TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 12029 - 12034

Secured Electrocardiograph (ECG) Signal Using Fully Homomorphic Encryption Technique

Muhammad Umair Shaikh, Faculty of Engineering, University Putra Malaysia (UPM), Serdang, Malaysia. Email: mushaikh1986@gmail.com

Siti Anom Ahmad, Dept. of Electrical and Electronic Engineering, Faculty of Engineering/ Malaysian Research Institute on Ageing (MyAgeing™), University Putra Malaysia (UPM), Serdang, Malaysia. Email: sanom@upm.edu.my

Wan Azizun Wan Adnan, Faculty of Engineering, University Putra Malaysia (UPM), Serdang, Malaysia.

Article Info
Volume 82
Page Number: 12029 - 12034
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 21 February 2020*

Abstract

Abstract: Digital signal processing and data analysis frequently utilized strategies in biomedical engineering research. This proposed study describes the steps of digital signal processing on electrocardiogram (ECG) and the security of the ECG signal by using Fully Homomorphic Encryption (FHE). Sharing the patient's information through the Internet of Thing (IoT) for faster diagnosis has security and privacy issues. The present situation demands extremely secured details of patients. Consequently, securing the patient's information from ransomware is the main challenge in the healthcare industry. Development of secured ECG signal is essential to protect patients' confidentially and to prevent mistreatment. The proposed encryption scheme FHE is performed on the encrypted ECG data where FHE can be applied in any system by using a various public key algorithm. The secured ECG transmission system will work on the fourth industrial revolution with four major themes: speed of care, ability to manage illness, the role of patient and the relationship between healthcare and service provider. Secure ECG signal provides innovation in multiple healthcare sectors such as medical research, patient care and hospital database. For the digital signal processing on ECG, QRS complex method will be used to display heart rate (HR) because it is the most visually obvious part of the ECG tracing and it is easy to encrypt the visual part in ECG tracing. This study demonstrates the implementation of FHE techniques that is Gentry algorithms in securing ECG signal transmission

Keywords: *Signal analysis, Electrocardiograph, Gentry encryption technique.*

I. INTRODUCTION

Cardiac muscle is a type of involuntary striated muscle found in the walls and histologic foundation of the heart, specifically the myocardium which causes the heart beats about 100,000 times each day nonstop. The electrocardiogram (ECG) wave-form recorded on the body surface is produced by the electrical activities associated with the muscles contraction and relaxation of the atria and ventricles. The ECG is the wave representation of the heart activity. The electrical current generated by the heart is commonly measured by an array of electrodes placed on the human body and the resulting tracing is in the form of ECG wave. There are many widespread applications for ECG signal such as clinical diagnosis, understanding of the physiology of cardiac arrhythmias, interpretation for medical researcher and human-machine interface. The use of ECG has some advantages such as providing a safe and easy method that demonstrates the electrical current and

January - February 2020
ISSN: 0193 - 4120 Page No. 12029 - 12034

potential difference generated by the heart. Many techniques have been proposed to improve the security of the ECG signal. The security feature protects the confidentiality and authenticity of the human ECG signal. Where the FHE technique is used for secured transmission of ECG.

Table I: Standard interval (SI) for ECG waveform

ECG waveform points	Standard Interval
PQ (PR)	0.10 ÷ 0.20s
QRS	0.06 ÷ 0.10s
QTC	0.32 ÷ 0.42
ST	< |0.05| mV

Table I displays the PQRST parameters of ECG. Our proposed study is focused on the QRS complex method. The QRS complex ordinarily views in 80% to 95% of ECGs. It is the most visible part of the ECG. Different arrhythmia can be diagnosed by using the QRS complex. The ECG voltage estimates the part of the following after the T wave and preceding the next P wave. Heart rate (HR) can be calculated by using R to R interval.

Security for healthcare database has the highest priority set by the clients and providers. The office of civil rights reported that there is in excess of 112 million patient records were undermined in 2015 [1]. From that point forward, cybercriminals have turned out to be much progressively mindful of the estimation of social insurance records.

This emergency in the medical services industry requires imaginative arrangements. One inventive arrangement might be less organized, that is reinforcement and recuperation. In any case, numerous variations erase shadow duplicates and some even distinguish document recuperation programming. The proposed study designs the secured ECG signal for patient safety.

