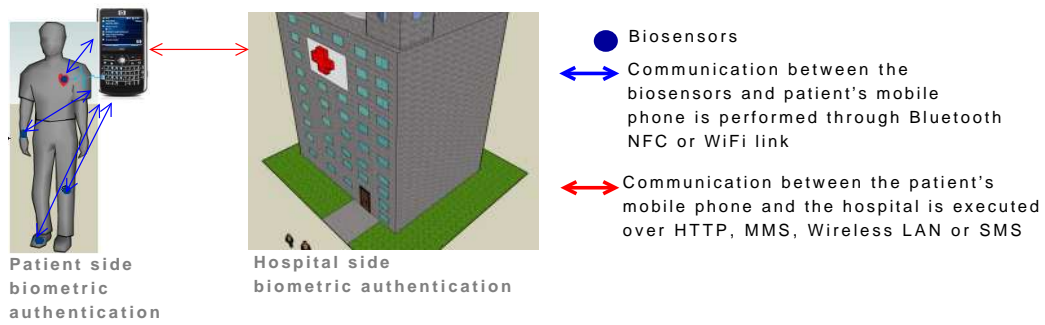


Figure 6.2: Two Types of Authentication Mechanism for Cardiovascular Patient

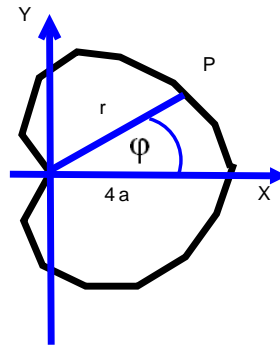


Figure 6.3: A typical Cardioid

on) of the patient’s mobile phone. The hospital then runs their algorithms in ascertaining the seriousness of the abnormalities. In case of urgency, patients location information (GPS coordinates) is pulled through the listener and emergency team is informed. Even if the patient is unconscious, the emergency team will be able to locate the patient to undergo life saving procedures. On the other hand, if the patient is not a member within the hospitals enlisted patients then the listener is turned off (the general hospitals may be notified). In case of less serious event (determined by hospitals diagnosis algorithms), the listener is also communicated and instructed to undergo shut down procedures.

### 6.3 Cardioid based Authentication Mechanism

Template matching is the core process for any biometric authentication. Identification template or verification template is matched against the enrolment template. For our cardioid-based biometric, both identification and verification ECG templates are commonly termed as recognition ECG template. These recognition ECG templates and enrolment ECG templates are matched against each other to determine the identity of a person. Within the context of this chapter, we have designed, developed and investigated two cardioid based authentication mechanisms referred as method 1 and method 2.

A cardioid (as shown in Figure 6.3) drawn from ECG sample has distinguishing features such as its area, perimeter and center coordinates. This is obvious in Table 6.1 where cardioids of different segments of ECGs from two different persons are plotted. This is the basis and motivation of our work for this novel authentication mechanism. Most of the ECG biometric features are kept as points in Cartesian co-ordinate system in both the methods. However, for our method 1 there are two parameters (Area and Circumference), which are maintained as decimal values. Therefore, within the context of this research, matching essentially means obtaining two types of distances: straight line distance and percentage distance. Therefore, enrolment ECG can be represented as follows:

$$E_1 = \{(c_x^e, c_y^e), A_e, U_e\} \quad (6.1)$$

Similarly, recognition ECG can be expressed as:



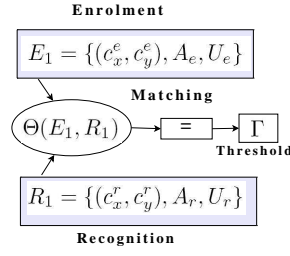


Figure 6.4: Matching Process (Method 1 as an Example) in ECG Cardioid based Biometric

$$R_1 = \{(c_x^r, c_y^r), A_r, U_r\} \quad (6.2)$$

Here,  $(c_x, c_y)$  is the Cartesian coordinate points ( $r$  and  $e$  denotes recognition and enrolment respectively),  $A$  is the area and  $U$  is the circumference or perimeter.

The matching function  $(\Theta(E_1, R_1))$  for method 1 produces a set of thresholds,  $\Gamma = \{\Gamma_1, \Gamma_2, \Gamma_3\}$ . In fact,

$$\begin{aligned} \Theta(E_1, R_1) &= \left\{ \sqrt{(c_x^e - c_x^r)^2 + (c_y^e - c_y^r)^2}, \right. \\ &\quad \left. \frac{A_e - A_r}{A_e} \times 100, \frac{U_e - U_r}{U_e} \times 100 \right\} \\ &= \Gamma \end{aligned} \quad (6.3)$$

Whenever, during a matching process (as shown in Figure 6.4) the threshold is less than a pre-defined value, a successful recognition is thought to be made.

Template creations for both methods are preceded by acquisition, loop generation and

loop segregation process in the cardioid-based system as shown in Figure 6.5. However, the actual template creation for method 1 and method 2 are quite different. Owing to this difference in template creation for both the methods, method 1 provides computational intensive and highly accurate ECG biometric (since this method has more feature templates like  $A$  and  $U$ ), and method 2 provides lower complexity ECG biometric.

- *Acquisition:* During the acquisition of ECG, as a biometric entity, acquisition devices like GE ST 5500, Alive Heart Monitor, Phillips Page Writer etc. can be used. After the data acquisition, data is converted to millivolt (mV) ranges from their proprietary format. ECG data can be de-noised with the help of embedded feature of the ECG acquisition device. However, for the research presented in this chapter, we have only used publicly available ECG data from MIT BIH [Phy, Accessed 2009]. MIT BIH Database contains ECG data that were collected from numerous patients with cardiac abnormality using ECG acquisition devices following digitization of the data. Mathematically, ECG can be represented by  $x(n)$  as in Eq. (1).

$$x(n) = \{x(1), x(2), x(3), \dots, x(N)\} \quad (6.4)$$

where  $x(1), x(2) \dots$  are ECG samples and  $N$  is the length of ECG signal.

- *Loop Generation:* Apart from ECG, none of the biometric modalities are time series signal. For biometric detection, discarding time information is sometimes important as this allows us to utilize techniques adopted in other biometric modalities. This is the purpose of our proposed loop generation phase. With our loop generation process, time

series ECG graph is converted to a 2 dimensional loop. From this closed loop pattern, features can be extracted like other popular biometric mechanisms (e.g. finger print, iris, palm print, face etc.).

At the commencement of the loop generation procedure, ECG data is differentiated.

$$y(l) = x(n) - x(n - 1) \quad (6.5)$$

where ,  $l = 1, 2, 3, \dots, (M - 1)$

After obtaining vector  $x$  (original ECG in millivolt range) and vector  $y$  (differentiated ECG), loop generation is plotted as a scatted xy graph. Therefore, the X-axis of the graph holds all the mV ranges ECG amplitudes (vector  $x$ ) and Y-axis of the graph holds differentiated ECG (vector  $y$ ). Figure 6.6 shows the original ECG on the left side and the generated loop on the right side. It is clearly seen that with the loop generation process, time information is not retained (ECG is time varying signal). Our experimentation with 30 randomly selected ECG entries from MIT BIH reveal all the loops are quite different. This the basis of our research in person identification with ECG based biometric, presented in this chapter.

- *Loop Segregation:* A loop is defined as a curvature that originates from a particular point and ends at the same point. Therefore, in our experimentation, we used a .Net program to detect a drawing point (in pixel) that was previously painted. By doing so, in a window sliding fashion, the program can efficiently detect the previous point (or the originator of the loop) and the current point (or the end point of the loop) as these



Figure 6.5: 3 Steps in Biometric Template Creation for Patient Authentication

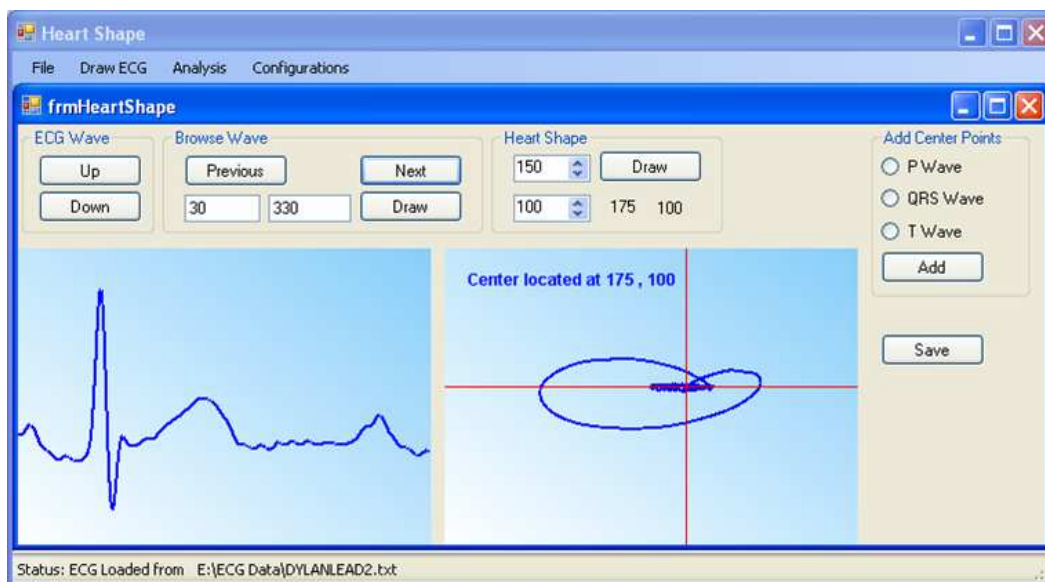


Figure 6.6: Cardioid based Patient Authentication and Diagnosis System (Desktop Implementation)

two points are being placed at the same pixel location (or in a close proximity).

### 6.3.1 Method 1: ECG based Person Identification with Centroid, Four Extremas, Area and Perimeter as template

The loop resulting from QRS complex appears as the shape of cardioid as seen in Figure 6.6. From the equation of the cardioids (Eq. 6.6), the area ( $A$ ) and the perimeter ( $U$ ) can be calculated from Eq. 6.7 and Eq. 6.8.

$$r = 2a[1 + \cos(t)] \quad (6.6)$$

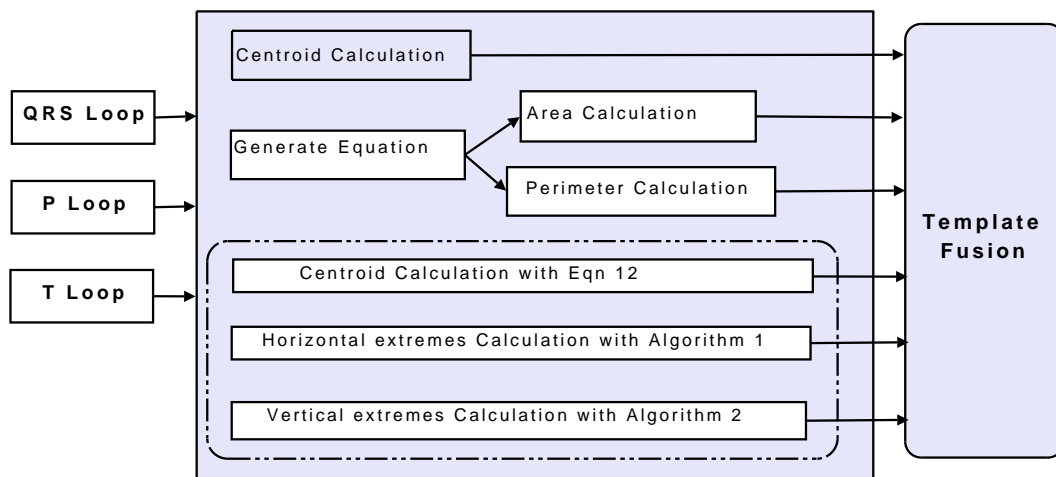


Figure 6.7: Block Diagram of ECG based Person Identification with Centroid, Area and Perimeter as Template (Method 1)

$$\begin{aligned}
 A &= \frac{1}{2} \int_0^{2\pi} r^2 d\varphi = .. \\
 &= 2a^2 \int_0^{2\pi} (1 + \cos \varphi)^2 d\varphi = .. \\
 &= 6\pi a^2
 \end{aligned} \tag{6.7}$$

$$\begin{aligned}
 U &= 2 \left| \int_0^\pi \sqrt{\left(\frac{dr}{d\varphi}\right)^2 + r^2} d\varphi \right| = .... \\
 &= 2\sqrt{2}a \left| \int_0^\pi \sqrt{1 + \cos \varphi} d\varphi \right| = .... \\
 &= 16a
 \end{aligned} \tag{6.8}$$

However, the loops generated from P wave and T wave appears to be ellipse. The equation for cardioid is given as:

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \quad (6.9)$$

Here,  $a$  is called vertex or major axis and  $b$  is co-vertex or minor axis. The vertex and the co-vertex for P wave loop are  $a_p$  and  $b_p$ . On the other hand, the vertex and the co-vertex for T wave loop are  $a_t$  and  $b_t$ . Our initial experimentation shows that  $a_t$  for T wave is more than three times  $a_p$  for P wave. Therefore,  $a_t > 3a_p$

Area,  $A$  and Perimeter (circumference),  $U$  can be calculated (or approximated) with the following equations.

$$A = \pi \times a \times b \quad (6.10)$$

$$U \approx \pi \left[ 3(a + b) - \sqrt{(3a + b)(a + 3b)} \right] \quad (6.11)$$

Calculation of  $U$  is based on Ramanujan's ellipse approximation.  $U$  approximation for ellipse with  $U \approx 2\pi\sqrt{\frac{a^2+b^2}{2}}$  is unsuitable for T wave, since  $b > 3a$ , according to our experimentation. Centroid is created by the following equation, for all the loops (QRS Complex, P wave and T wave).

$$centroid = \left[ \frac{\sum_{i=1}^N x_i}{N}, \frac{\sum_{i=1}^N y_i}{N} \right] \quad (6.12)$$

To calculate the extreme points as shown in Figure 6.9, intersections of the coordinates (transformed) and approximated equation of the original shape (loop) are required to be calculated. However, estimations of the exact equations that represent the loops are computationally expensive for mobile and embedded devices using existing curve fitting techniques.

