Pertanika J. Sci. & Technol. 28 (S2): 231 - 242 (2020)

PERTANIKA JOURNALS

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

# Secured Electrocardiograph (ECG) Signal Using Partially Homomorphic Encryption Technique–RSA Algorithm

**Muhammad Umair Shaikh[1], Wan Azizun Wan Adnan[3] and Siti Anom Ahmad[1, 2]***

*[1]Department of Electrical and Electronic Engineering, Faculty of Engineering, Universiti Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia*
*[2]Malaysian Research Institute on Ageing (MyAgeing™), Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia*
*[3]Department of Computer and Communication System Engineering, Faculty of Engineering, Universiti Putra Malaysia 43400 UPM, Serdang, Selangor, Malaysia*

## ABSTRACT

ECG signal differs from individual to individual, making it hard to be emulated and copied. In recent times ECG is being used for identifying the person. Hence, there is a requirement for a system that involves digital signal processing and signal security so that the saved data are secured at one place and an authentic person can see and use the ECG signal for further diagnosis. The study presents a set of security solutions that can be deployed in a connected healthcare territory, which includes the partially homomorphic encryption (PHE) techniques used to secure the electrocardiogram (ECG) signals. This is to record confidentially and prevent the information from meddling, imitating and replicating. First, Pan and Tompkins's algorithm was applied to perform the ECG signal processing. Then, partially homomorphic encryption (PHE) technique - Rivest-Shamir-Adleman (RSA) algorithm was used to encrypt the ECG signal by using the public key. The PHE constitutes a gathering of semantically secure encryption works that permits certain arithmetical tasks on the plaintext to be performed straightforwardly on the ciphertext. The study shows a faster and 90% accurate result before and after encryption that indicates the lightweight and accuracy of the RSA algorithm. Secure ECG signal provides innovation in multiple healthcare sectors such as medical research, patient care and hospital database.

*Keywords:* ECG signal, arrhythmias detection, PHE technique–RSA algorithm

ARTICLE INFO

*Article history:*
Received: 10 February 2020
Accepted: 13 November 2020
Published: 31 December 2020

DOI: https://doi.org/10.47836/pjst.28.S2.18

*E-mail addresses*:
mushaikh1986@gmail.com (Muhammad Umair Shaikh)
wawa@upm.edu.my (Wan Azizun Wan Adnan)
sanom@upm.edu.my (Siti Anom Ahmad)
* Corresponding author

ISSN: 0128-7680
e-ISSN: 2231-8526

## INTRODUCTION

Cardiovascular disease (CVD) generally refers to conditions that involve narrowed or blocked blood vessels that can lead to a heart attack, chest pain (angina) or stroke. CVD, especially coronary artery disease (CAD) is a leading cause of human morbidity and mortality. According to the world health organization (WHO), one in every four death is caused because of CVD [WHO, 2017]. The ECG is the wave representation of the heart activity. There are many widespread applications for ECG signals such as clinical diagnosis, understanding of the physiology of cardiac arrhythmias, interpretation for medical researcher and human-machine interface.

Similarly, sharing the patient's information through the internet of thing (IoT) for faster diagnosis has security and privacy issues. The patient's health database security is one of the greatest dangers looked by the providers. Ensuring and verifying this information has never been progressively basic. According to Civil Rights reports 2015, above 0.112 billion healthcare data were undermined ("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.," 2013). From that point forward, cybercriminals have turned out to be much progressively mindful of the estimation of healthcare records. The present situation demands extremely secured details of patients. Consequently, to secure the patient's information, the development of the secured ECG signal is the main challenge in the healthcare industry because it is very essential to record confidentially and to prevent mistreatment. This issue will be tackled by encrypting the ECG signals, utilizing the proposed PHE technique. The study contributes the natural algorithm -RSA-calculation and signal processing steps. In RSA, the sender will encode the ECG information by utilizing the public key and the receiver will unscramble the information by utilizing private keys for providing high security. According to the various applications of ECG, the secured ECG signal helps the healthcare providers and researchers for further studies of arrhythmia detection.

The Pan and Tompkins, QRS complex method used in this study to process the acquired ECG signal. The QRS complex is a method for determining the statistical self-affinity of a signal. This method has been used for the detection and analysis of cardiovascular abnormalities or ECG analysis (Shaikh, Ahmad, & Wan Adnan, 2019). The security features of the study protect the authenticity and confidentiality of the patient's information.