This paper is organized as follows: Section 2 discussed briefly previous related work on ECG. Section 3 introduced our proposed methodology consisting of QRS complex detection and the encryption of ECG using FHE. Simulations results are presented and discussed in section 4 and finally, section 5 presents the conclusion.

A brief introduction of the QRS complex method is studied first then the ECG recording techniques and security techniques are reviewed subsequently. This study focuses on improving the security of the ECG signal.

II. RELATED WORK

The self-diagnostic ability of ECG signal is crucial in the process of detecting the ECG arrhythmias. On top of that, the transmission of the ECG must be secured in order to protect the patient's information.

Vithya et al. [2] used the RSA algorithm to secure the ECG distribution for telemedicine application. The approach is based on the SET PARTITIONING IN HIERARCHICAL TRESS (SPHIT) where RSA encryption is implemented for encrypting ECG signal. The RSA encryption and decryption algorithm need a lot of calculation and the speed is slow compared with the symmetric cryptographic [3]. RSA technique allows performing either addition or multiplication on encrypted data whereas FHE such as Gentry algorithm allows performing both addition and multiplication simultaneously. Hence, the signal is more secured.

A system for long term real-time continuous monitoring of cardiac patients based on GSM and wireless technology has been proposed. The proposed system has enhanced the mobility for both medical practitioners and patients [4] and also enabled the medical practitioner to be monitor the patients' cardiac reading remotely. A ubiquitous healthcare system dedicated to real-time continuous cardiac arrhythmia detection and monitoring under the surveillance of a medical practitioner has also been implemented [5].

This study covers a greater scope than the Vithya, Sukanesh and Li research. It explored the QRS wave indicator calculation so as to recognize diverse QRS and ECG investigation. Furthermore, the ECG signal is suggested to be encrypted by using FHE technique

January - February 2020
ISSN: 0193 - 4120 Page No. 12029 - 12034

to make it more secured. This helps in data sharing application within the healthcare industry such as telemedicine. To the best of our knowledge, none of the ECG systems discussed so far has incorporated security techniques using FHE relating to the authentication and secure data storage, transmission or reception issues.

III. METHODOLOGY

Our research is divided into two parts. The first part is QRS complex detection and the second part is the encryption of ECG using FHE technique to make the signal more secured and difficult for a hacker to hack the information.

A. QRS Complex Detection

One complete cardiac cycle consists of the P wave, QRS complex and T wave. The QRS complex is the most visual part of the ECG tracing. Different arrhythmia can be detected by using this complex. There are various algorithms used for the detection of the QRS complex. Different algorithms have different performance and accuracy. After comparing different QRS complex detection methods "Pan and Tompkins" method is the best choice because of higher sensitivity and predictivity.

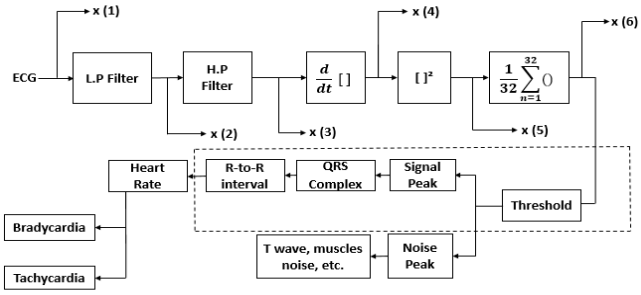

Fig. 1. Stages of high-speed QRS detection that includes x(1): Input ECG signal, x(2): Low Passed ECG, x(3): Band Passed ECG, x(4): Differentiated ECG, x(5): Squaring output, x(6): Window Integrated output [6].

The dotted line in fig. 1. Demonstrates the activity done by utilizing the encryption qualities and after decryption can get the outcome in the form of a pulse. A survey of literature review for the detection of QRS complex shows that Pan and Tompkins algorithm is one of the important algorithms for the detection of the QRS complex [7]. The algorithm has two stages. The first stage is the preprocessing stage in which the signal is prepared for later detection, removing noise, smoothing the signal and amplifying the QRS slope and width. The second stage is the decision stage. In this stage, thresholds are applied to the signal in order to remove noise peaks and consider only signal peaks [6]

B. Fully Homomorphic Encryption (FHE)

The encryption of the ECG is derived from Gentry FHE Cryptosystem proposed by Jian Li Danjie Song in 2012 [8] which is known as SDC scheme. The SDC scheme only has to transmit a constant big integer q to the weak server, which makes it more secured. The detail of the SDC scheme is as follows;

KeyGen (p): The key p is a random odd integer of P-bit.