The procedures involved in method 1 are summarised in Fig 6.7. Advantage of method 1, is its accuracy, with possible lower misclassification rate, as this method has two extra template parameters (Area and perimeter). However, it has a higher computational expense. This computational expense is mainly caused by the custom equation-based-curve-fitting technique on the loop points. The average time taken from these custom equation-based-curved-fitting was more than 1.8 second on our desktop system. However, when implemented on smart phones the calculation time was found to be as high as 30 seconds. Therefore, for biometric authentication on remote telecardiology (involving mobile phone), a computationally inexpensive method is required.

### 6.3.2 Method 2: ECG Biometric based on Centroid and Extreme Points

This method, as depicted in Figure 6.8, is simpler compared to method 1 as it does not require computations of  $A$  and  $U$ . After generating the loops for the heart shape (originated from QRS complex), ellipse originated from T wave and ellipse originated from P wave, 15 points were initially selected for representing each ECG sample. For the QRS,

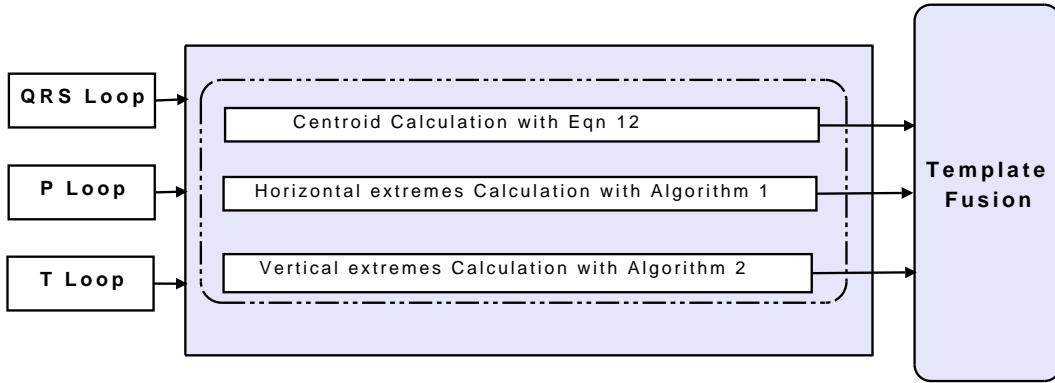


Figure 6.8: Block Diagram of ECG based Person Identification with Centroid and Four Extremas

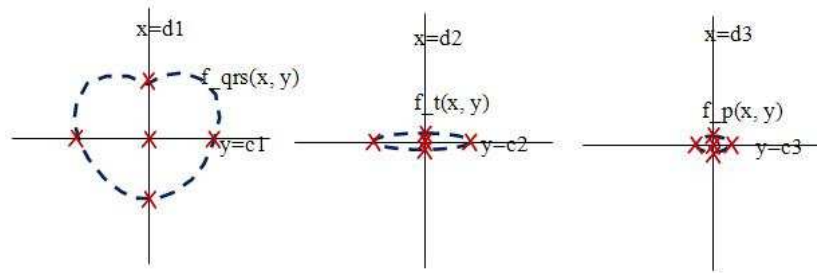


Figure 6.9: Calculation of Centroid and Four Extremas for QRS Complex, T Wave and P Wave

loop the points are Centroid  $(d1, c1)$ ,  $(f\_qrs(c1, y), c1)$ ,  $(-f\_qrs(c1, y), c1)$ ,  $(d1, f\_qrs(c1, y))$ ,  $(d1, -f\_qrs(c1, y))$ . For the T wave, loop the points are Centroid  $(d2, c2)$ ,  $(f\_qrs(c2, y), c2)$ ,  $(-f\_qrs(c2, y), c2)$ ,  $(d2, f\_qrs(c2, y))$ ,  $(d2, -f\_qrs(c2, y))$ . For the P wave, loop the points are Centroid  $(d3, c3)$ ,  $(f\_qrs(c3, y), c3)$ ,  $(-f\_qrs(c3, y), c3)$ ,  $(d3, f\_qrs(c3, y))$ ,  $(d3, -f\_qrs(c3, y))$ .

The functions  $f\_qrs(x, y)$ ,  $f\_t(x, y)$  and  $f\_p(x, y)$  are all estimated functions, that can be approximated based on different techniques. Curve fitting is one of the techniques, which has been used in our earlier researches on PDM (Chapter 3). In those previous researches, we have used the polynomial coefficients as the ECG feature, which were compared to identify



human. However, the major problem for using coefficients as ECG feature is the size of the coefficients. Multiple coefficients (as high as 32) increase the overall template size of the feature set. Higher template size requires higher computational expense as well as time to perform comparison task (biometric matching time) for biometric identification. Therefore, within this chapter, we initially selected only five points to represent shapes (Centroid and the four extreme points for each of the shapes).

To save computational resources for resource limited devices, approximation of the extreme points (Figure 6.9) is crucial. Rather than approximating the equations of the loops and finding the intersections with the coordinates (as it was done for method 1), four vertical extreme points can be calculated for each of the loops, using the following rules.

**Rule 1:** Point  $p(x_n, y_n)$  is the chosen to be upper extrema, when  $y_n > c$  and  $|(x_n - d)|$  is minimum for all points  $p(x, y)$  in the loop. In the same way for lower extrema,  $y_n < c$  and  $|(x_n - d)|$  is minimum (notation descriptions can be found in 6.9). Therefore:

$$\forall p(x, y) \exists y_n : |(x_n - d)|$$

**Rule 2:** Point  $p(x_n, y_n)$  is the chosen to be the right extrema, when  $x_n > d$  and  $|(y_n - c)|$  is minimum for all the points  $p(x, y)$  in the loop. For the left extrema  $x_n < d$  and  $|(y_n - c)|$  is minimum (notation descriptions can be found in 6.9). Therefore,

$$\forall p(x, y) \exists x_n : |(y_n - c)|$$

Based on these rules, algorithm 1 and 2 were designed and implemented.

From experimentations, we noted for the left and right extreme points,  $y$  value is very close to  $c$ . This is because,  $y$  is basically the change (derivative) in waveform and for all the wave forms, negative change is followed by equivalent positive change. From Figure 6.6, we

---

Algorithm 1: Detection of Right and Left Point of the Loop  
 $rightX, rightY, leftX, leftY, tempDistance$

---

**Loop for all points in the feature loop**  
**if**  $(y_i - c) < tempDistance$  **and**  $y_i > d$  **then**  
 $tempDistance = |(y_i - c)|$   
 $rightX = x_i$   
 $rightY = y_i$   
**endif**  
**if**  $(y_i - c) < tempDistance$  **and**  $y_i < d$  **then**  
 $tempDistance = |(y_i - c)|$   
 $leftX = x_i$   
 $leftY = y_i$   
**endif**  
**End Loop**

---

can clearly see that for all the waves (QRS Complex, P wave and T wave), positive wave change is followed by equivalent negative change. Left and Right extreme points are situated on the vertically opposite side of the Centroid and the  $y$  value of the Centroid is essentially the average of change of the waveform (which is near zero). This can be clearly seen from Table 6.1, where all the  $y$  values for the three persons are approximately 100.

Hence, for all the loops,  $y$  values of Centroid, left extrema and right extrema are least important.  $Y$  values for these three points for all the loops can easily be omitted for generation of template. The insignificance of these values ( $y$  values for left and right extreme points) for identifying person also become apparent by using Principal component analysis (PCA).

### 6.3.3 Implementation & Experimentation Results

We have implemented the cardioid based biometric authentication both on PC (desktop) and mobile phone environment. Method 1 based biometric authentication took about 24 seconds in PC based environment. This higher requirement of processing time is mainly

Algorithm 2: Detection of Upper and Lower Extreme Points of the Loop

$upperX, upperY, lowerX, lowerY, tempDistance$

**Loop for all points in the feature loop**

**if**  $(x_i - d) < tempDistance$  **and**  $y_i > c$  **then**

$tempDistance = |(x_i - d)|$

$upperX = x_i$

$upperY = y_i$

**endif**

**if**  $(x_i - d) < tempDistance$  **and**  $y_i < c$  **then**

$tempDistance = |(x_i - d)|$

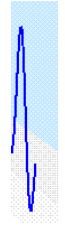
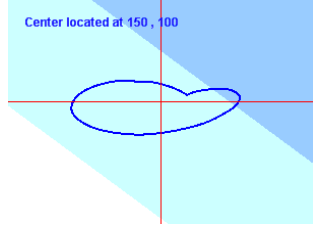
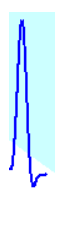
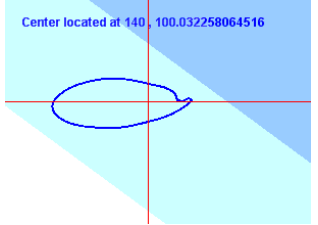
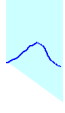
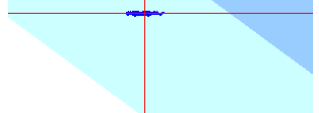
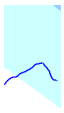
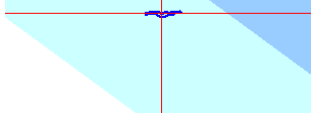
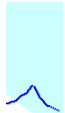



$lowerX = x_i$

$lowerY = y_i$

**endif**

**End Loop**

Table 6.1: The Difference in ECG Feature Waves between Two Different Individuals

ECG Wave Segment	Person A		Person B	
	Original Wave	Generate Loop	Original Wave	Generated Loop
QRS Complex				
T Wave				
P Wave				

because of the estimation of the equation from the cardioid shape, calculation of area and calculation of perimeter. To estimate the equation, curve fitting tools were utilized similar to our previous research (Chapter 3). After approximation of the equation of the cardioid, area and perimeter were calculated. Again, the calculation process for Area and Perimeter were quite different in every individual, as the cardioid equation varied from person to person. Higher computational complexity was the main obstacle for implementing method 1 based biometric authentication on mobile environment.

In method 1 (desktop system), area for the QRS loop ranges from 42 to 117, while the perimeter lies between 24 and 44. T wave loop area spans between 1.5 and 7.8. T wave loop perimeter ranges from 5.21 to 13. Similarly, P wave loop area ranged from 2.355 to 9.42 and P wave loop perimeter ranged from 2.13 to 8. When implemented in our desktop system, method 2 only consumed 300 milliseconds and on smart phones, it only took 2 second.

We have used the publicly available ECG entries from MIT-BIH Normal Sinus Rhythm Database (nsrdb) to show the difference in centroid across different individual (Table 6.2). Table 6.2 also shows the similarity of enrolment centroid (for QRS only) and recognition centroid. As QRS complex demonstrates the most uniqueness across individuals [Wubbeler et al., 2007], centroid of QRS are matched first. Then, the other templates (centroid for T wave / P wave, four extremas) are matched. However, it appears obvious that centroid of QRS alone can uniquely identify persons. When other QRS extremas are added as identification features, centroid and extremas of P or T waves may not be necessary.

Table 6.2: Uniqueness of Cardioids of Various MIT\_BIH Entries

Entry	Centroid of Enrolment QRS	Location of Enrolment	Centroid of Recognition QRS	Location of Recognition
16265	(127, 100.8)	[47:57]	(128, 100.4)	[1233:1243]
16420	(146, 99.89)	[66:75]	(146, 100.11)	[1226:1235]
16773	(138, 100)	[48:58]	(138, 99.7)	[982:992]
16795	(151, 100.1)	[10:20]	(152, 100.2)	[1198:1208]
17453	(143, 100.38)	[89:102]	(142:100.38)	[1131: 1144]

Table 6.3: Misclassification Rate for PRD, CC, WDM and PDM

Method	Misclassification Rate (%)
PRD [Chan et al., 2008]	25
CC [Chan et al., 2008]	21
WDM [Chan et al., 2008]	11
PDM (without Alg. 1, without Alg.2) [Sufi et al., 2010a; Sufi and Khalil, 2008a]	13.33
PDM (with Alg. 1, without Alg.2) [Sufi et al., 2010a; Sufi and Khalil, 2008a]	6.66
PDM (with Alg. 1, with Alg.2) [Sufi et al., 2010a; Sufi and Khalil, 2008a]	0
Proposed (Method 1)	1
Proposed (Method 2)	1

### Misclassification Rate

Both Method 1 and Method 2 had single misclassification errors (for each of them) as seen in Table 6.3. However, we believe that experimenting with a larger sample size will reveal higher accuracy of method 1 with the expense of higher computational requirements. Table 6.4 shows the False Match Rate (FMR) and False Non Match Rate (FNMR) wise comparisons of Method 1 and 2 with other existing biometric techniques.