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

A brief introduction of the Pan and Tompkins method is studied first then the ECG recording techniques and security techniques- RSA- technique are reviewed subsequently. This study focuses on improving the security of the ECG signal.

## RELATED WORK

The secured and self-diagnostic ability of the ECG signal plays a vital role in the detection of ECG arrhythmias and transmits the signal. PHE schemes are used in certain applications like e-casting or Private Information Retrieval (PIR). However, these applications were confined as far as the sorts of homomorphic assessment tasks. In other words, PHE plans must be utilized for specific applications, whose algorithms include only addition or multiplication operation.

Lin, et al. (2016) proposed a Community-Based ECG Monitoring System for Patients with Cardiovascular Diseases. They aimed to develop a community-based electrocardiogram (ECG) monitoring system for cardiac outpatients to wirelessly detect heart rate, provide personalized healthcare, and enhance interactive social contact because of the prevalence of deaths from cardiovascular disease and the growing problem of aging in the world. The system not only strengthens the performance of the ECG monitoring system but also emphasizes the ergonomic design of wearable devices and user interfaces. Besides, it enables medical professionals to diagnose cardiac symptoms remotely and electronically manage medical reports and suggestions. The downsides are this system does not have any selfdiagnostic capability and there is no assurance that patients' data are authenticated at the server-side.

Motwani and Chaudhari (2014) proposed a Chaos encryption method for data Encrypted concealment in the ECG signal. The chaos encryption scheme is used to encrypt the text before hiding into the signal. The scheme is suitable for data protection in hospitals. The drawback of this scheme is that it does not directly encrypt the signal whereas our proposed method encrypts the ECG signal and authenticates the information at the server-side.

Qin et al. (2017) proposed an adaptive and time effective R-peak detection algorithm for ECG processing. The algorithm performance, including accuracy and time consumption, is better than the Pan and Tompkins method. Qin's algorithm is a stand-alone that is capable of only acquiring the ECG signals and visualizing the signals. It does not have any connection to the database at the health care provider for further analysis and diagnosis. The ECG signal is not secure at the server-side.

Park and Lee (2018) proposed a medical diagnosis system using e-health cloud servers in a privacy-preserving manner when medical datasets were owned by multiple data owners. The proposed system is the first one that achieves the privacy of the medical dataset, symptoms, and diagnosis results and hides the data access pattern even from the

e-health cloud servers system. However, to the best of our knowledge, none of the ECG systems discussed so far has incorporated security techniques relating to the authentication and secure ECG signal using partially HE technique

This study covers a greater scope than Lin, et al. (2016), Motwani and Chaudhari (2014), Qin et al. (2017) and Park and Lee (2018) research. Firstly, Pan and Tompkins algorithm was performed on ECG signal for the detection of the QRS complex. Secondly, the ECG signal was encrypted by using the PHE- RSA- algorithm. Lastly, heart rate was calculated and arrhythmia detected. PHE technique is one of the block ciphers with lightweight properties for enhancing confidentiality, integrity and authentication in ECG signal transmission in comparison to Gentry (Li, et al., 2013) AES (Hameed, et al., 2019) algorithm and ECG steganography (Sivaranjani, 2017).

## METHODS

The research was divided into two parts. The first part was QRS complex detection using Pan and Tompkins algorithm and the second part was the encryption of ECG signal using the PHE technique to make the signal more secure and difficult for a hacker to hack the information. The methodology flowchart of this study began by applying two stages following the steps of the Pan and Tompkins algorithm. The first stage was the preprocessing stage in which the signal was prepared for later detection, removing noise, smoothing the signal and amplifying the QRS slope and width. The second stage was the decision stage, in this stage thresholds were applied to the signal to remove noise peaks and consider only signal peaks. Indeed, it necessitates making the data ready for feature extraction in the ECG signal preprocessing stage. In this way, a suitable feature space is provided and the accuracy of the system is increased. Subsequently, in the next step, the method of encryption was studied.