Encrypt (p, m): To encrypt a bit m ε {0, 1}

Cipher (c) = m + p + r * p * q

where r is a random number of R-bit and q is a constant Q-bit big integer.

Decrypt (p, c): Output (c mod p)

The SDC scheme for the additively homomorphic property is given below;

c1 = m1 + p + r1 * p * q (1)

c2 = m2 + p + r2 * p * q (2)

Here, in our case m1 and m2 are x(5) squaring output and moving window integrated output x(6) in ECG signal as shown in fig. 1 c1 and c2 are ciphertexts of these messages after encryption.

To check additively homomorphic property:

c3= c1+c2= (m1+m2) + (r1+r2)*p*q* 2p (3)

January - February 2020
ISSN: 0193 - 4120 Page No. 12029 - 12034

For decryption,

$$m3 = c3 \bmod p = m1 + m2 \qquad (4)$$

The FHE encryption technique will apply on squaring output x(5) and moving window integrated output x(6). After encrypting the signals x(5) and x(6) by using FHE technique the signal will be unreadable and send to the authorized person. By using the private key the authorized person will decrypt the result and display regular or irregular heartbeat. The heartbeat is irregular if its value is below 60bpm (bradycardia) and above 100bpm (tachycardia). This result will help for further analysis.

IV. SIMULATION RESULTS AND DISCUSSION

Arrhythmia datasets were downloaded from the MIT-BIH database for QRS detection using Pan and Tompkins Algorithm. The signal length is 21600 samples with a sampling rate of 360 Hz for each of ECG recording. Fig.2. shows an input of record 100 ECG with processing step

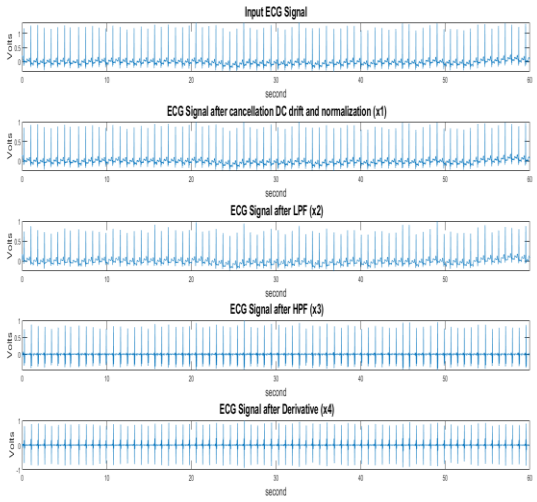

Fig. 2. Input ECG signal from the MIT-BIH database with processing steps for record 100.

In the preprocessing stage initially, low and high pass filter are used to remove the noise and any existing artifacts. The second step is to find the high slope for distinguishing the QRS complexes from other ECG waves. Then, step to step squaring of the sample is used to make all data positive and accentuates the higher frequencies in the signal. After that waveform passes through the moving window integrator are squared.

After squaring output x(5) and moving window integrated output x(6), the encryption-decryption algorithm for two points x(5) and x(6) are used. Fig .3 shows the encryption of signal x(5) and x(6). By encrypting the signal x(5) and x(6) the signal will be changed and used the encrypted signal for further analysis. After that Gentry FHE of SDC scheme is used to perform the homomorphic operation of ECG signal of addition as shown in fig. 3.

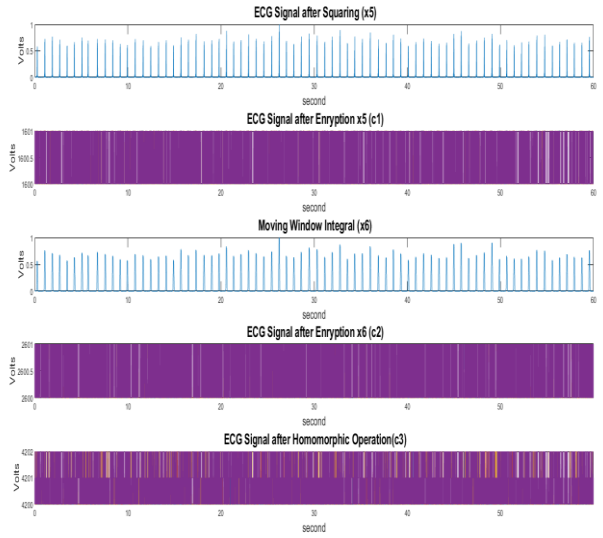

Fig. 3. Encrypted ECG signal

Fig. 3. shows the result in the form of cipher1 (c1) and cipher2 (c2) which is the encryption of x(5) and x(6) and c3 after the homomorphic operation. After the homomorphic operation, the system will request the private key which makes the system more secured as shown in fig. 4. By providing the correct private key, the system will display the result in the form of normal and abnormal heartbeat. If the heartbeat is abnormal, it will display two types of arrhythmias i.e. bradycardia (heartbeat below 60BPM) and tachycardia (heartbeat above 100BPM).