Table 6.4: FRM and FNMR Accross Different Modalities

Modality	FMR (%)	FNMR (%)	Reference
Face	1	10	[Phillips et al., Last accessed: Jan. 2009]
Fingerprint	0.01	2.54	[Maio et al., 2004]
Iris	0.00129	0.583	[Group, 2005]
On-line signature	2.89	2.89	[D.-Y. et al., 2004]
Speech	6	6	[Reynolds et al., 2004]
ECG	6.66	6.66	PDM (without Alg. 1, without Alg. 2) [Sufi et al., 2010a; Sufi and Khalil, 2008a]
ECG	3.33	3.33	PMD (with Alg. 1, without Alg. 2) [Sufi et al., 2010a; Sufi and Khalil, 2008a]
ECG	0	0	PDM (with Alg. 1 + with Alg. 2) [Sufi et al., 2010a; Sufi and Khalil, 2008a]
ECG	0.5	0.5	Proposed (Method 1)
ECG	0.5	0.5	Proposed (Method 2)

### Template Size

Shorter template size results in faster processing, during one to many matching performed during person identification. Table 6.5 shows differences in template sizes for different ECG biometric.

If matching of 1 byte takes  $t_b$  amount of time, then according to Table 6.5, method 1 and method 2 consume  $(69 \times t_b)$  and  $(63 \times t_b)$  times respectively. Therefore, method 1 is approximately 4452 times faster and method 2 is approximately 4876 times faster then face [Yu et al., 2008] recognition, which has a template size of approximately 307200 bytes of data. Clearly, the proposed method 2 requires less storage and executes faster for person identification task compared to the existing biometric mechanisms.

*Table 6.5: Comparison of Template Sizes*

Biometric Data Type	Size in bytes
Iris [Yu et al., 2008]	512
Face [Yu et al., 2008]	153600-307200
Voice [Yu et al., 2008]	2048-10240
ECG [Wubbeler et al., 2007]	600
ECG (WDM) [Chan et al., 2008]	1371
ECG (PRD / CC) [Chan et al., 2008]	2210
ECG (PDM) [Sufi et al., 2010a; Sufi and Khalil, 2008a]	340
ECG (Proposed Method 1)	69
ECG (Proposed Method 2)	63

### Authentication Time

To estimate how this cardioid based automated authentication mechanism (method 2) helps in mission critical health application, we have compared this innovative patient authentication mechanism with existing username / password based telecardiology application. Three different level of mobile phone users (novice, moderate and expert) were put under the test of providing their username/password pair to mimic a cardiovascular subscriber establishing a connection with the service provider. Each group consisted of 5 people. Table 6.6 shows the timing requirement of the three groups.

Apart from saving time, the obvious benefit from this automated biometric scheme is the correctness of authentication process. If the cardiovascular patient suffers a sudden attack, patient may enter wrong username and password as manual task becomes harder because of anomaly in autonomic nervous system (ANS).

Table 6.6: Comparison of Cardiod based Automated Authentication Technique Against Username / Password based Authentication (Times are in Seconds. Cardiod Biometric were Performed on Randomly Selected MIT BIH Entries)

Novice Users	Moderate Users	Expert Users	cardiod Biometric
33.50	20.25	14.50	0.235
32.2	22.90	15.90	0.339
29.6	23.80	11.90	0.487
26.0	18.85	13.75	0.912
31.9	27.30	12.40	0.226

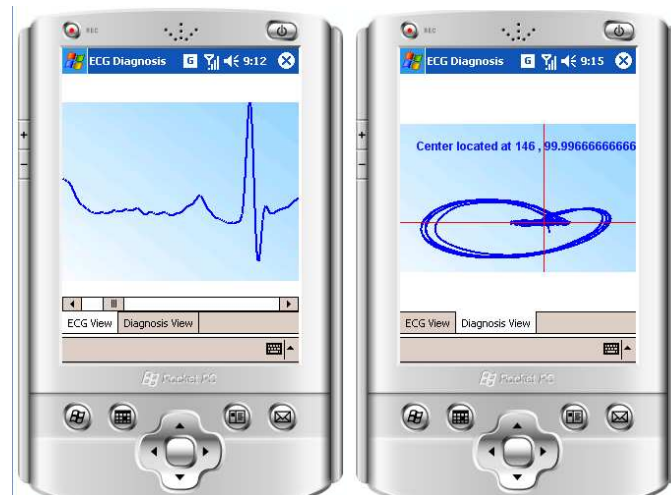


Figure 6.10: Mobile Phone Implementation of Cardiod (for ECG Abnormality Diagnosis within Doctor's Mobile Phone) Running in Pocket PC Emulator under MS Visual Studio 2005.



#### 6.4 Cardioid based Diagnosis

We can employ this cardioid based technique for detecting abnormal cardiac conditions. Any abnormality in ECG trace can be either manually detected by the expert cardiologists, or by automated algorithms. These algorithms usually detect onset and offset of QRS complex, T wave and P waves. After detection of these fiducial points (3 onsets and 3 offsets), width, amplitude and other parameters are calculated for each of the waves. Performing all these calculations simultaneously in real time is resource extensive. Therefore, most of the automated algorithms for detecting heart abnormalities are designed for PC based systems (or resource expensive ECG Acquisition devices). Center of cardioid can play a significant role in instant detection of cardiovascular abnormality, as any sudden change of ECG trace will cause instant change in the center of cardioid. As discussed earlier, calculation of center of cardioid is a simple and resource efficient technique, that can be easily implemented on mobile devices. This will help a roaming cardiologist to instantly detect abnormalities of cardiac conditions for ECG traces forwarded by the medical server (medical server on the other hand, received this ECG messages from the patient's mobile phone). Experimentation with MIT BIH entries proves this point.

The diagnosis programs were implemented in Visual Studio .Net environment and tested on the pocket PC emulator environment (as shown in Figure 6.11). After the successful deployment on the emulator platform, the cardioid based programs were deployed on HP 912 Business Messenger Smart phone (Figure 6.11). Our real life experimentation revealed that cardioid based authorization and diagnosis is the fastest solution for Mission Critical Alerting mechanism, where every seconds count towards saving irrecoverable cardiac cell

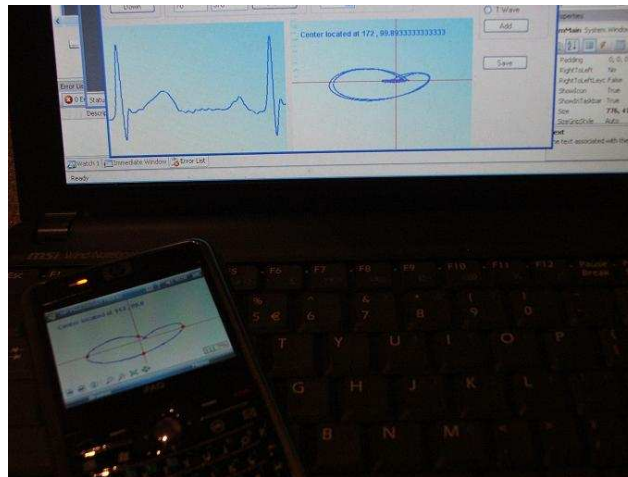


Figure 6.11: Deployment of Cardioid based Patient Authorization and Diagnosis on HP 912 Business Messenger Mobile Smartphone

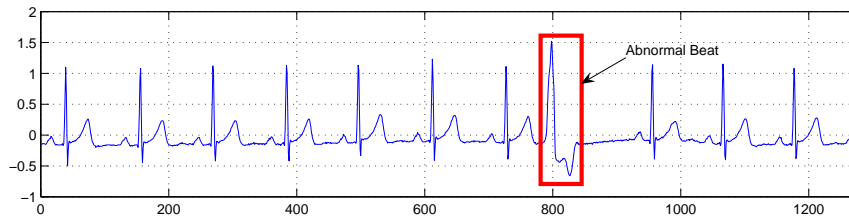


Figure 6.12: Occurrence of Ventricular Beat from MIT-BIH Supraventricular Arrhythmia Database (svdb) Entry No. 803

damage.

Figure 6.12 shows a sudden Ventricular beat (shown by box) from record 803 of MIT BIH Supra-ventricular Arrhythmia Database (svdb). This record corresponds to only a subsection of the whole record (from 29:40 minute to 29:50 minute), and a random window size of 100 samples (out of the total 128 samples) is used for calculation of center of cardioid. For these normal beats, the  $x$  coordinate of the centroid ranged from 150 to 153. On the other hand the  $y$  coordinate ranged from 99.77 to 100.29. One such plot using normal beat is shown in Figure 6.16. However, during the onset of the Ventricular beat the centroid was

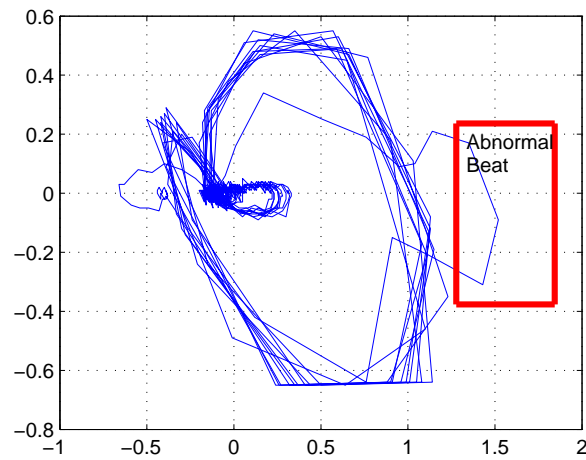


Figure 6.13: Cardioid Drawn from the Entire ECG Strip Presented in Figure 6.12 (from MIT-BIH Supraventricular Arrhythmia Database (sadb) Entry No. 803)

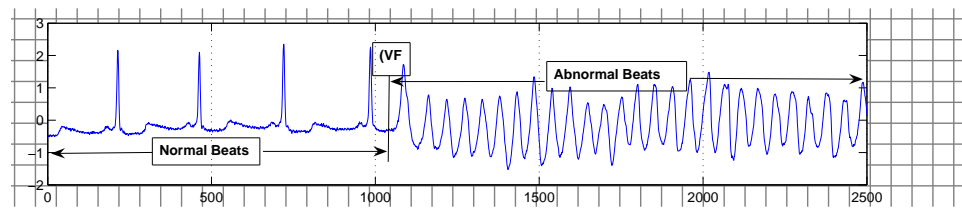


Figure 6.14: Occurrence of Ventricular Fibrillation from CU Ventricular Tachyarrhythmia Database (cudb) Entry No. 01

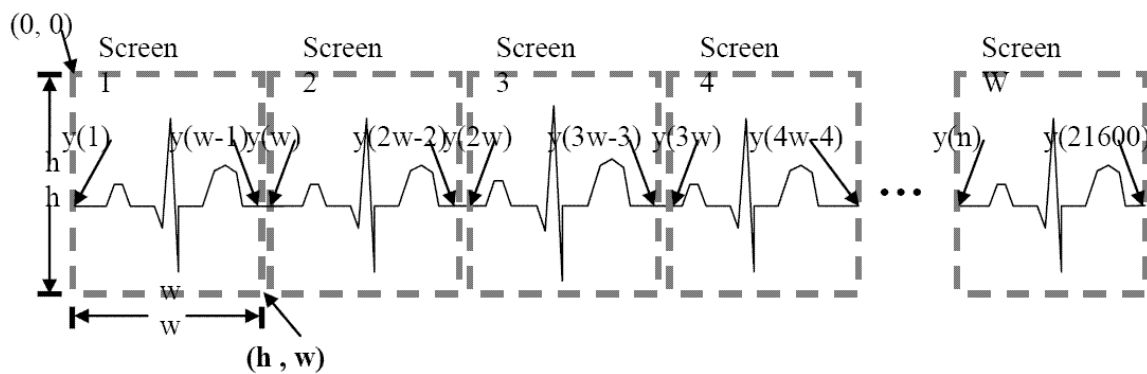


Figure 6.15: Drawing of ECG Curve in Multiple Screens of a Mobile Phone

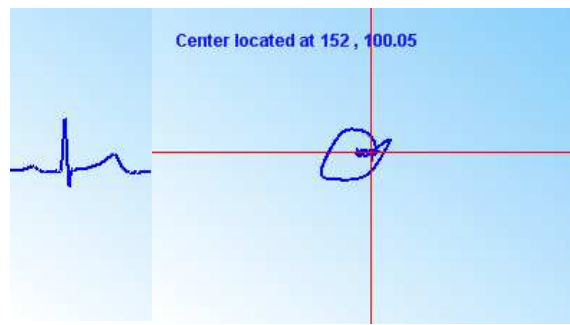


Figure 6.16: Centroid using the Normal Beats of Figure 6.12

(147, 99.73) as shown in Figure 6.17, when the centroid calculation period was from 700 to 800. A sudden drop of  $x$  coordinate of the centroid identified sudden abnormality within the ECG trace. This deviation in the values of centroid clearly shows how normal heart conditions suddenly changes. This form of presentation can help not only cardiologists, but also medical technicians to quickly diagnose cardiac abnormalities at the hospitals. Similarly, the centroid values calculated for sample range (800-900) and (810-910) of the same record are (156, 100.35) and (156, 99.93). These values are out of the normal ranges of centroid for that person, and therefore, identify cardiac abnormality. It should be noted that these values were calculated by our software (both desktop as in Figure 6.6 and mobile as in Figure 6.11). Figure 6.13 shows the entire ECG trace of Figure 6.12 transformed into cardioid. Even though the plot in Figure 6.13 is similar to the output of our software (both desktop and mobile), our software has normalized the coordinates (both X and Y) for obtaining integer values (as the pixels in desktop and mobile screens are represented by integer values). This fact (the difference in value range) is true for the subsequent cardioid figures presented in this chapter (Figure 6.22, Figure 6.20, Figure 6.21 and Figure 6.24).