In the feature extraction phase, the functionality of all features, namely, signal to noise ratio, use of threshold, signal peaks defined as those of the QRS complex and R-R interval were studied. Additionally, for the security of the ECG signal PHE was considered. After the moving window coordinates output (x6), the encryption-decryption calculation had been utilized. By encrypting the signal, the signal would be changed. The final result after the decryption was in the form of a normal or abnormal heart rate (HR). It offers assistance to the therapeutic professional for encouraging the conclusion and restorative analyst for advance considers. Ultimately, the performances of the algorithm are evaluated by calculating the classification error and accuracy using some statistical analysis. Likewise, the methodology flow chart of this research is demonstrated in Figure 1 involving the whole procedure step by step.

The MIT-BIH Arrhythmia database from the physio net website was used to test the proposed method of this study (Moody & Mark, 2001). The database was the primary for

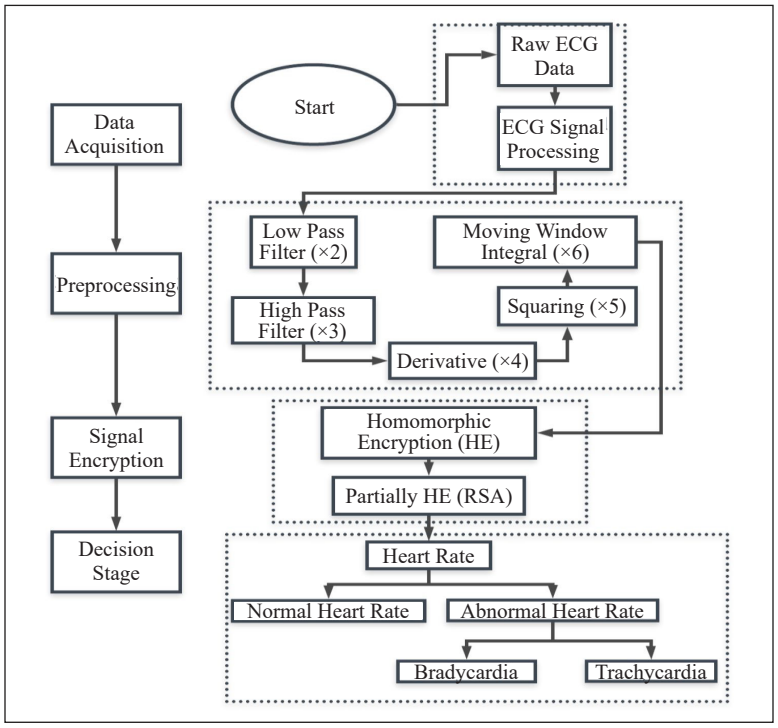



*Figure 1.* Methodology flow chart of the study in detail

the most part accessible set of standard test fabric for assessment of arrhythmia finders and had been utilized for that reason as well as for fundamental investigations into the cardiac flow at more than 500 destinations around the world.

The designed algorithm was 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 was applied to 20 random different ECG signals from the MIT-BIH arrhythmia database. The signal length was 21,600 samples. For example, a one- minute waveform with a sample rate of 360 samples per second requires 21,600 rows of data for each column with a sampling rate of 360 Hz for each ECG recording (Michalek, 2006).

## ECG Signal Processing

The methodology followed Pan and Tompkins algorithm. The raw ECG signal was passed through the bandpass filter for the QRS detection reduced noise by matching the spectrum of the average QRS complex. Then the filtered signal was passed through derivative, squaring and window integration phases. The signal-to-noise ratio increase, after the ECG signal, had passed through the bandpass filter stage x(3). This permits the use of thresholds that are just above the noise peak levels. Thus, the overall sensitivity of the detector improves.

Whereas, signal peaks are defined as those of the QRS complex, while noise peaks are those of the T waves, muscle noise, etc. After the determination of the QRS complex the point which showed the location of R points were determined. The cardiac cycle (RR) interval was obtained and heart rate was calculated.

## ECG Signal Encryption

The methodology followed Pan and Tompkins algorithm (Afonso et al., 1999). The raw ECG signal was passed through the bandpass filter for the QRS detection reduced noise by matching the spectrum of the average QRS complex. Then the filtered signal was passed through derivative, squaring and window integration phases. The signal-to-noise ratio increase, after the ECG signal, had passed through the bandpass filter stage x(3). This permits the use of thresholds that are just above the noise peak levels. Thus, the overall sensitivity of the detector improves. Whereas, signal peaks are defined as those of the QRS complex, while noise peaks are those of the T waves, and muscle noise. After the determination of the QRS complex the point which showed the location of R points was determined. The cardiac cycle (RR) interval was obtained and heart rate was calculated. The complete process is shown in Figure 2.

