DEVELOPMENT OF A CRYPTOGRAPHY MODEL BASED ON IMPROVED FILTERING, COMPRESSION AND ENCRYPTION TECHNIQUES FOR ECG SIGNAL PROCESSING

MUSTAFA EMAD HAMEED

DOCTOR OF PHILOSOPHY

2022

Faculty of Electronics and Computer Engineering

DEVELOPMENT OF A CRYPTOGRAPHY MODEL BASED ON IMPROVED FILTERING, COMPRESSION AND ENCRYPTION TECHNIQUES FOR ECG SIGNAL PROCESSING

Mustafa Emad Hameed

Doctor of Philosophy

2022

DEVELOPMENT OF A CRYPTOGRAPHY MODEL BASED ON IMPROVED FILTERING, COMPRESSION AND ENCRYPTION TECHNIQUES FOR ECG SIGNAL PROCESSING

MUSTAFA EMAD HAMEED

A thesis submitted
in fulfillment of the requirements for the degree of
Doctor of Philosophy

Faculty of Electronics and Computer Engineering

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2022

DECLARATION

I declare that this thesis entitled “An Enhanced Cryptography Model Based on Improved Filtering, Compression and Encryption Techniques for ECG Signal Processing“ is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : Mustafa Emad

Name : Mustafa Emad Hameed

Date : 23/06/2022

APPROVAL

I hereby declare that I have read this thesis and in my opinion, this thesis is sufficient in terms of scope and quality for the award of Doctor of Philosophy.

Signature : .....

Supervisor Name : Associate Professor Dr. Masrullizam Mat Ibrahim

Date : 24/6/2022

DEDICATION

This thesis is dedicated to my family and friends.

ABSTRACT

Electrocardiography is the process of producing an electrocardiogram (ECG) which is a convenient tool for identifying people with potential heart diseases which may need immediate referral to a hospital or emergency medical services in E-healthcare. The ECG signal remote monitoring application in the healthcare services face many challenges related to the real-time diagnosis. The noise cancellation of the ECG signal is critical for accurate extraction of useful heart data from ECG. Additionally, the continuous flow of signals may lead to a sheer increase in the volume of the data, the ECG data needs a large memory storage device. At the same time, security and privacy of the data is considered as a significant aspect of remote diagnosis medical application that further increases the volume of data sharing, including the risk factor. This research work proposed a model to combine approaches for ECG denoising, data encoding, and encryption. Further, improved ECG signal processing based on improved filtering, an adaptive lossless compression mechanism, and hybrid cryptography are proposed. For the denoising of the ECG signal, an enhanced and extended Kalman and adaptive Recursive Least Square (RLS) filtering have been used for signal filtering along with Discrete Wavelet Transform (DWT). The compression mechanism is performed using adaptive lossless compression based on Huffman encoding. Furthermore, to increase security, a cryptography mechanism has been employed using the Advanced Encryption Standard (AES) algorithm and Cipher Block Chaining (CBC) operation mode scheme with a 256-bit key. The Diffie-Hellman key exchange and Rivest Shamir Adleman (RSA) key generation algorithms have been used to authenticate the receiver, and key generation for encrypting and decrypting processes, respectively. Consequently, the main contributions of this research work include a high level of security, privacy, encoding with low error reconstruction along with reduced noise and processing time for the ECG signal in e-healthcare services. The proposed model is for denoising, assuring data security, and compression performance for ECG data storage and transmission on MIT-BIH and PTB Diagnostic ECG dataset. The experimental results show that the proposed system model is successfully the denoising, and secure storage and transmission of ECG data. Based on the simulation results show a decrease for SNR by SNRimp of 55 in dB, a significant improvement of 21.92 for MSE and good accuracy for PSNR and CC. Furthermore, the throughput average of CR is enhanced by 26.66 and 0.8416 for PRD compared with existing different compression schemes for the ECG signal. Finally, the proposed system model is utilized for high-level security against for various kinds of attacks such as denial-of-service (DoS), Distributed DoS, privacy attack, and Man-in-the-middle (MitM).