Now if we look into more serious event of cardiac abnormality, such as ventricular fibrilla-

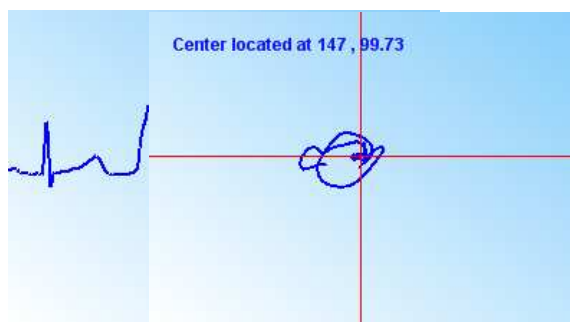


Figure 6.17: Centroid using the Abnormal Beats (i.e. During the Onset of the Ventricular Beat) of Figure 6.12

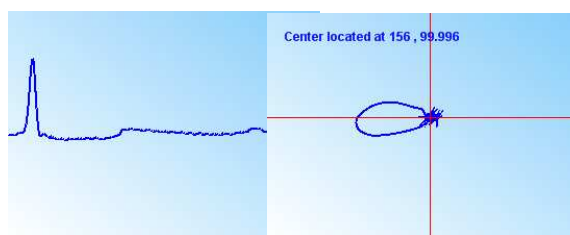


Figure 6.18: Centroid using the Normal Beats of Figure 6.14

tion (VF), we will also find the center of cardioid method useful for disease identification. We randomly selected an ECG trace containing VF onset to test the center of cardioid method. Figure 6.14 shows a 10 second segment (from 3:30 min to 3:40 min) ECG record (Entry no. cu01) from CU Ventricular Tachycardia Database (cudb). The onset of VF is annotated and marked within this trace. The normal, abnormal and the entire section of Figure 6.14 are represented by Figure 6.20, Figure 6.21 and Figure 6.22.

For testing the center of cardioid method, we selected a window size of 250 and calculated the center of cardioid in a window sliding fashion. For all the 4 normal QRS complexes of Figure 6.14, the centroid was  $(156 \pm 2, 100.03 \pm 0.26)$  as shown in Figure 6.18. At the event of VF, the center of cardioid changes to  $(160, 100.2)$  for segment 1100 to 1350 as visible in Figure 6.19.

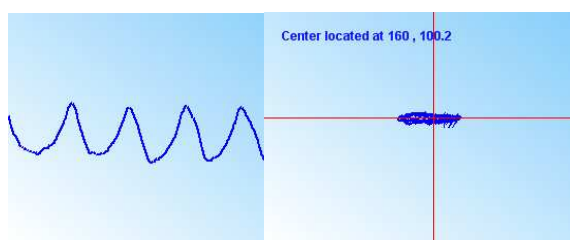


Figure 6.19: Centroid using the Abnormal Beats of Figure 6.14 (during Occurrence of Ventricular Fibrillation)

An ECG trace with 360 Hz sampling frequency and 1 minute duration spans horizontally and needs long scrolling facility even on a 20 inch monitor with  $1280 \times 1024$  resolutions. Even if we use a single pixel (of Mobile phone) to represent a single sample of ECG point, the mobile phone screen needs to be 21600 pixels wide to draw the 1 minute ECG curve (in a single screen) without the necessity of horizontal scrolling for ECG signal (with an acquisition sampling frequency of 360 Hz). However, mobile phones used during our experimentation had only 170 to 240 pixels in width. Therefore, the MIDlets were designed with horizontal scrolling facility to navigate forward the ECG with multiple screens (Figure 6.15).

Further more, drawing ECG curve onto a mobile phone screen is different than PC display, because of their variation in coordinate system. In mobile phone's screen, the coordinate  $(0, 0)$  starts from top left corner (Figure 6.15), unlike bottom left corner for PC graphics. Therefore, a coordinate transformation is required for the ECG signal  $x_n$ , before drawing them on mobile phone screen. Equation 6.13, demonstrates the transformation operation.

$$y_n = h - x_n \quad (6.13)$$

where  $h$  is the height of supported pixels for mobile phone. Therefore, generating curves

and graphs of biosignals needs proper calculation and translation before drawing them on to the mobile phone's screen. Figure 6.15 shows the end result of graphing (schematic). Figure 6.15 makes it obvious that a particular ECG signal can be spanned to  $W$  number of screens, where  $W$  is determined by Eq. 6.14.

$$W = \text{ceil}(f \times t(w - 1)) \quad (6.14)$$

where,  $\text{ceil}$  denotes the ceiling operation,  $f$  is the sampling frequency of ECG acquisition and  $t$  is the total duration of the ECG trace.

If the mobile phone, used by the doctor, has moderately higher resolution and supports 240 pixel in width then 1 minute ECG (250 sampling frequency) requires  $\text{Ceil}(15000/239)$  or 63 screen. Therefore, if the doctor intends to browse through the entire 1 minute ECG trace, then he requires at least 62 clicks on the mobile phone. Now if each click consumes 0.5 seconds of delay, the mobile cardiologist needs at least 31 second, just to draw the complete ECG trace. Viewing and taking decision on the ECG will take further time on top of the drawing time.

However, using our cardioid based diagnosis approach, this time (i.e. clicking and viewing of the screens) could be minimized to less than 0.5 second, as no clicking operation is required by the cardiologist. The entire signal can be plotted on a single screen. On that screen, the abnormal ventricular beats will be clearly misaligned. As seen in the cu\_1 record (in Figure 6.14), VF event started (approximately from sample no. 1026) after first four normal beats. If the cardioid is drawn from 0 to 1026 sample, we would see the regular (normal) beat

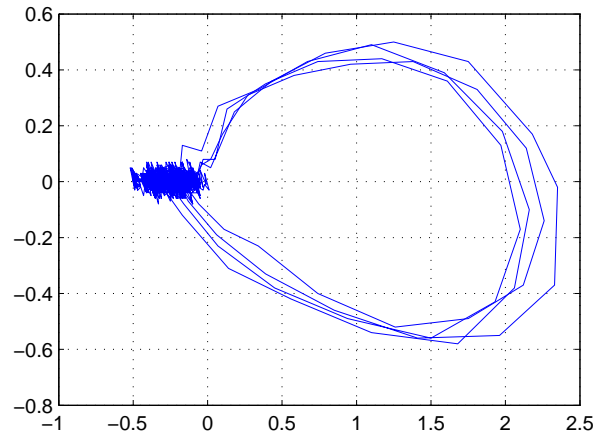


Figure 6.20: Cardioid Drawn from the Four Normal Beats of Figure 6.14

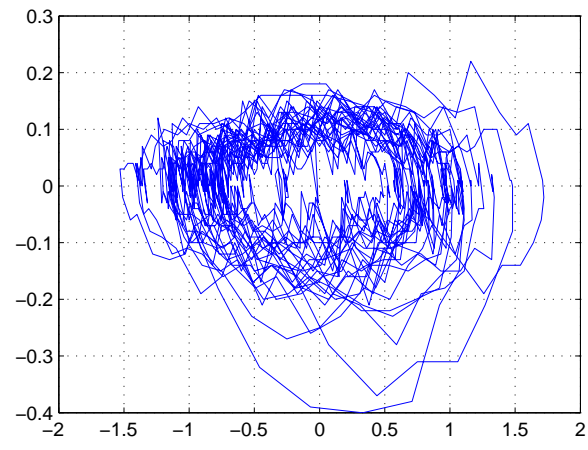


Figure 6.21: Cardioid Drawn After the Occurrence of VF in Figure 6.14



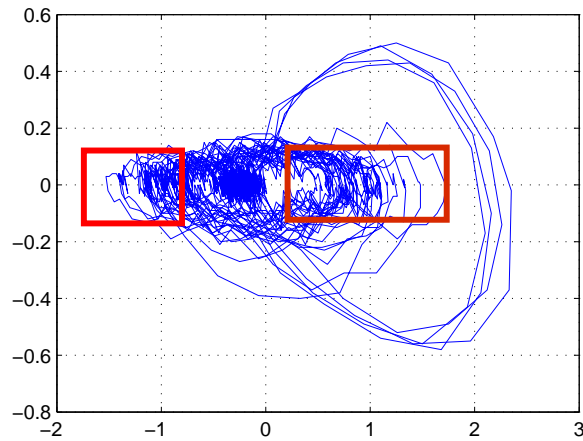


Figure 6.22: Cardioid Drawn from the Entire ECG Trace Presented in Figure 10

pattern for that person as seen in Figure 6.20.

However, just after the initiation of the deadly VF event, the cardioid takes a totally different pattern as shown in Figure 6.21. It is evident from the pictures (Figure 6.20 and Figure 6.21) that the regular beat and VF beat doesn't share the same pattern. If a cardiologist is given with the cardioid drawn from the entire 10 second ECG trace (from sample 1 to sample 2500) for the same record, then he / she will see two different patterns and will instantly identify occurrences of abnormality (as depicted in Figure 6.22). In fact, automated algorithms can be developed and deployed to notify any instance of drawing on highlighted area (termed as abnormal area) on the mobile phone screen (canvas class [Sufi, 2007; Yuan, c2004]). In Figure 6.22, we can see the possible VF region marked with boxes. Any drawing on that box signifies occurrence of Ventricular abnormal beat.

Algorithm 3 performs the automated abnormality detection by detecting any drawing on a boxed region. Boxed region  $(x_1, y_1, x_2, y_2)$  is area of the Cartesian coordinate (either implemented on PC or Mobile Screen) that has been marked as abnormal region. During the

---

Algorithm 3: Cardioid based Automated ECG Diagnosis

---

*Cur\_Point, Prepoints* //the points are in Cartesian coordinate

*Cur\_Point* = (0, 0)

*Pre\_Point* = (0, 0)

*Cur\_Point* = *GetCurrentPoint()* // Using Eqs. (4-5)

**Loop**

**if**  $x1 \leq Cur\_Point.X \leq x2$  **AND**  $y1 \leq Cur\_Point.Y \leq y2$  **then**

**Abnormality\_Detected** = **TRUE**

*Count* = *Count* + 1

**endif**

**Drawline** (*Pre\_Point*, *Cur\_Point*)

*Pre\_Point* = *Cur\_Point*

**EndLoop**

---

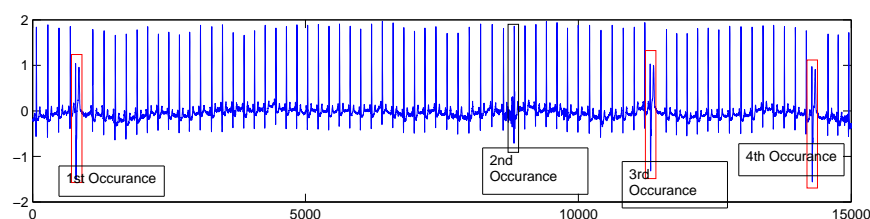


Figure 6.23: Occurrences of Ectopic beats / premature beats (ectopic beats marked with red boxes and a suspected beat marked with blue box) from AHA Database entry no. 01

regular plotting activity (looping in Algorithm 3), if the current coordinate (*Cur\_Point.X*, *Cur\_Point.Y*) is bounded within the boxed region, then abnormality is identified. More than one boxed region can be created for identifying multiple cardiac abnormalities.

Figure 6.23 represents the first 1 minute's ECG data from AHA Database Entry no. 01. We can see that four abnormal beats are highlighted with boxes. If the same ECG extract is used for generating a cardioid, all the abnormal beats will be clearly identified as shown in Figure 6.24. Within the cardioid map, all the similar beat patterns share the same region of the screen.

Similarly, if cardioid is drawn using the Supraventricular Arrhythmia Database (svdb) entry no. 803 that is plotted in Figure 6.12, then the event of 'V' or wide QRS complex can

Table 6.7: Execution Time (in seconds) on HP iPAQ 912 Business Messenger for Cardioid, First Derivative based Technique, Second Derivative based Technique and Threshold based Technique

ECG No.	ABT	FDT	SDT	Cardioid
100	3	16	17	1
102	4	16	18	1
105	3	16	19	1
111	3	16	18	1
114	3	16	18	1
201	4	16	18	1
210	4	17	18	1

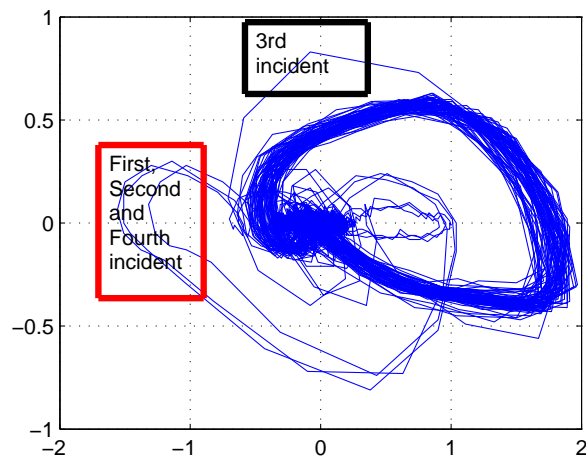


Figure 6.24: Cardioid Drawn from the Entire ECG Strip Presented in Figure 6.23

be easily visible (Figure 6.13).

Beat alignment operation in time series (original ECG trace) can also reveal abnormal beats from normal beats, as seen from Figure 6.25. These types of beat alignment can be performed with direct threshold based techniques [Friesen et al., 1990], transformational techniques [Kim et al., 2006] or ever other complex techniques involving Artificial Intelligence [Kumar et al., 2007].