## Partially Homomorphic Encryption (PHE)

For encrypting the signal RSA algorithm was used. The RSA is an asymmetric cryptography algorithm. It is also known as public-key cryptography with two different keys, because

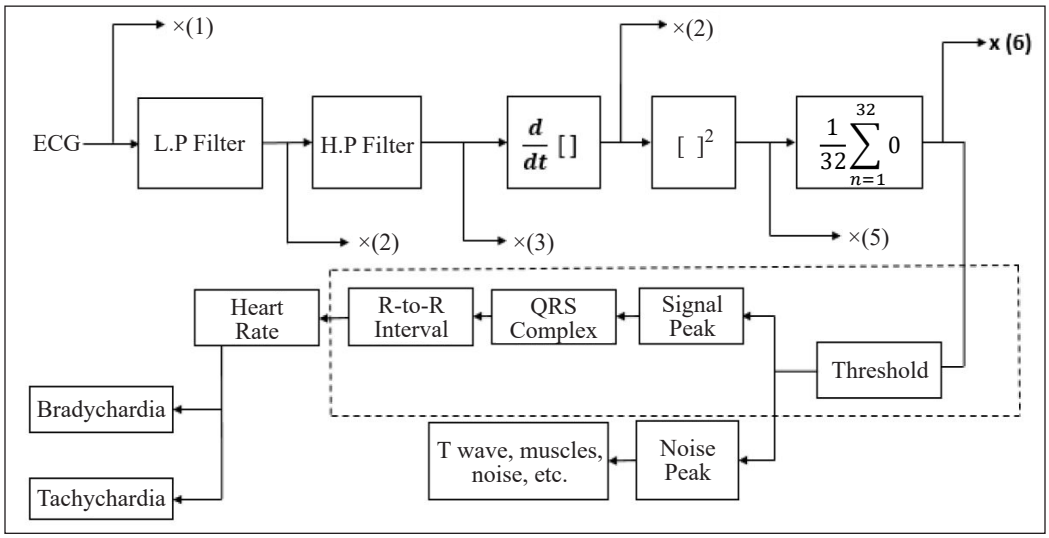



*Figure 2.* Various stages of high-speed QRS detection. x(1) is the input ECG signal. x(2) is the low passed ECG, x(3) is the band passed ECG, x(4) is the differentiated ECG, x(5) is the squaring output, x(6) is the window integrated output (Shaikh et al., 2019).

one of the keys is a public key and the other key must be kept private. The result obtained from RSA is in the form of normal and abnormal heart rate.

Where,

pk is public-key = (n,e), m1 is plaintexts. m1 is ECG signals after window integrated output (x6).

RSA is a public-key encryption technique used to encrypt and decrypt the signal by using two keys. RSA is used to encrypt the ECG information by using public and private keys.

**RSA Algorithm Design.**

Input: ECG signal after moving window integrated output (x6)

Output: Normal or abnormal heartbeat.

Step1: Get ECG signal (x6)

Step2: Convert (x6) to integer representation Ims Step3: Generate key pair

1. Choose two random primes p and q
2. Perform n = p*q
3. By using Euler's totient function calculate Phi
4. Calculate e that is relatively prime to Phi
5. Compute the private exponent d from e, p and q.
6. Output (n, e) as the public key and (n, d) as the private key.

Step4: Encrypt the (x6) with a public key (n,e).

Step5: The ciphertext (C) is computed.

Step6: Decrypt the signal using the private key.

**Encryption Process.** The public key *(n, e)* is used to encrypt the signal (x6) at the transmitter to produce the cipher message *C* by using the formula:

$$C = M^e \bmod n$$

Then, this ciphered or encrypted message *C* is transmitted to the intended receiver.

*Decryption Process*

The private key *(n, d)* is used to decrypt the ciphered message *C* at the receiver to produce the plain message *M* by using the following formula:

$$M = C^d \bmod n$$

**Decision Stage.** After the encryption of the ECG signal, the next stage was the decision stage. By encrypting the signal the signal values will change. After the decryption, the system would show the same result without compromising the signal efficiency meant the RSA algorithm would not affect the signal value and showed the same results. The decrypted

result displays regular or irregular heartbeat. The heartbeat is irregular if its value is below 60bpm (bradycardia) and above 100bpm (tachycardia). This result will help further analysis.