January - February 2020
ISSN: 0193 - 4120 Page No. 12029 - 12034

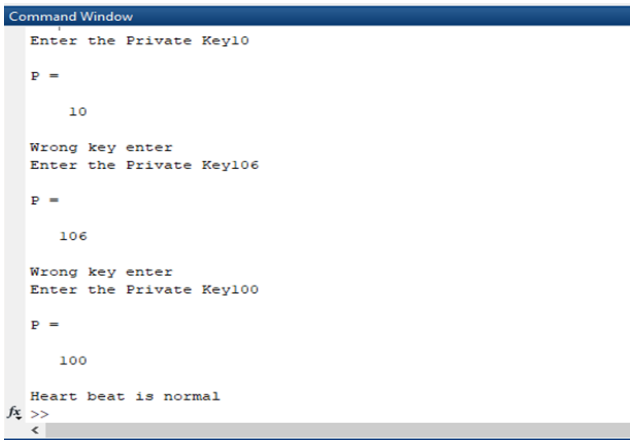

Fig. 4. Display result after providing the private key.

A. Speed Execution Test

The designed algorithm is performed using MATLAB (R2019a) with an Intel Core (TM) i5 3.10 GHz processor, 8 GB RAM, and 500 GB hard disk running on a windows 10. The simple and fast proposed algorithm is applied to 29 random different ECG signal from the MIT-BIH arrhythmia database. The average encryption and decryption time spent on the proposed algorithm depends on the input of private key from the user as shown in fig. 4. It is found that the total time for encryption and decryption process is less than 0.6 second which is better than the (Zhai and Amine 2017[9], Mathivanan and Balaji [10], Jati and Rizqy [11]).

The obtained results are summarized in Table 2.

Table II. Result comparison with the MIT-BIH database with FHE technique

Record No.	MIT-BIH Arrhythmia Database	Proposed methodology mean HR	Result
Record 100	70-89 bpm	73.5 bpm	Normal
Record 101	55-79 bpm	64.86 bpm	Normal
Record 102	72-78 bpm	80 bpm	Normal
Record 103	62-92 bpm	67.9 bpm	Normal
Record 104	69-82 bpm	71 bpm	Normal
Record 105	78-102bpm	58 bpm	Abnormal (Bradycardia)
Record 106	49-87 bpm	72 bpm	Normal
Record 108	44-78 bpm	60.5 bpm	Normal
Record 109	77-101 bpm	88 bpm	Normal
Record 111	64-82 bpm	69 bpm	Normal
Record 112	74-91 bpm	84 bpm	Normal
Record 113	48-87 bpm	59 bpm	Abnormal (Bradycardia)
Record 114	51-82 bpm	57 bpm	Abnormal (Bradycardia)
Record 115	50-84 bpm	69 bpm	Normal
Record 116	74-86 bpm	78 bpm	Normal
Record 117	48-66 bpm	49 bpm	Abnormal (Bradycardia)
Record 118	54-91 bpm	72 bpm	Normal
Record 121	55-83 bpm	58 bpm	Abnormal (Bradycardia)
Record 122	67-97 bpm	84 bpm	Normal
Record 123	41-65 bpm	55 bpm	Abnormal (Bradycardia)
Record 124	47-64 bpm	48 bpm	Abnormal (Bradycardia)
Record 201	31-61 bpm	140 bpm	Abnormal (Tachycardia)
Record 210	63-158 bpm	109 bpm	Abnormal (Tachycardia)
Record 213	101-113bpm	110 bpm	Abnormal (Tachycardia)
Record 215	81-215 bpm	122 bpm	Abnormal (Tachycardia)
Record 231	49-69 bpm	68 bpm	Normal
Record 232	24-28 bpm	50 bpm	Abnormal (Bradycardia)