In Table 6.7, we have performed beat alignments based on three existing direct methods. These three methods, namely Amplitude based technique (ABT), First Derivative based technique (FDT) and Second Derivative based (SDT) beat detection (for the experimentation in Table 6.7) are explained in detail by earlier research works [Friesen et al., 1990; Sufi et al., 2007]. Using these techniques, the QRS complex is located first and then the actual alignment is performed. Our cardioid based technique can offer beat alignment facility on small handheld platform in a very fast manner. Implementing the most simple existing beat alignment techniques (ABT, FDT and SDT) [Friesen et al., 1990] consumes at least 3 times more computational time, compared to the presented cardioid based diagnosis as seen from Table 6.7.

## 6.5 Discussion

In this chapter, we intend to reduce the delay in cardiac care in two main areas: patient authentication and diagnosis. The Authentication mechanism ensures security in Mission Critical Alert (MCA) Mechanism. The communication framework is tied with HTTP/ MMS/ SMS/ Bluetooth/ WiFi. Therefore, the presented MCA uphold elastic and distributed net-

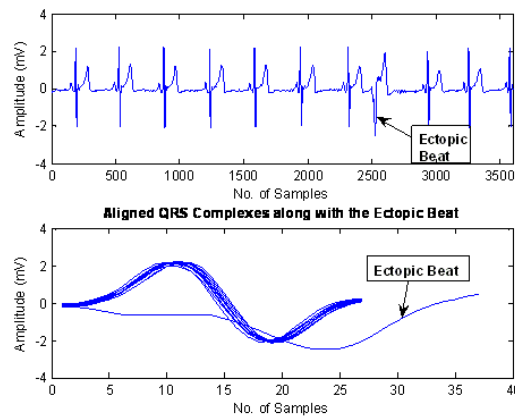


Figure 6.25: Beat Alignment in time Series Domain

work. In case, HTTP fails, patient's mobile to hospital communication can be executed on MMS or SMS [Sufi et al., 2009a], for ensuring reliability. Within the mobile phone based wireless cardiac care solution, we can observe the following five key actors:

- *Patient*: This patient is monitored with portable ECG acquisition devices. Patient is the center (or key player) within the mobile phone based patient centric solution.
- *Patient's Mobile Phone*: Patient's mobile phone serves as the communicator between the patient and the hospital / cardiologist / ambulance service provider. Also, this mobile phone performs repeated detection facility that continuously searches for abnormality from the patient's ECG trace. This is done via calculating the centroid of an ECG trace and measuring the centroid against a set threshold. Any centroid outside the threshold range signals a possible abnormality and initiates communication with the hospital. The mobile phone also performs local authentication (before local monitoring) as well as remote authentication (before connecting and informing the hospital about an abnormal event).

- *Hospital*: Hospital provides the cardiovascular monitoring facility to the patient, who subscribed for the continuous monitoring facility. The hospital runs its existing algorithms to check the validity and seriousness of the cardiac abnormality. In case of serious abnormality, the hospital informs the cardiologist and the ambulance for rescuing the patient.
- *Ambulance*: The ambulance locates the patient by retrieving GPS locations from the patient's mobile phone (a listener within the patient's mobile phone is responsible as in 6.1). Within the ambulance, a 12 lead ECG acquisition is performed and transmitted to the hospital via HTTP or Socket routine. The Hospital then views the ECG and decides on the action plan (e.g. Surgery in catheterization lab and therefore, activates the catheterization lab) for the patient in consultation with cardiologist. The ambulance is instructed accordingly about where to admit the patient (e.g. catheterization lab).
- *Mobile cardiologist*: The hospital can also receive expert opinions on special cases from the remote cardiologists. The cardiologist receives ECG information in compressed and encrypted format either from the patient or from the hospital. Cardiologist's mobile phone executes the cardioid based diagnosis program, which assists in faster diagnosis of the abnormal event.

The ECG transmission from the patient to the hospital / cardiologist or from the ambulance to the cardiologist is performed utilizing compression and encryption technology described in Chapter 2. Therefore, fast and secured transmission is guaranteed upholding Health Insurance Portability and Accountability Act (HIPAA) act of US (1996) [Cen, Ac-

cessed 2008; Off, Accessed 2009; Lee and Lee, 2008]. The value added to the MCN alert mechanism by this chapter, is by the innovative utilization of cardioid based authentication and diagnosis method and by strategically placing them on the existing cardiac care scenario [Otsuka et al., 2009; Sillesen et al., 2008; Ortolani et al., 2007; Khalil and Sufi, 2008b; Lee et al., 2007; Hung and Zhang, 2003]. With this piece of research in place even the fastest timing (22 minutes in [Sillesen et al., 2008]) in patient rescue can be reduced farther. Moreover, the architecture outlined in this chapter addresses the following two main criteria (as urged by [Bradley et al., 2006]) for reducing door-to-balloon time:

- Innovative, standardized protocols
- Data feedback to monitor progress and identify problems or successes

## 6.6 Conclusion

According to the cardiovascular experts, the delay in diagnosis can cause significant and everlasting damage to patient's heart and drastically increase the chance of reduced life span [Otsuka et al., 2009; Luca et al., 2004]. Therefore, minimizing the delay in cardiovascular patient care is a global urge, with cardiovascular disease being the number one killer of modern era. Within this chapter, we endeavoured in minimizing the cardiovascular patient care by harnessing the modern technological settlements of wireless communication and portable ECG sensors. By identifying two specific long haul bottlenecks (authentication and diagnosis) in mobile phone based cardiovascular patient monitoring, we have shown that several minutes delays can be reduced to a mere 0.5 second with Cardioid based techniques. Moreover, due to smaller template size our ECG based biometric method with Cardioid based technique

is much faster than existing biometrics systems like Face recognition. Apart from minimizing the delay in CVD patient care, we have also depicted a structured process of alerting mechanism which can potentially save lives of the CVD afflicted person.



# Chapter 7

## Conclusion

This chapter draws conclusion of our research work based on the preceding chapters. It also outlines the contributions and states suggestions for future work. Finally, a short summary for this research work is presented.

### 7.1 Summary of Research Progress

Table 7.1 provides a glimpse of our research achievements. The objective column relates directly to our research questions. Result column depicts how the objectives have been met, in terms of research output. The core contributions of this research outcome are briefed as follows:

- According to the literature, we have achieved the highest possible compression ratio of 20.06 (95% compression) on ECG signal, without any loss of information. According to our experiments, execution of our unique compression, which was designed specifically for running on mobile devices with lower computational ability, causes minimal delay

Table 7.1: Summary of research progress

Objective	Result	Conclusion
Minimizing transmission Delay	Substantially achieved with our proposed ECG compression algorithms [Sufi and Khalil, 2008b; Sufi et al., 2009a; Sufi and Khalil, 2010a; Sufi et al., 2006b]	Our proposed ECG compression algorithm can execute in realtime and provides substantially higher compression ratio (about 90%). Therefore, during compressed ECG packet transmission between the patient and the doctor, minimal delay is incurred.
Minimizing the authentication time	Substantially achieved with proposed ECG based Biometric techniques [Sufi et al., 2010a;c; 2009b; Sufi and Khalil, 2008a; Khalil and Sufi, 2008a; Sufi and Khalil, 2011a; Sufi et al., 2010b]	Compared to the existing user name and password based techniques of [Blount et. al., 2007], one of our automated ECG biometric methods (cardioid based) perform substantially faster authentication (approximately 70 times faster) [Sufi et al., 2010b]. Our innovative methods successfully minimized the delay of authentication with faster ECG biometric technique.
Protecting patient's privacy and upholding HIPAA regulations with secured ECG transmission	Fully achieved with innovative mechanisms [Sufi and Khalil, 2008b; Sufi et al., 2009a; Sufi and Khalil, 2009b; Sufi et al., 2008e;d;f; Sufi and Khalil, 2010b]	Our methods provide significantly higher level of security strengths after encrypting the ECG (compared to existing encryption algorithms like DES, AES etc.) [Sufi and Khalil, 2008b; Sufi et al., 2009a].
Saving patient's life and increasing patient's life span with faster cardiovascular disease diagnosis	Substantially achieved with different techniques [Sufi et al., 2009a; 2005; Sufi and Khalil, 2010c; Sufi et al., 2011; 2010b]	Our novel diagnosis methods based on compressed ECG provide several times faster diagnosis of cardiovascular abnormality. Therefore, faster patient care is achieved.

(detailed in Chapter 2).

- We have proposed new methods of ECG based biometric authentication mechanisms that work on plain ECG (i.e. suitable for existing tele-cardiology applications that do not harness efficient transmission with compressed ECG). On the other hand, we have proposed innovative solutions that perform ECG based biometric directly from the compressed ECG. Most of these proposed methods are substantially faster than existing methods of ECG based biometrics (detailed in Chapter 3). For example, our Data Mining based compressed-ECG-Biometric method is approximately 16.67 times faster than [Wubbeler et al., 2007], 38.08 times faster than WDM [Chan et al., 2008] and 61.38 times faster than PRD / CC [Chan et al., 2008] while still providing the lowest level of misclassification. Moreover, we proposed another completely new approach of faster ECG based biometric with our cardioid system. According to our experimentations (shown in Chapter 6), the authentication time can be reduced from 30.64 sec. (manual authentication by novice mobile user as depicted in [Blount et. al., 2007]) to 0.4398 sec. in mobile platform (automated authentication).
- Our 3 layer permutation cipher based ECG encoding mechanism can raise the security strength substantially higher than conventional AES or DES algorithms. If in near future, a grid of supercomputers can compare a trillion trillion trillion ( $10^{36}$ ) combinations of one ECG segment (comprising 500 ECG samples) per second for ECG morphology matching, it will take approximately  $9.333 \times 10^{970}$  years (detailed in Chapter 4). This encoding also drastically reduces the ECG packet size (i.e. perform compression). How-

ever, for tele-cardiology systems not utilizing our compression algorithm, we proposed wavelet based anonymization techniques (discrete wavelet and wavelet packet) that work on plain ECG. These techniques also remove most of the ECG features required to identify the patients and their cardiovascular conditions. Lastly, we proposed noise based ECG obfuscation technique, which tricks the hacker in believing the obfuscated ECG as the plain ECG (i.e. for tele-cardiology systems not adopting our compression technique). Only the authorized personnel possessing the secret key, which is only 0.04 % of the original ECG in size, can de-obfuscate the obfuscated ECG.

- We have proposed and implemented new techniques for faster ECG based CVD diagnosis (detailed in Chapter 5). The first method was our implementation of a rule based CVD detection algorithm that works on plain ECG, on mobile platform. Then we introduced our Instant Detection Algorithm, which does not require to read the compressed ECG packet (i.e. this method only reads the payload size of the compressed ECG packet). This algorithm is approximately 3 times faster than existing Amplitude Based Method (ABM) ([Sufi et al., 2009a]) and more than 13 times faster than existing Second Derivative Based Method (SDBM) [Sufi et al., 2007]. Next, our direct compressed ECG based method [Sufi et al., 2009a] produces faster diagnosis by directly reading compressed ECG. Our Data Mining (DM) based intelligent approach also reads compressed ECG and performs more accurate diagnosis [Sufi et al., 2011; Sufi and Khalil, 2011b] and even detect the on-set (start) of abnormality. Lastly, our cardioid based technique is about 4 times and 18 times faster than ABM and SDBM [Sufi et al., 2010b] respectively.

- Finally, we have established a tele-cardiology framework comprising of faster and secured transmission of compressed ECG, faster authentication, faster diagnosis, portable computational platform (with regular mobile phones), portable ECG sensors and background surveillance agent with data mining techniques [Sufi et al., 2006b; Sufi and Khalil, 2011b; Sufi et al., 2011; 2008a; Sufi, 2007; Khalil and Sufi, 2008b; Sufi et al., 2008c; 2009a; Sufi and Khalil, 2008b; 2009b; Sufi et al., 2010c; 2007; Sufi and Khalil, 2008a; Khalil and Sufi, 2008a; Ibaida et al., 2009; Sufi and Khalil, 2009a; Sufi et al., 2008e;d; 2010b; Sufi and Khalil, 2011a; Sufi et al., 2009b; Sufi and Khalil, 2010a;b;c; Sufi et al., 2008b;f; Khalil and Sufi, 2008b; 2009]. Our tele-cardiology framework has been designed to save CVD patients from sudden death occurring from cardiac anomaly.

## 7.2 Limitations and Suggested Future Work

Our research work presented within this thesis provides a complete solution for remote monitoring of CVD patients harnessing the power of mobile computational platform, wireless sensors (ECG sensors), telecommunication infrastructure and a new breed of algorithms. The telecardiology platform presented within this thesis assists in saving the life of CVD patient with faster solutions for transmission, authentication, diagnosis and privacy (security). However, there is room for improvement in the following areas:

- Research on even faster and efficient ECG transmission with innovative lossless ECG compression algorithms is needed. With our research, we were able to raise the compression ratio up to 20.06 from 3.281 mark of DCCR + SPIHT +BPC (Suggested Method of [Jalaleddine et al., 1990]) without any loss of information.