## RESULTS AND DISCUSSION

The database was downloaded from the MIT-BIH website for arrhythmia detection. Pan and Tompkins's algorithm was used to do signal processing before applying the RSA algorithm for Signal encryption. The length of the signal was 21,600 samples having a sampling rate of 360 Hz for 20 random ECG recording. Figure 3. shows an input of record 100 ECG from the database.

Figure 4 shows the processing steps for record 100. In the preprocessing stage, low and high pass filters were used to remove the noise and any existing artifacts. The next step was differentiation use to find the high slope use to distinguish the QRS complexes from other ECG waves. The next step consisted of step to step squaring of the sample used to make all data positive and accentuated the higher frequencies in the signal. After that squared waveform passed through the moving window integrator.

Figure 5 shows the encryption of the ECG signal using the RSA algorithm. After the encryption of the signal (x6) system would request the private key. If the user entered the wrong private key the signal would not decrypt and request for the correct private key as shown in Figure 6. By providing the correct private key the system would display the result in the form of normal and abnormal heartbeat. If the heartbeat was abnormal it would display two types of arrhythmias i.e. bradycardia (heartbeat below 60BPM) and tachycardia (heartbeat above 100BPM).

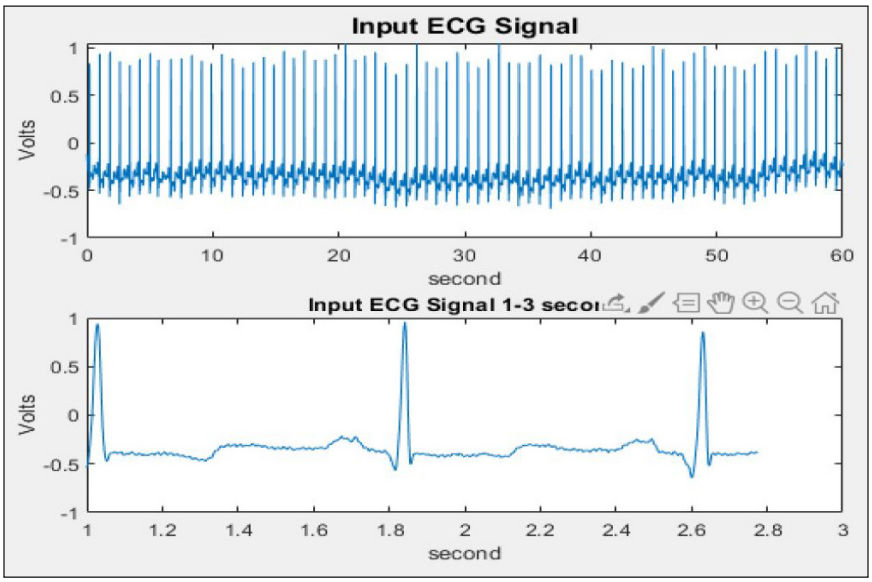



*Figure 3.* Input ECG signal from the MIT-BIH database

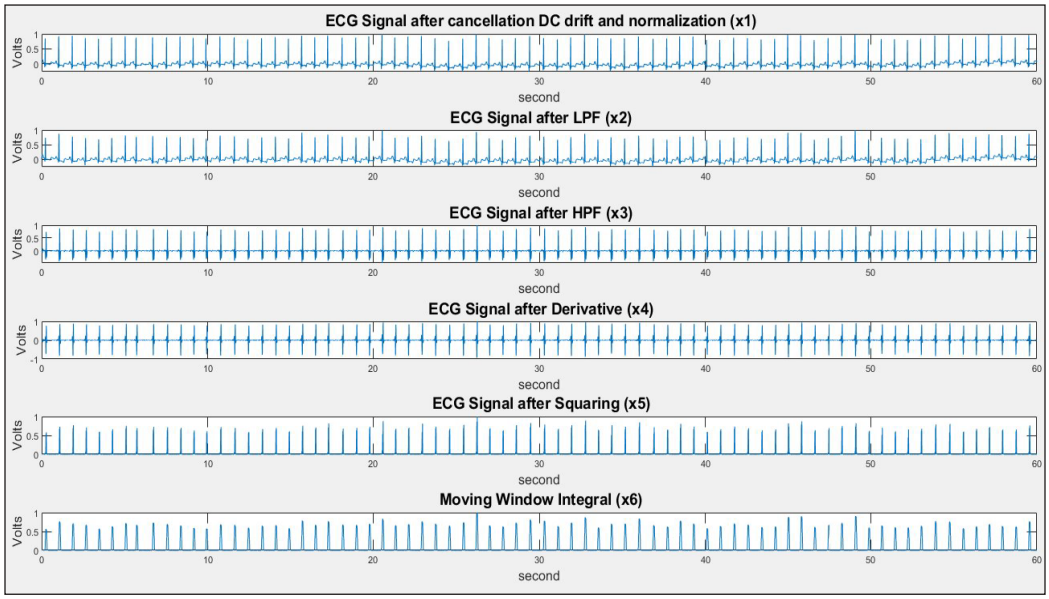
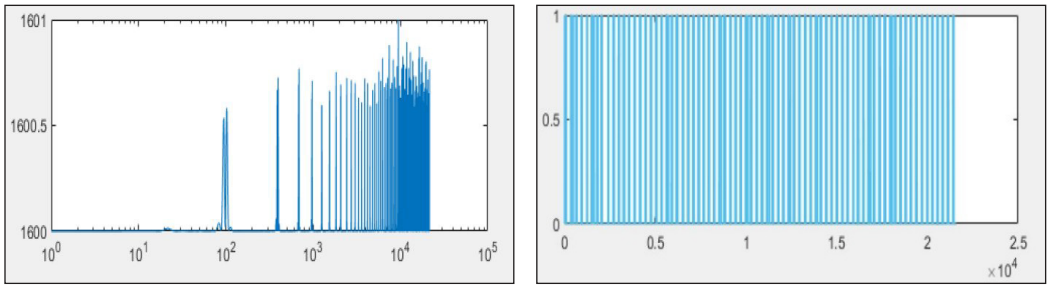



*Figure 4.* Signal processing steps of ECG 100 record




(a) (b)

*Figure 5.* Shows ECG signal encryption using the RSA algorithm (a) Encryption of signal (x6) (b) Cipher of a signal.

```
end.
end
Enter tifie Private E<ey65 P =
65
Wrong key enter
Enter tifie Private KeylQ2
P =
102
Wrong key enter
Enter tifie Private KeylOO
P =
lOO
Heart beat is normal
fx »
```

*Figure 6.* System request for the correct private key to display the result

Figure 7 shows the result in the form of a heartbeat after entering the correct private key. The obtained results are summarized in Table 1. The 20 records were considered from the MIT-BIH database arrhythmia database. The MIT-BIH database was used to compare the result with our design PHE techniques and decryption. Out of 20 records, 18 records showed the same result after the decryption of the ECG signal.