V. CONCLUSION

In this study, the signal processing of the ECG signal and the FHE technique are proposed for secured transmission of ECG. The proposed approach can provide the same result without sacrificing the compression efficiency compared to

January - February 2020
ISSN: 0193 - 4120 Page No. 12029 - 12034

the unencrypted result. As a result, the output of the Pan and Tompkins algorithm for ECG signal processing using QRS complex with FHE technique shows the same sensitivity and predictivity. On the other hand, FHE provides a more secure signal because it allows performing both addition and multiplication simultaneously and can encrypt the signal. The security parameter in this investigation will verify the restorative information with the goal that the information isn't lost and to keep patient's data in a single place that helps the medical practitioner and researcher for further studies of arrhythmia detection.

VI. REFERENCES

[1] Kathleen Sebelius, Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA rules. 2nd edn." Fed. Regist. Vol. 78 No. 17, 2015.

[2] V.Kp. "Secured ECG Distribution using Compression and RSA Algorithm for Telemedicine Application. International Journal of recent technology and engineering, vol. 3, no. 2, pp. 46–48, 2014.

[3] NaQi. , Analysis and Research of the RSA Algorithm. Information Technology Journal, Volume 12 (9): 1818-1824, 2013.

[4] R. Sukanesh, A Portable Wireless ECG Monitoring System using GSM Technique with Real-Time Detection of Beat Abnormalities. International journal of engineering research, vol. 3, no. 2. Innovative Research Publications, 2014.

[5] J. Li., Ubiquitous health monitoring and real-time cardiac arrhythmias detection: a case study.Biomed. Mater. Eng., vol. 24, no. 1, pp. 1027–33, 2014.

[6] M. U. Shaikh, S. A. Ahmad, and W. A. Wan Adnan, "Investigation of data encryption algo-rithm for secured transmission of electrocardiograph (ECG) signals," 2018 IEEE EMBS Conf. Biomed. Eng. Sci. IECBES 2018 - Proc., pp. 274–278, 2019.

[7] S. L. Pingale, Using Pan Tompkin ' S Method, Ecg Signal Processing and Diagnose Various Diseases in Matlab, Proc. IRF Int. Conf., 2014.

[8] J. Li., A. Simple fully homomorphic encryption scheme available in cloud computing, Proc. - 2012 IEEE 2nd Int. Conf. Cloud Comput. Intell. Syst. IEEE CCIS 2012, vol. 1, pp. 214–217, 2013.

[9] X. Zhai, A. Ait Si Ali, A. Amira, and F. Bensaali, "ECG encryption and identification based security solution on the Zynq SoC for connected health systems," J. Parallel Distrib. Com-put., vol. 106, pp. 143–152, 2017.

[10] P. Mathivanan, A. B. Ganesh, and R. Venkatesan, "QR code–based ECG signal encryp-tion/decryption algorithm," Cryptologia, vol. 43, no. 3, pp. 233–253, 2019.

[11] G. Jati, A. R. Rachmasari, W. Jatmiko, P. Mursanto, and W. Sediono, "An efficient secure ECG compression based on 2D-SPIHT and SIT algorithm," Proc. - WBIS 2017 2017 Int. Work. Big Data Inf. Security., vol. 2018–January, pp. 155–160, 2018.

AUTHORS PROFILE

M Umair Shaikh is doing his Master of Engineering by research in Biomedical Engineering at Universiti Putra Malaysia. His research area is biomedical signal processing and signal encryption.

Siti Anom Ahmad is an Associate Professor at the Department of Electrical and Electronic Engineering, Faculty of Engineering, Universiti Putra Malaysia. She received her BEng in Electronic/ Computer from Universiti Putra Malaysia in 1999. Dr. Siti Anom received a Ph.D. in Electronics in 2009 and MSc in Microelectronics System Design in 2004 from the University of Southampton, UK. Her research interests are biomedical engineering, signal processing and intelligent control system. She has published more than 100 journal articles and proceedings in her field.

Wan Azizun Adnan obtained her first degree in Mathematics from the University of Southampton, UK in 1984 before obtaining her Master and Ph.D. in Computer Science at the Universiti of Malaya in 1996 and 2010 respectively. Currently, she is an Assoc. Professor at the Department of Computer and Communication System Engineering, Faculty of Engineering, Universiti Putra Malaysia. Her areas of interest and research are software development, watermarking and also biometrics. She has presented papers at conferences both home and abroad, published articles and papers in various journals related to her research areas