- Our compression algorithm was mainly designed for MIT-BIH Arrhythmia Database [Phy, Accessed 2009] entries (i.e. 360 Hz. sampling frequency, 10 bit resolution with 5 mV stepping). Research on innovative ECG compression algorithms suitable for other ECG devices (preferably generic and implantable devices) needs to be carried out. Compression of ECG in HL7 format also needs to be researched on .
- Our authentication mechanisms were tested against a limited set of ECG data collected from only a handful of individuals (mostly MITBIH entries). The authentication mechanisms needs to be rigorously validated for misclassification, False Match Ratio (FMR), False Non Match Ratio (FNMR) on a larger set of ECG data (collected from more human participants under varying physiological conditions).
- For securing ECG transmission, this thesis describes several mechanisms (ECG encoding/ encryption with 3 layer permutation cipher, ECG obfuscation with noise smearing, ECG anonymization with discrete wavelet and ECG anonymization with wavelet packet). All of these mechanisms are shared key based encryption techniques, meaning the people knowing the shared key would be able reconstruct the ECG. Research on secured key distribution techniques, needs to carried out for telecardiology scenarios, since this topic has not been addressed in our thesis. Apart from the symmetric ciphers described in this thesis, research on asymmetric ciphers for ECG encryption should be investigated.
- Within this thesis, we have investigated the detection of only handful of ECG abnormalities (such as Arrhythmia, Bradycardia, Tachycardia, Wide QRS syndrome, WPS,

Right Bundle Branch Block, Left Bundle Branch Block, Ventricular Conduction Problem etc.). Research on more CVD detection mechanisms must be carried out for covering all of the common cardiac anomalies.

- For ECG transmission, we have only used MMS, SMS, Bluetooth and HTTP. Transmission via other communication protocols (e.g. Zigbee) needs to be evaluated for feasibility.
- In the limited scope of this thesis, we have not performed security strength analysis of wavelet based and noise based anonymization techniques. However, we understand that with billions of noise signal combinations, the security strength of noise based anonymization technique would be unmatched. Detailed experimentation and calculation on security strengths should be performed in future.

### 7.3 Summary

CVD being the number one killer of modern age, more people are diagnosed with cardiac abnormalities [Acc, Accessed 2008]. If the CVD affected patients are diagnosed and treated with urgency (i.e. within shortest possible time) then abnormal deaths could be prevented and longevity of the patients could be preserved [Luca et al., 2004; Otsuka et al., 2009; Sillesen et al., 2008; Ortolani et al., 2007; Bradley et al., 2006]. Therefore, within this thesis our primary effort was focused on faster CVD monitoring solution. We have achieved our objectives by introducing a unique telecardiology scenario, where the patient is attached with ECG acquisition device that sends ECG packets to the patient's mobile phone. The patient's mobile phone then compresses the ECG packets achieving a significantly higher compression

ratio of up to 95%. Moreover, our proposed set of algorithms are applied to encrypt the compressed ECG for protection of patient's privacy, upholding HIPAA regulations. The compressed (and encrypted) ECG packets being smaller in size, transmit faster to the CVD monitoring agencies (like hospital or doctor). The receiver then performs faster patient authentication and diagnosis with a new breed of proposed algorithms. Therefore, faster patient care is achieved with our innovative model.



## Appendix A

# Definitions of Selected Abbreviations

**3G** : The third generation of developments in wireless technology, especially mobile communications

**ABT**: Amplitude based technique, a technique used for QRS Complex detection

**AES**: Advanced Encryption Standard is a symmetric key encryption adopted by US Government

**ANS**: Autonomic Nervous System is part of the peripheral nervous system that acts as a control system functioning mostly below the level of consciousness

**API** : Application Programming Interface defines how to access a software based service

**BDA**: Bluetooth Device Address, a 6 byte long globally unique identifier for Bluetooth

## APPENDIX A. DEFINITIONS OF SELECTED ABBREVIATIONS

devices

**BSN:** Body Sensor Network, a network of ambulatory sensors (e.g. ECG sensor, movement sensor etc.) situated within a single human body

**CC:** Cross-Correlation, used for measuring the difference

**CLDC:** Connected Limited Device Configuration, a configuration of java based mobile devices

**CVD:** Cardiovascular Disease (i.e. disease of the heart) between two ECG signals in [Chan et al., 2008]

**DDoS:** Distributed Denial of Service Attack, an attempt to make a computer resource unavailable to its intended users

**DES:** Data Encryption Standard is a complete description of a mathematical algorithm for encrypting and decrypting binary coded information

**DM:** Data Mining, a computational approach that can be used for making sense out of unstructured data

**DMA:** Data Mining Agent

**ECG:** Electrocardiogram, graphical display of the electrical activity of the heart

**EEG :** Electroencephalogram is a device that records the electrical activities of different parts of the brain

## APPENDIX A. DEFINITIONS OF SELECTED ABBREVIATIONS

**EM:** Expectation Maximization, is a data mining technique that has been used within this thesis for ECG based biometric and abnormality detection

**EMG :** Electromyography is a diagnostic test that records the electrical activities of muscles

**FDBT:** First Derivative based Technique, an algorithm for QRS complex detection

**FMR:** False Match Rate, a metric used for performance comparison of biometric modalities

**FNMR:** False Non Match Rate, a metric used for performance comparison of biometric modalities

**GSM :** Global System for Mobile Communication, a popular standard for mobile telephony system

**HIPAA:** Health Insurance Portability and Accountability Act (HIPAA) of United States in 1996

**HR:** Heart Rate, the number of heart beats per Minute

**HTTP:** Hyper Text Transfer Protocol, a popular networking protocol

**J2ME:** Java 2 Micro Edition, a platform for mobile computation. Most of our programming on mobile phones was performed with J2ME using NetBeans environment

**JCP:** Java Community Process, a formalized process that allows interested parties to get involved in the definition of future versions and features of the Java platform

**JSR:** Java Specification Requests, the formal documents that describe proposed specifications and technologies for adding to the Java platform

## APPENDIX A. DEFINITIONS OF SELECTED ABBREVIATIONS

**KVM:** Kilobyte Virtual Machine, a java runtime environment for miniature devices

**LZW:** Lempel-Ziv-Welch Algorithm, a common compression technique

**MIDP:** Mobile Information Device Profile, a specification published for the use of Java on embedded devices such as mobile phones

**MMS:** Multimedia Messaging Service, a popular telecommunication protocol

**NFC :** Near Field Communication is a data transmission scheme based on radio frequency

**NSRDB:** Normal Sinus Rhythm Database, an ECG repository containing normal ECG segments

**NOp/S:** Number of Operations per Second, a metric used for measuring the complexity of an algorithm

**PDM:** Polynomial Distance Measurement, one of our mechanisms for ECG based biometric on plain ECG

**PRD:** Percentage Root-Mean-Square Deviation, used for measuring the difference between two ECG signals in [Chan et al., 2008]

**PIN:** Personal Identification Number, codes used for securing digital devices

**SpO<sub>2</sub> :** Oxygen Saturation measures the capacity of blood in transporting oxygen to other parts of a body from the lungs

**SAPA:** Scan Along Polynomial Approximation, a compression algorithm

**SDBT:** Second Derivative based Technique, an algorithm for QRS complex detection

## APPENDIX A. DEFINITIONS OF SELECTED ABBREVIATIONS

**SMS:** Short Messaging Service, a popular telecommunication protocol

**WDM:** Wavelet Distance Measurement, used for measuring the difference between two ECG signals in [Chan et al., 2008]

**WP:** Wavelet Packet, a signal processing technique based on Wavelet

**WSP:** Weighted Signal Processing, one of our mechanisms for ECG based biometric on plain ECG using PRD, CC and WDM

**ZOP:** Zero Order Prediction, a compression algorithm

# Bibliography

S. Abboud and D. Sadeh. The use of cross-correlation function for the alignment of ECG waveforms and rejection of extrasystoles. *Computers and Biomedical Research*, 17:258–266, 1984.

[Acc] - *The shifting burden of cardiovascular disease in Australia, A report of Heart foundation*. Access Economics Pty Limited, Accessed 2008. [Online]. Available at [http://www.heartfoundation.com.au/media/nhfa\\_shifting\\_burden\\_cvd\\_0505.pdf](http://www.heartfoundation.com.au/media/nhfa_shifting_burden_cvd_0505.pdf).

S. Akselrod, D. Gordon, F. A. Ubel, D. C. Shannon, A. C. Barger, and R. J. Cohen. Power spectrum analysis of heart rate fluctuation: A quantitative probe of beat to beat cardiovascular control. *Science*, 213(1981):220–222, Oct. 2007.

A. Alesanco, S. Olmos, R. S. H. Istepanian, and J. Garcia. Enhanced real-time ECG coder for packetized telecardiology applications. *IEEE Transactions on Information Technology in Biomedicine*, 10(2), Apr. 2006.

[Ali] - *Alive Heart Monitor*. Alive Technologies, Accessed 2009. [Online]. Available at <http://www.alivetec.com/>.

## BIBLIOGRAPHY

- R. A. Balda. The HP ECG analysis program, trends in computer-processed electrocardiograms. *J. H. van Bemmel and J. L. Willems, Eds. North Holland*, pages 197–205, 1977.
- G. D. Barlas, G. P. Frangakis, and E. S. Skordalakis. Dictionary based coding for ECG data compression. *Proceedings of Computers in Cardiology, London*, 1993.
- A. Bartolo, B. Clymer, R. Burgess, J. Turnbull, J. Golish, and M. Perry. An arrhythmia detector and heart rate estimator for overnight polysomnography studies. *Biomedical Engineering, IEEE Transactions on*, 48(5):513–521, May. 2001.
- L. Biel, O. Pettersson, L. Philipson, and P. Wide. ECG analysis: a new approach in human identification. *Instrumentation and Measurement, IEEE Transactions on*, 50(3):808–812, Jun. 2001. doi: 10.1109/19.930458.
- T. Blanchett and G. C. Kember. Klt-based quality controlled compression of single lead ECG. *IEEE Transactions on Biomedical Engineering*, 45(7), Jul. 1998.
- M. Blount et. al. Remote health-care monitoring using personal care connect. *IBM Systems Journal*, 46(1):95–113, Mar. 2007.
- E. Bradley et al. Achieving rapid door-to-balloon times: how top hospitals improve complex clinical systems. *Circulation*, 113(8):1079–1085, Mar. 2006.
- F. M. Bui and D. Hatzinakos. Biometric methods for secure communications in body sensor networks: Resource-efficient key management and signal-level data scrambling. *EURASIP Journal on Advances in Signal Processing*, 2008.

## BIBLIOGRAPHY

[Car] - *Cardionet: Get to the Heart of the Problem*. Cardionet, Accessed 2009. [Online].

Available at <http://www.cardionet.com/>.

[Cen] - *Health Insurance Portability Accountability Act of 1996 (HIPAA)*. Centers

for Medicare and Medicaid Services (CMS), Accessed 2008. [Online]. Available at:

<http://www.cms.hhs.gov/hipaageninfo>.

A. Chan, M. Hamdy, A. Badre, and V. Badee. Wavelet distance measure for person identification using electrocardiograms. *Instrumentation and Measurement, IEEE Transactions on*, 57(2):248–253, Feb. 2008. doi: 10.1109/TIM.2007.909996.

J. Chen, J. Ma, Y. Zhang, and X. Shi. ECG compression based on wavelet transform and golomb coding. *IEE Electronics Letters*, 42(6):322–324, 2006.

H. Cheng and X. Li. Partial encryption of compressed images and videos. *IEEE Transaction on Signal Processing*, 48(8):2439–2451, Aug. 2000.

H.-W. Chiu and T. Kao. A mathematical model for autonomic control of heart rate variation. *Engineering in Medicine and Biology Magazine, IEEE*, 20(2):69–76, Mar. 2001. doi: 10.1109/51.917726.

G. D. Clifford, F. Azuaje, and P. E. McSharry. *Advanced Methods and Tools for ECG Data Analysis*. Artech House Inc, Norwood, MA, USA, 2006. ISBN 978-1-4051-4440-7.

J. R. Cox and K. L. Ripley. Compact digital coding of electrocardiographic data. *Proceedings of VI International Conference on System Science*, Jan. 1973.



## BIBLIOGRAPHY

- Y. D.-Y., H. Chang, and Y. Xiong et al. C2004: first international signature verification competition. *In Proceedings 2004 Biometric Authentication: First International Conference (ICBA 2004), Hong Kong, China*, pages 16–22, Jul. 2004.
- Z. Dokur, T. Olmez, and E. Yazgan. Comparison of discrete wavelet and fourier transforms for ECG beat classification. *Electronics Letters*, 35(18):1502–1504, Sep. 1999. doi: 10.1049/el:19991095.
- K. Duda, P. Turcza, and T. P. Zielinski. Lossless ECG compression with lifting wavelet transform. *Instrumentation and Measurement Technology Conference Budapest, Hungary*, May. 2001.
- B. Filho, W. Viana, R. Andrade, and A. Monteiro. Pearl: a performance evaluator of cryptographic algorithms for mobile devices. *MATA 2004, LNCS 3284*, pages 275–284, 2004.
- G. Friesen, T. Jannett, M. Jadallah, S. Yates, S. Quint, and H. Nagle. A comparison of the noise sensitivity of nine qrs detection algorithms. *Biomedical Engineering, IEEE Transactions on*, 37(1):85–98, Jan. 1990.
- L. Gang, Y. Wenyu, L. Ling, Y. Qilian, and Y. Xuemin. An artificial-intelligence approach to ECG analysis. *Engineering in Medicine and Biology Magazine, IEEE*, 19(2):95–100, Mar. 2000. doi: 10.1109/51.827412.
- T. Gao, D. Greenspan, M. Welsh, R. Juang, and A. Alm. Vital signs monitoring and patient

## BIBLIOGRAPHY

- tracking over a wireless network. *Proceedings of the 27th Annual Conference of IEEE Engineering in Medicine and Biology, Shanghai, China*, pages 102–105, Sep. 2005.
- H. Gilbert. Data compression: Techniques and applications hardware and software considerations. *John Wiley and Sons Ltd.*, 1987.
- M. M. Goudarzi, M. H. Moradi, and A. Taheri. Efficient method for ECG compression using two dimensional multiwavelet transform. *Transactions On Engineering, Computing And Technology*, 2, Dec. 2004.
- O. Govrin, S. Sadeh, S. Akselrod, and S. Abboud. Cross-correlation techniques for arrhythmia detection using pr and pp intervals. *Computers and Biomedical Research*, 18:37–45, 1985.
- I. B. Group. Independent testing of iris recognition technology. *Final Report, NBCHC030114/0002*, May. 2005.
- M. Hall. Correlation-based feature selection of discrete and numeric class machine learning. *in (Working paper 00/08), Computer Science Working Papers, 2000, University of Waikato, Department of Computer Science*, 1999.
- P. S. Hamilton and W. J. Tompkins. Compression of the ambulatory ECG by average beat subtraction and residual differencing. *IEEE Transactions on Biomedical Engineering*, 38(3), Mar. 1991.
- P. S. Hamilton and W. J. Tompkins. Quantitative investigation of qrs detection rules using the mit/bih arrhythmia database. *Biomedical Engineering, IEEE Transactions on*, BME-33(12):1157–1165, Dec. 1986.