PEMBANGUNAN MODEL KRIPTOGRAFI BERASASKAN TEKNIK PENAMBAHBAIKAN PENAPISAN, PEMAMPATAN DAN ENKRIPSI UNTUK PEMPROSESAN ISYARAT ECG

ABSTRAK

Elektrokardiografi adalah proses menghasilkan elektrokardiogram (ECG) yang merupakan alat yang mudah untuk mengenal pasti pesakit yang berpotensi menderita penyakit jantung yang mungkin memerlukan rujukan segera ke hospital atau perkhidmatan perubatan kecemasan di E-penjagaan kesihatan. Aplikasi pemantauan jarak jauh isyarat ECG dalam perkhidmatan penjagaan kesihatan menghadapi cabaran yang banyak berkaitan dengan diagnosis terhadap masa nyata. Pembatalan hingar terhadap isyarat ECG sangat penting berguna untuk pengekstrakan dengan tepat data jantung dari ECG. Selain itu, aliran isyarat yang berterusan boleh menyebabkan peningkatan jumlah data, data ECG memerlukan peranti penyimpanan memori yang besar. Pada masa yang sama, keselamatan dan privasi data dianggap sebagai aspek penting dalam aplikasi diagnosis perubatan secara jauh yang meningkatkan lagi jumlah perkongsian data, termasuk faktor risiko. Penyelidikan ini mencadangkan model untuk menggabungkan pendekatan untuk penyahhingar ECG, pengekodan data, dan enkripsi. Selanjutnya, pemprosesan isyarat ECG yang lebih baik berdasarkan penapisan yang lebih baik, mekanisme suai pemampatan tanpa kerugian, dan kriptografi hibrid dicadangkan. Untuk pemberian isyarat ECG, penyaringan Kalman dan penyesuaian Recursive Least Square (RLS) yang disempurnakan dan diperluas telah digunakan untuk penyaringan isyarat bersama dengan Discrete Wavelet Transform (DWT). Mekanisme pemampatan dilakukan menggunakan pemampatan tanpa kerugian suai berdasarkan pengekodan Huffman. Selanjutnya, untuk meningkatkan keselamatan, mekanisme kriptografi telah digunakan dengan menggunakan algoritma Advanced Encryption Standard (AES) dan skema mod operasi Cipher Block Chaining (CBC) dengan kunci 256-bit. Algoritma penjanaan kunci Diffie-Hellman dan Rivest Shamir Adleman (RSA) telah digunakan untuk mengesahkan penerima, dan penjanaan kunci masing-masing untuk proses penyulitan dan penyahsulitan. Oleh itu, sumbangan utama penyelidikan ini merangkumi tahap keselamatan, privasi, pengekodan yang tinggi dengan penyusunan semula ralat yang rendah bersama dengan pengurangan bunyi dan masa pemprosesan untuk isyarat ECG dalam perkhidmatan e-penjagaan kesihatan. Model yang dicadangkan adalah untuk penyahhingar, menjamin keselamatan data, dan prestasi mampatan untuk penyimpanan dan penghantaran data ECG pada set data ECG MIT-BIH dan PTB Diagnostik. Hasil eksperimen menunjukkan bahawa model sistem yang dicadangkan berjaya dalam menyahingar, dan penyimpanan dan penghantaran data ECG yang selamat. Berdasarkan hasil simulasi menunjukkan penurunan untuk SNR oleh SNRimp 55 dalam dB, peningkatan yang signifikan 21.92 untuk MSE dan ketepatan yang baik untuk PSNR dan CC. Tambahan pula, rata-rata throughput CR ditingkatkan sebanyak 26.66 dan 0.8416 untuk PRD berbanding dengan skema mampatan yang berbeza untuk isyarat ECG. Akhirnya, model sistem yang dicadangkan boleh digunakan untuk keselamatan tingkat tinggi untuk pelbagai jenis serangan seperti penolakan-perkhidmatan (DoS), Distribusi DoS, serangan privasi, dan Man-in-the-middle (MitM).

ACKNOWLEDGEMENTS

In the Name of Allah, the Most Gracious, the Most Merciful

First and foremost, I would like to thank and praise Allah the Almighty, and His final messenger Prophet Muhammad (peace be upon him), for everything I received since the beginning of my life. I would like to extend my appreciation to the Universiti Teknikal Malaysia Melaka (UTeM) for providing the research platform.

My utmost appreciation goes to my main supervisor, Associate Professor Dr. Masrullizam Mat Ibrahim, for all his support, advice and inspiration. His constant patience for guiding and providing priceless insights will forever be remembered. I am also thankful to my co-supervisor, Associate Professor Dr. Nurulfajar Abd Manap.

Lastly, I would like to thank my beloved wife, Samar Farhan Mahmood, for her encouragement and availability during hard times. My eternal love to my son, Hassan M and my daughter Jumana M, for there adorable acts that make me comfortable. I am also thankful to my father Emad H, mother Izdehar J, sisters, in-laws and all of their kids for their encouragement and patience shown during my course of studies. Finally, thanks to the entire lab staff FKEKK who had provided me the assistance, support whenever required. I am also thankful to my friends for their technical support and inspiration to embark on my study.

.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

2D-SPIHT	-	2D Set Partitioning in Hierarchical Tree
AWGN	-	Additive White Gaussian Noise
AES	-	Advanced Encryption Standard
BW	-	Baseline Wander
CPET	-	Cardiopulmonary Exercise Test
CVD	-	Cardiovascular Disease
CBC	-	Cipher Block Chaining
CN	-	Colour Noise
CS	-	Compressed Sensing
CR	-	Compression Ratio
CC	-	Cross-Correlation
DTLS	-	Datagram Transport Layer Security
DLP	-	Discrete Logarithm Problem
DWT	-	Discrete Wavelet Transform
ECG	-	Electrocardiogram
EM	-	Electrode Movement
EEG	-	Electroencephalogram
EMG	-	Electromyography
EHRs	-	Electronic Health Records
E-healthcare	-	Electronic Healthcare

ECC	-	Elliptic-curve Cryptography
EMD	-	Empirical Mode Decomposition
EKF	-	Extended Kalman Filter
AFD	-	Fourier Decomposition
IFP	-	Integer Factorization Problem
IMF	-	Intrinsic Mode Functions
LMS	-	Least Mean Squares Filters
LQE	-	Linear Quadratic Estimation
MSE	-	Mean Squared Error
MCU	-	Micro-Control Unit
MC	-	Muscle Contraction
NIST	-	National Institute of Standard and Technology
OSOS	-	Optimum Sparsity Order Selection
PSNR	-	Peak Signal to Noise Ratio
PRD	-	Percentage Root-mean-square Difference
RTOS	-	Real-Time Operating System
RSA	-	Rivest-Shamir-Adleman
RLS	-	Recursive Least Square
SAS	-	Security Attack Scenario
SNR	-	Signal to Noise Ratio
SVD	-	Singular Value Decomposition
SNRimp	-	SNR improvement
SS	-	Symbol Substitution
VLSI	-	Very-Large-Scale Integration
WDR	-	Wavelet Differential Reduction

WBSNs	-	Wireless Body Sensor Networks
WHO	-	World Health Organization

LIST OF APPENDICES

LIST OF PUBLICATIONS

Hameed, M.E., Ibrahim, M.M., and Manap, N.A., 2018. Review on Improvement of Advanced Encryption Standard (AES) Algorithm based on Time Execution, Differential Cryptanalysis and Level of Security. *Journal of Telecommunication, Electronic and Computer Engineering*, 10 (1), pp. 139–145.

Hameed, M.E., Ibrahim, M.M., and Manap, N.A., 2019. Compression and encryption for ECG biomedical signal in healthcare system. TELKOMNIKA, 17 (6), pp. 2826–2833.

Hameed, M.E., Ibrahim, M.M., Manap, N.A., and Ali, A., 2020. An Enhanced Cryptography Model Based on Improved Filtering, Compression and Encryption Techniques for ECG signal Processing. Sensors, pp. 1–27. (In Review).

Hameed, M.E., Ibrahim, M.M., Manap, N.A., and Attiah, M.L., 2019. Comparative study of several operation modes of AES algorithm for encryption ECG biomedical signal. International Journal of Electrical and Computer Engineering, 9 (6), pp. 4850–4859.

Hameed, M.E., Ibrahim, M.M., Manap, N.A., and Mohammed, A.A., 2020. A lossless compression and encryption mechanism for remote monitoring of ECG data using Huffman coding and CBC-AES. Future Generation Computer Systems, pp. 829–840.

Hameed, M.E., Ibrahim, M.M., Manap, N.A., and Mohammed, A.A., 2020. An enhanced lossless compression with cryptography hybrid mechanism for ECG biomedical signal monitoring. International Journal of Electrical and Computer Engineering, 10 (3), pp.3235–3243.