## BIBLIOGRAPHY

- J. Han and M. Kamber. *Data mining: Concepts and Techniques*. Morgan Kaufmann, 2006.
- Y. Hao, P. Marziliano, M. Vetterli, and T. Blu. Compression of ECG as a signal with finite rate of innovation. *Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th annual conference, Shanghai, China*, Sep. 2005.
- R. N. Horspool and W. J. Windels. An LZ approach to ECG compression. *Published in proceedings of 1994 IEEE Seventh Symposium on Computer-Based Medical Systems (CBMS'94), Winston-Salem, NC*, pages 71–76, Jun. 1994.
- H. S. Hou and H. C. Andrews. Cubic splines for image interpolation and digital filtering. *IEEE Transaction on Acoustics, Speech, Signal Processings*, ASSP-26:508–517, Dec. 1978.
- D. A. Huffman. A method for the construction of minimum-redundancy codes. *in Proceedings of IRE*, 40:1098–1101, Sep. 1952.
- K. Hung and Y. T. Zhang. Implementation of a wap-based telemedicine system for patient monitoring. *IEEE Transactions on Information Technology in Biomedicine*, 7(2):101–107, Jun. 2003.
- A. Ibaida, I. Khalil, and F. Sufi. Cardiac abnormalities detection from compressed ECG in wireless telemonitoring using principal components analysis (PCA). *International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2009. ISSNIP 2009.*, Dec. 2009.
- E. Ifeachor and B. Jervis. *Digital Signal Processing: A Practical Approach*. Wokingham, England: Addison-Wesley Publishing Company, 1993.

## BIBLIOGRAPHY

- J. M. Irvine, B. K. Wiederhold, L. W. Gavshon, S. A. Israel, S. B. mcGehee, R. Meyer, and M. D. Wiederhold. Heart rate variability: a new biometric for human identification. *International Conference on Artificial Intelligence, Las Vegas, Nevada*, pages 1106–1111, 2001.
- S. A. Israel, W. T. Scruggs, W. J. Worek, and J. M. Irvine. Fusing face and ECG for personal identification. in *Proceedings of 32nd IEEE Application of Imagery Pattern Recognition Workshop*, page 226231, 2003.
- S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, , and B. K. Wiederhold. ECG to identify individuals. *Pattern Recognition*, 38(1):133–142, 2005.
- R. Istepanian and A. Petrosian. Optimal zonal wavelet-based ECG data compression for a mobile telecardiology system. *Information Technology in Biomedicine, IEEE Transactions on*, 4(3):200–211, Sep. 2000.
- A. K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *IEEE Transaction on Circuit, Systems and Video*, 14:4–20, 2004.
- S. Jalaeddine, C. Hutchens, R. Strattan, and W. Coberly. ECG data compression techniques - A unified approach. *IEEE Transactions on Biomedical Engineering*, 37(4):329–343, Apr. 1990.
- Y. Jasemian and L. Arendt-Nielsen. Evaluation of a realtime, remote monitoring telemedicine system using the bluetooth protocol and a mobile phone network. *Journal of Telemedicine and Telecare*, 11(5):256–260, 2005.

## BIBLIOGRAPHY

- [JCP] - *List of all Java Service Requests (JSR)*. JCP, Accessed 2008. [Online]. Available at: <http://jcp.org/en/jsr/all>.
- T. Kanade and N. E. Jain. Addressing vulnerabilities of likelihood ratio based face verification. in *Proceedings of 6th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, LNCS 3546:426435, 2005.
- S. V. Kartalopoulos. Primer on cryptography in communications. *IEEE Communications Magazine*, Apr. 2006.
- I. Khalil and F. Sufi. Legendre polynomials based biometric authentication using qrs complex of ECG. *International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2008. ISSNIP 2008.*, pages 297–302, Dec. 2008a.
- I. Khalil and F. Sufi. Mobile device assisted remote heart monitoring and tachycardia prediction. *International Conference on Technology and Applications in Biomedicine, 2008. ITAB 2008.*, pages 484–487, May. 2008b.
- I. Khalil and F. Sufi. Cooperative remote video consultation on demand for e-patients. *Journal of Medical Systems*, 33(6):475–483, 2009.
- B. Kim, S. Yoo, and M. Lee. Wavelet-based low-delay ECG compression algorithm for continuous ECG transmission. *IEEE Transactions on Information Technology in Biomedicine*, 10(1):77–83, Jan. 2006.
- K. Kira and L. Rendell. A practical approach to feature selection. in *Proceedings of the ninth international workshop on Machine learning*, pages 249–256, 1992.

## BIBLIOGRAPHY

- M. Kumar, M. Weippert, R. Vilbrandt, S. Kreuzfeld, and R. Stoll. Fuzzy evaluation of heart rate signals for mental stress assessment. *Fuzzy Systems, IEEE Transactions on*, 15(5): 791–808, Oct. 2007.
- F. M. Kusumoto. *ECG Interpretation: From Pathophysiology to Clinical Application*. Springer, Pennsylvania, 2009.
- M. Kyoso. A technique for avoiding false acceptance in ECG identification. In *in Proceedings of IEEE EMBS Asian-Pacific Conference in Biomedical Engineering*, pages 190–191, 2003.
- M. Kyoso and A. Uchiyama. Development of an ECG identification system. In *in Proceedings of 23rd IEEE Engineering Medical Biology Conference*, volume 4, pages 3721–3723, 2001.
- T. Last, C. D. Nugent, and F. J. Owens. Multi-component based cross correlation beat detection in electrocardiogram analysis. *BioMedical Engineering OnLine*, 3(26), 2004.
- R.-G. Lee, K.-C. Chen, C.-C. Hsiao, and C.-L. Tseng. A mobile care system with alert mechanism. *IEEE Transactions on Information Technology in Biomedicine*, 11(5):507–517, Sep. 2007.
- W.-B. Lee and C.-D. Lee. A cryptographic key management solution for hipaa privacy/security regulations. *Information Technology in Biomedicine, IEEE Transactions on*, 12(1):34–41, Jan. 2008. doi: 10.1109/TITB.2007.906101.
- C. Lei, L. Shiyong, and J. Ram. Compressed pattern matching in dna sequences. *Computational Systems Bioinformatics Conference, 2004. CSB 2004. Proceedings. 2004 IEEE*, pages 62–68, Aug. 2004.

## BIBLIOGRAPHY

- D. Lemire, C. Pharand, J. Rajaonah, B. Dube, and A. LeBlanc. Wavelet time entropy, t wave morphology and myocardial ischemia. *Biomedical Engineering, IEEE Transactions on*, 47(7):967–970, Jul. 2000. doi: 10.1109/10.846692.
- C.-F. Lin and C.-S. Chung. A chaos base visual encryption mechanism in ECG medical signal. *in IFMBE Proceedings on World congress on Medical Physics and Biomedical Engineering 2006*, 14(4):2366–2369, 2007.
- T. H. Linh, S. Osowski, and M. Stodolski. On-line heart beat recognition using hermite polynomials and neuro-fuzzy network. *IEEE Transactions on Instrumentation and Measurement*, 52(4):1224–1231, Aug. 2003.
- M. L. Liou. Spline fit made easy. *IEEE Transaction on Computers*, C-15:522–527, 1976.
- Z. Lu, D. Kim, and W. Pearlman. Wavelet compression of ECG signals by the set partitioning in hierarchical trees algorithm. *IEEE Transactions on Biomedical Engineering*, 47(7):849–856, 2000.
- G. D. Luca, H. Suryapranata, J. P. Ottervanger, and E. M. Antman. Time delay to treatment and mortality in primary angioplasty for acute myocardial infarction: Every minute of delay counts. *Circulation*, 109:1223– 1225, 2004.
- A. Mahmood, C. Leckie, and P. Udaya. An efficient clustering scheme to exploit hierarchical data in network traffic analysis. *Knowledge and Data Engineering, IEEE Transactions on*, 20(6):752–767, Jun. 2008. doi: 10.1109/TKDE.2007.190725.
- D. Maio, D. Maltoni, R. Cappelli, J. Wayman, and A. Jain. Fv c2004: third fingerprint

## BIBLIOGRAPHY

- verification competition. *Proceedings of the First International Conference on Biometric Authentication*, 3072:1–7, 2004.
- M. Malik, T. Farrell, T. Cripps, and A. Camm. Heart rate variability in relation to prognosis after myocardial infarction: selection of optimal processing techniques. *European Heart Journal*, 10:1060–1074, 1989.
- Y. Mao and M. Wu. A joint signal processing and cryptographic approach to multimedia encryption. *IEEE Transaction on Image Processing*, 15(7):2061–2075, Jul. 2006.
- J. P. Martinez, R. Almeida, S. Olmos, A. Rocha, and P. Laguna. A wavelet-based ECG delineator: evaluation on standard databases. *IEEE Transactions on Biomedical Engineering*, 51(4):570–581, 2004.
- T. Matsumoto. Gummy finger and paper iris: An update. *in Proceedings of the 2004 Workshop on Information Security Research*, 2004.
- T. Matsumoto, K. Matsumoto, K. Yamada, and S. Hoshino. Impact of artificial gummy fingers on fingerprint systems. In *in Proceedings of SPIE*, volume 4677, page 275289, 2002.
- O. Meste, B. Khaddoumi, G. Blain, and S. Bermon. Time-varying analysis methods and models for the respiratory and cardiac system coupling in graded exercise. *Biomedical Engineering, IEEE Transactions on*, 52(11):1921–1930, Nov. 2005.
- S. G. Miaou and S. N. Chao. Wavelet-based lossy-to-lossless ECG compression in a unified vector quantization framework. *IEEE Transactions on Biomedical Engineering*, 52(3), Mar. 2005.



## BIBLIOGRAPHY

- S. G. Miaou and C. L. Lin. A quality-on-demand algorithm for wavelet-based compression of electrocardiogram signals. *IEEE Transactions on Biomedical Engineering*, 49(3), Mar. 2002.
- S.-G. Miaou, S.-T. Chen, and C.-L. Lin. An integration design of compression and encryption for biomedical signals. *Journal of Medical and Biological Engineering*, 22(4):183–192, 2002.
- G. B. Moody, K. Soroushian, and R. G. Mark. ECG data compression for tapeless ambulatory monitors. *Computers in Cardiology*, pages 467–470, 1998.
- K. Nandakumar, A. Jain, and S. Pankanti. Fingerprint-based fuzzy vault: implementation and performance. *IEEE Transactions on Information Forensics and Security*, 2(4):744–757, 2007.
- [Nex] - *NEXPERTS Web site*. Nexperts, Accessed 2008. [Online]. Available at: <http://www.nexperts.com/typo/>.
- [NFC] - *NFC Forum Web site*. NFC Forum, Accessed 2008. [Online]. Available at: <http://www.nfc-forum.org/>.
- [Off] - *Health Related Privacy Information for Australians*. Office of Privacy Commission, Accessed 2009. [Online]. Available at: <http://www.privacy.gov.au>.
- R. Ogden. *Essential Wavelets for Statistical Applications and Data Analysis*. Birkha user, Boston, pp 174203, 1997.
- P. Ortolani, A. Marzocchi, C. Marrozzini, T. Palmerini, F. Saia, F. Baldazzi, S. Silenzi, N. Taglieri, M. Bacchi-Reggiani, and G. Gordini. Usefulness of prehospital triage in pa-

## BIBLIOGRAPHY

- tients with cardiogenic shock complicating st-elevation myocardial infarction treated with primary percutaneous coronary intervention. *The American Journal of Cardiology*, 100(5):787–792, 2007.
- Y. Otsuka, H. Yokoyama, and H. Nonogi. A novel mobile telemedicine system for real-time transmission of out-of-hospital ECG data for st-elevation myocardial infarction. *Catheterization and Cardiovascular Interventions*, 2009. doi: 10.1002/ccd.22019.
- W. Philips. ECG data compression with time-warped polynomials. *IEEE Transactions on Biomedical Engineering*, 40(11):1095–1101, Nov. 1993.
- W. Philips. Adaptive noise removal from biomedical signals using warped polynomials. *IEEE Transactions on Biomedical Engineering*, 43(5):480–492, May. 1996.
- W. Philips and G. Jonghe. Data compression of ECG’s by high-degree polynomial approximation. *IEEE Transactions on Biomedical Engineering*, 39(4):330–337, Apr. 1992.
- P. Phillips, P. Grother, R. Micheals, D. Blackburn, E. Tabassi, and M. Bone. Facial recognition vendor test 2002, evaluation report. *March 2003; available online at <http://www.frvt.org/>*, Last accessed: Jan. 2009.
- [Phy] - *Physiologic signal archives for biomedical research*. PhysioBank, Accessed 2009. [Online]. Available at <http://www.physionet.org/physiobank/>.
- K. N. Plataniotis, D. Hatzinakos, and J. K. M. Lee. ECG biometric recognition without fiducial detection. *Proceedings of Biometrics Symposiums (BSYM), Baltimore, USA*, 2006.