CHAPTER 1

INTRODUCTION

1.1 Research Background

Electronic healthcare (E-healthcare) is pricted to be the next big thing in the healthcare system. This system assists every kind of patient and supports their vital daily life activities. Due to its importance, the healthcare applications and accessibility to the E-healthcare system start revolutionizing healthcare services (McMullen et al., 2014). The researchers and the analysts recognized the remote monitoring system for the E-healthcare platform as one of the most advanced innovations with the potential to influence the health, security, and efficiency of billions of people and a significant economic impact (Yüksel et al., 2017). E-healthcare primarily consists of physical objects embedded with sensors, actuators, electronic systems and have the capabilities for data communication, which are further connected to data transmission networks.

There are many types of data for the E-healthcare remote monitoring system, including electroencephalogram (EEG), Electrocardiogram (ECG), heart rate, blood pressure, blood sugar, to name a few (Paré et al., 2010; Ghebreyesus et al., 2018). The E-healthcare remote monitoring system applications assist us in tracking our health condition so that possible problems may be recognized early and modifications can be made to enhance specific elements of our health (Rodríguez and Riveill, 2011). Others render healthcare devices and systems more accessible to people who live in remote areas or perhaps could not visit medical centres in person.

The e-healthcare system includes tools that send patients' data to an intermediate device such as pc, smartphone, or other smart devices connected by wireless technologies such as Wi-Fi, Bluetooth, NFC, or RFID. The hospital or cloud server receives the patient data from intermediate devices by a communication network. A typical E-healthcare system shown in Figure 1.1.

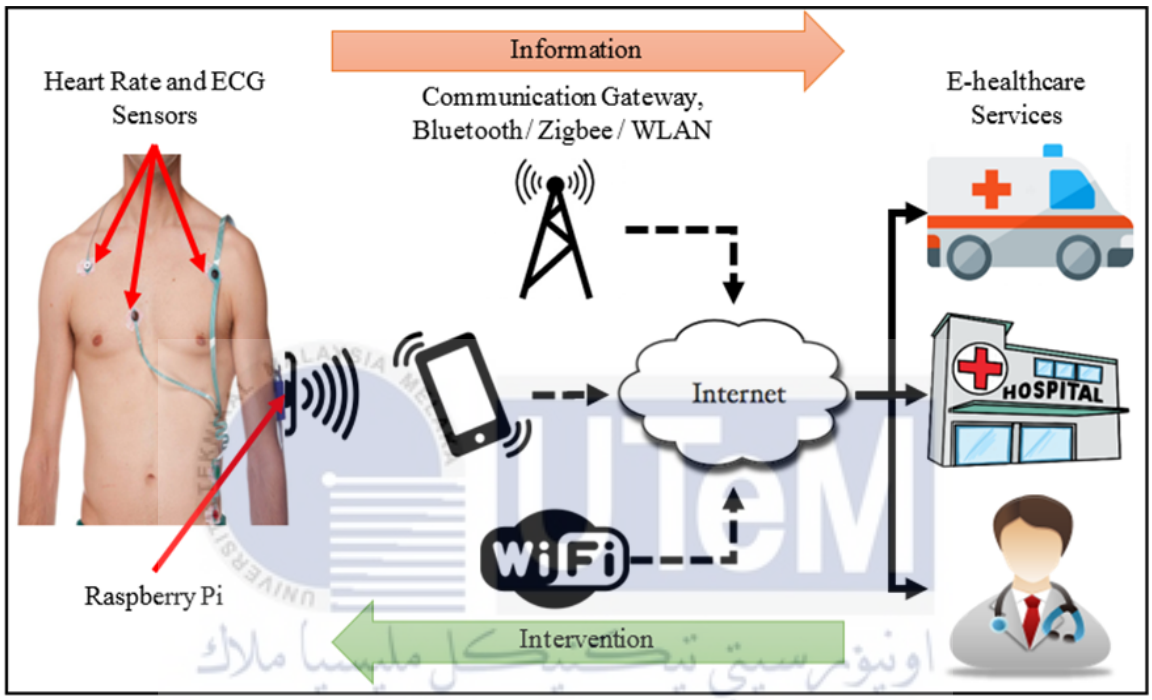

Figure 1.1 E- Healthcare remote monitoring system

The researchers give due importance to biomedical signal analysis due to their association with practical applications towards developing devices for clinical diagnosis, tracking of patients, and patient management. The processing of biomedical signals primarily consists of the extraction stage to extract the points of concern in the signals indicating the body circumstances, such as the start of the Electromyography (EMG) signal indicate muscle activation and the variation of the heart rate from the ECG signal (Dey et al., 2018). The ECG is broadly used in pathology to monitor minute electrical changes on patient's skin, which arise due to heart activities measured using electrodes (also referred to as channels).