## BIBLIOGRAPHY

- R. Poli, S. Cagnoni, and G. Valli. Genetic design of optimum linear and nonlinear qrs detectors. *IEEE Transactions on Biomedical Engineering*, 42(11):1137–1141, Nov. 1995.
- C. C. Y. Poon, Y. T. Zhang, and S. D. Bao. A novel biometric method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communication Magazine*, pages 73–81, 2006.
- B. Potter. Bluetooth vulnerabilities. *Network Security 2004*, 2004(3):4–5, May. 2004.
- [Pub] - *Health Insurance Portability and Accountability Act of 1996*. Public Law, 104th congress edition, 1996.
- D. Reynolds, W. Campbell, and T. Gleason et al. The 2004 mit lincoln laboratory speaker recognition system. *In Proceedings IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2005), Philadelphia, USA*, pages 177–180, Mar. 2004.
- I. M. Rezazadeh, M. H. Moradi, and A. M. Nasrabadi. Implementing of spiht and sub band energy compression (SEC) method on two-dimensional ECG compression: A novel approach. *Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th annual conference, Shanghai, China*, Sep. 2005.
- M. Robnik-Sikonja and I. Kononenko. An adaptation of relief for attribute estimation in regression. *in Proceedings of the Fourteenth International Conference on Machine Learning*, pages 296–304, 1997.
- P. Rossi, A. Casaleggio, M. Chiappalone, M. Morando, G. Corbucci, M. Reggiani, G. Sartori,

## BIBLIOGRAPHY

- and S. Chierchia. Computationally inexpensive methods for intra-cardiac atrial bipolar electrogram compression. *Europace*, 4:295–302, Nov. 2002.
- A. Ruha, S. Sallinen, and S. Nissila. A real-time microprocessor qrs detector system with a 1-ms timing accuracy for the measurement of ambulatory hrv. *Biomedical Engineering, IEEE Transactions on*, 44(3):159–167, Mar. 1997. doi: 10.1109/10.554762.
- A. Sandman and B. Sapir. Third order polynomial-its use in data compression. *Signal Processing*, 15:405–418, 1988.
- J. Scholl, J. Agre, and L. Clare. Wavelet packet based target classification schemes. *in Proceedings of the 1998 Meeting of the IRIS Specialty Group on Acoustic and Seismic Sensing, APL/Johns Hopkins University, Laurel MD, 29 September to 1 October 1998*, 1, 1998.
- S. Schuckers. Spoofing and anti-spoofing measures. *Information Security technical report*, 7(4):5662, 2002.
- S. Seydnejad and R. Kitney. Real-time heart rate variability extraction using the kaiser window. *Biomedical Engineering, IEEE Transactions on*, 44(10):990–1005, Oct. 1997. doi: 10.1109/10.634651.
- T. Shen and W. J. Tompkins. Biometric statistical study of one-lead ECG features and body mass index (BMI). *In the Proceedings of the 2005 IEEE EMBS Conference, Shanghai, China*, 2005.

## BIBLIOGRAPHY

- T. W. Shen. Biometric identity verification based on electrocardiogram (ECG). *PHD Dissertation, University of Wisconsin, Madison*, 2005.
- T. W. Shen, W. J. Tompkins, and Y. H. Hu. One-lead ECG for identity verification. *in Proceedings of 2nd Joint EMBS/BMES Conference*, pages 62–63, 2002.
- M. Sillesen, M. Sejersten, S. Strange, S. Nielsen, F. Lippert, and P. Clemmensen. Referral of patients with st-segment elevation acute myocardial infarction directly to the catheterization suite based on prehospital teletransmission of 12-lead electrocardiogram. *Journal of Electrocardiology*, 41(1):49–53, 2008.
- L. Srnmo and P. Laguna. *Bioelectrical Signal Processing in Cardiac and Neurological Applications*. Elsevier, Amsterdam, The Netherlands, 2003.
- F. Sufi. Mobile phone programming java 2 micro edition. *Proceedings of the 2007 International Workshop on Mobile Computing Technologies for Pervasive Healthcare, Phillip Island, Melbourne, Australia*, pages 64–80, Dec. 2007.
- F. Sufi and I. Khalil. Efficient transmission in telecardiology. *Mobile Web 2.0: Developing and Delivering Services to Mobile Phones, Book Edited by: Syed Ahson and Mohammad Ilyas, CRC Press*, Dec. 2010a.
- F. Sufi and I. Khalil. Secured transmission & authentication. *Mobile Web 2.0: Developing and Delivering Services to Mobile Phones, Book Edited by: Syed Ahson and Mohammad Ilyas, CRC Press*, Dec. 2010b.
- F. Sufi and I. Khalil. Efficient cardiovascular diagnosis. *Mobile Web 2.0: Developing and*

## BIBLIOGRAPHY

- Delivering Services to Mobile Phones, Book Edited by: Syed Ahson and Mohammad Ilyas, CRC Press, Dec. 2010c.*
- F. Sufi and I. Khalil. An automated patient authentication system for remote telecardiology. *International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2008. ISSNIP 2008.*, pages 279–284, Dec. 2008a.
- F. Sufi and I. Khalil. Diagnosis of cardiovascular abnormalities from compressed ECG: A data mining based approach. *9th International Conference on Information Technology and Applications in Biomedicine, Larnaca, Cyprus*, Nov. 2009a.
- F. Sufi and I. Khalil. Faster person identification using compressed ECG in time critical wireless telecardiology applications. *Journal of Network and Computer Applications, Elsevier*, 34(1):282–293, Jan. 2011a.
- F. Sufi and I. Khalil. A new feature detection mechanism and its application in secured ECG transmission with noise masking. *Journal of Medical Systems*, 33(2), Apr. 2009b.
- F. Sufi and I. Khalil. Enforcing secured ECG transmission for realtime telemonitoring: A joint encoding, compression, encryption mechanism. *Security and Communication Networks*, 1(5):389 – 405, 2008b.
- F. Sufi and I. Khalil. Diagnosis of cardiovascular abnormalities from compressed ECG: A data mining based approach. *IEEE Transaction in Information Technology in Biomedicine*, 15(1):33 – 39, Jan. 2011b.
- F. Sufi and I. Khalil. Diagnosis of cardiovascular abnormalities from compressed ECG: A

## BIBLIOGRAPHY

- data mining based approach. *9th International Conference on Information Technology and Application in Biomedicine, ITAB 2009, Cyprus.*, Nov. 2009c.
- F. Sufi, Q. Fang, I. Cosic, and R. Ferguson. Client side decompression technique provides faster dna sequence data delivery. *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the*, pages 2817–2820, 2005.
- F. Sufi, I. Cosic, and Q. Fang. Design and implementation of an intelligent agent system for genome data retrieval. *Biomedical and Pharmaceutical Engineering, 2006. ICBPE 2006. International Conference on*, pages 475–480, Dec. 2006a.
- F. Sufi, Q. Fang, S. Mahmoud, and I. Cosic. A mobile phone based intelligent telemonitoring platform. *Medical Devices and Biosensors, 2006. 3rd IEEE/EMBS International Summer School on ISSMDBS*, pages 101–104, Sept. 2006b.
- F. Sufi, Q. Fang, and I. Cosic. ECG R-R peak detection on mobile phones. *Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE*, pages 3697–3700, Aug. 2007.
- F. Sufi, I. Cosic, and Q. Fang. A mobile phone based remote patient assessment system. *International Journal of Cardiovascular Medicine*, 9(Supplement):8–9, 2008a.
- F. Sufi, Q. Fang, and I. Cosic. A mobile phone based intelligent scoring approach for assessment of critical illness. *International Conference on Technology and Applications in Biomedicine, 2008. ITAB 2008*, pages 290–293, May. 2008b.
- F. Sufi, I. Khalil, Q. Fang, and I. Cosic. A mobile web grid based physiological signal moni-

## BIBLIOGRAPHY

- toring system. *International Conference on Technology and Applications in Biomedicine, 2008. ITAB 2008.*, pages 252–255, May. 2008c.
- F. Sufi, S. Mahmoud, and I. Khalil. A wavelet based secured ECG distribution technique for patient centric approach. In *Medical Devices and Biosensors, 2008. ISSS-MDBS 2008. 5th International Summer School and Symposium on*, pages 301–304, Jun. 2008d.
- F. Sufi, S. Mahmoud, and I. Khalil. A novel wavelet packet based anti spoofing technique to secure ECG data. *International Journal of Biometrics*, 1(2), 2008e.
- F. Sufi, S. Mahmoud, and I. Khalil. A new ECG obfuscation method: A joint feature extraction & corruption approach. In *Technology and Applications in Biomedicine, 2008. ITAB 2008. International Conference on*, pages 334–337, May. 2008f.
- F. Sufi, Q. Fang, I. Khalil, and S. S. Mahmoud. Novel methods of faster cardiovascular diagnosis in wireless telecardiology. *IEEE Journal on Selected Areas in Communications*, 27(4):537–552, May. 2009a.
- F. Sufi, I. Khalil, and J. Hu. Chapter 17: Secure human identification. *Handbook of Information & Communication Security, Book Edited by: Peter Stavroulakis, Springer*, 2009b.
- F. Sufi, I. Khalil, and I. Habib. Polynomial distance measurement for ECG based biometric authentication. *Security and Communication Network*, 3(4):303–319, Jul. 2010a.
- F. Sufi, I. Khalil, and I. Habib. Cardioids-based faster authentication and diagnosis of remote cardiovascular patients. *Security and Communication Networks, Wiley InterScience (in Press)*, 2010b.



## BIBLIOGRAPHY

- F. Sufi, I. Khalil, and A. Mahmood. Compressed ECG biometric: A fast, secured and efficient method for identification of cvd patient. *Journal of Medical Systems*, DOI: /10.1007/s10916-009-9412-4 (in Press), 2010c.
- F. Sufi, A. Mahmood, and I. Khalil. A clustering based system for instant detection of cardiac abnormalities from compressed ECG. *Expert Systems with Applications*, Elsevier, 38(5):4705–4713, May. 2011.
- L. Talavera. Dependency-based feature selection for clustering symbolic data. *Intelligent Data Analysis*, 4(1/2000):19–28, 1999a.
- L. Talavera. Feature selection as a preprocessing step for hierarchical clustering. in *Proceedings of the Sixteenth International Conference on Machine Learning*, pages 389–397, 1999b.
- K.-A. Toh, X. Jiang, and W.-Y. Yau. Exploiting global and local decisions for multimodal biometrics verification. *IEEE Transactions on Signal Processing*, 52(10):3059–3072, 2004.
- K. Urar and Y. Z. Ider. Development of compression algorithm suitable for exercise ECG data. *Proceedings of the 23rd Annual EMBS International Conference, Istanbul, Turkey*, Oct. 2001.
- M. B. Velasco, F. C. Roldan, F. L. Ferreras, A. B. Santos, and D. M. Munoz. A low computational complexity algorithm for ECG signal compression. *Medical Engineering and Physics*, 26:553–568, 2004.
- Y. Wang, F. Agraftoti, D. Hatzinakos, and K. N. Plataniotis. Analysis of human electrocar-

## BIBLIOGRAPHY

- diagram for biometric recognition. *EURASIP Journal on Advances in Signal Processing*, 2008.
- J. J. Wei, C. J. Chang, N. K. Chou, and G. J. Jan. ECG data compression using truncated singular value decomposition. *IEEE Transactions on Information Technology in Biomedicine*, 5(4), Dec. 2001.
- M. Wickerhauser. *Adapted wavelet analysis from theory to software*. A Peters Wellesley, Massachusetts, (486p), 1994.
- C. P. Wu and C. C. J. Kuo. Design of integrated multimedia compression and encryption systems. *IEEE Transactions on Multimedia*, 7(5):829–839, Oct. 2005.
- G. Wubbeler, M. Stavridis, D. Kreiseler, R.-D. Bousseljot, and C. Elster. Verification of humans using the electrocardiogram. *Pattern Recognition Letters*, 28:1172–2275, 2007.
- F. Yu, H. Tang, V. Leung, J. Liu, and C. Lung. Biometric-based user authentication in mobile ad hoc networks. *Security and Communication networks*, 1:5–16, 2008.
- M. J. Yuan. Enterprise j2me: developing mobile java. *Upper Saddle River, NJ: Prentice Hall PTR*, c2004.
- T. Zhang, S. Simske, and D. Blakley. Scalable ECG compression for long-term home health care. *Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th annual conference, Shanghai, China*, Sep. 2005.
- H. Zhou, K. Hou, J. Ponsonnaille, L. Gineste, and C. Vaulx. A real-time continuous cardiac

## BIBLIOGRAPHY

- arrhythmias detection system: Recad. *Proceedings of the 27th Annual Conference of IEEE Engineering in Medicine and Biology, Shanghai, China*, pages 875–881, Sep. 2005.
- Y. Zigel, A. Cohen, and A. Katz. ECG signal compression using analysis by synthesis coding. *IEEE Transactions on Biomedical Engineering*, 47(10), Oct. 2000a.
- Y. Zigel, A. Cohen, and A. Katz. The weighted diagnostic distortion (WDD) measure, for ECG signal compression. *IEEE Transactions on Biomedical Engineering*, 47(11):1422–1430, Nov. 2000b.
- J. Ziv and A. Lempel. Compression of individual sequences via variable-rate coding. *IEEE Transactions on Information Theory*, 24(5):530–536, Sep. 1978.