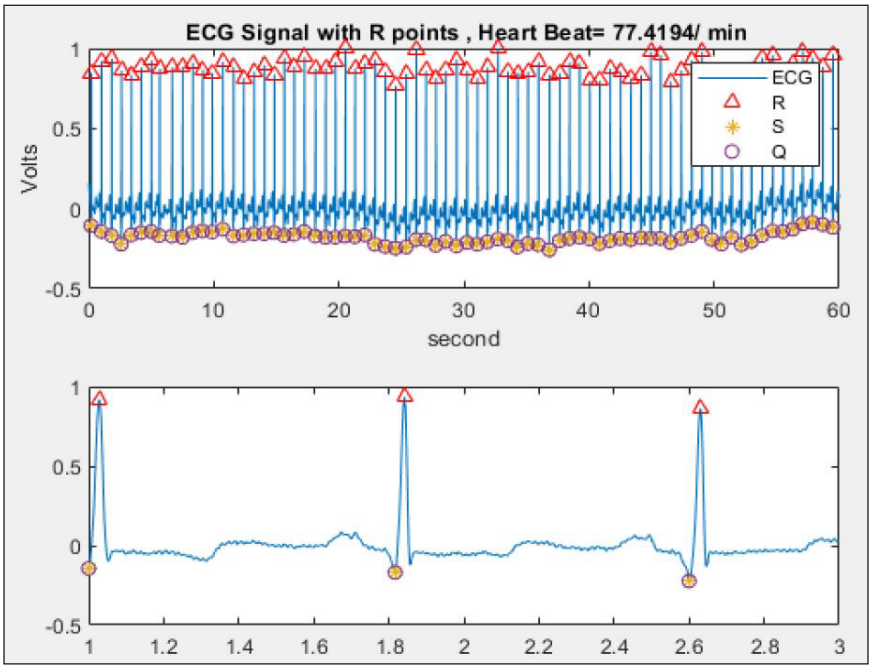



*Figure 7.* R-R interval and heartbeat detection

Table 1
*Comparison of result with MIT-BIH data and result after RSA algorithm*

| ***Record No.*** | **MIT-BIH Arrhythmia Database** | **Proposed methodology mean HR** | **Result** |
|---|---|---|---|
| ***Record 100*** | 70-89 bpm | 73.5 bpm | Normal (Same output) |
| ***Record 101*** | 55-79 bpm | 64.86 bpm | Normal (Same output) |
| ***Record 102*** | 72-78 bpm | 80 bpm | Normal (Same output) |
| ***Record 105*** | 78-102bpm | 58 bpm | Abnormal (Bradycardia, Not same output) |
| ***Record 106*** | 49-87 bpm | 72 bpm | Normal (Same output) |
| ***Record 113*** | 48-87 bpm | 59 bpm | Abnormal (Bradycardia, Same output) |
| ***Record 114*** | 51-82 bpm | 57 bpm | Abnormal (Bradycardia, Same output) |
| ***Record 115*** | 50-84 bpm | 69 bpm | Normal (Same output) |
| ***Record 116*** | 74-86 bpm | 78 bpm | Normal (Same output) |

Table 1 (*continue*)

| *Record No.* | MIT-BIH Arrhythmia Database | Proposed methodology mean HR | Result |
|---|---|---|---|
| ***Record 117*** | 48-66 bpm | 49 bpm | Abnormal (Bradycardia, Same output) |
| ***Record 118*** | 54-91 bpm | 72 bpm | Normal (Same output) |
| ***Record 121*** | 55-83 bpm | 58 bpm | Abnormal (Bradycardia, Same output) |
| ***Record 122*** | 67-97 bpm | 84 bpm | Normal (Same output) |
| ***Record 123*** | 41-65 bpm | 55 bpm | Abnormal (Bradycardia, Same output) |
| ***Record 124*** | 47-64 bpm | 48 bpm | Abnormal (Bradycardia, Same output) |
| ***Record 201*** | 31-61 bpm | 140 bpm | Abnormal (Tachycardia. Not same output) |
| ***Record 210*** | 63-158 bpm | 109 bpm | Abnormal Tachycardia , Same output) |
| ***Record 213*** | 101-113bpm | 110 bpm | Abnormal (Tachycardia, Same output) |
| ***Record 215*** | 81-215 bpm | 122 bpm | Abnormal (Tachycardia, Same output) |
| ***Record 232*** | 24-28 bpm | 50 bpm | Abnormal (Bradycardia, Same output) |

## CONCLUSION

Accessibility, reliability, confidentially and secrecy of data are the main aspects that should be maintained in ECG signal security. Protecting ECG signal from modification, disruption, extermination as well as the illegal access are the main goal of signal security. A secure and efficient communication system for the ECG signal based on the PHE algorithm is designed in this work. The presented cryptosystem was implemented and its performance was evaluated using different signals from the MIT-BIH arrhythmia database. The results obtained demonstrated that the accuracy of signal was at a satisfying level which confirmed the suitability, reliability, high security and effectiveness of the introduced scheme to be applied in practical applications like signal data encryption/decryption. After comparing the signal before and after encryption the proposed RSA algorithm provided 90% accuracy compared to the unencrypted database result. The output shows the result in the form of the normal and abnormal heartbeat which helps to diagnose the different arrhythmias like bradycardia and tachycardia. The idea from this study can be used to secure other medical signals. The security parameter in this investigation will verify the restorative information with the goal that the information is not lost and to keep patient's data in a single place.

## ACKNOWLEDGEMENTS

The authors are grateful for the financial support provided by the Ministry of Education of Malaysia through Universiti Putra Malaysia under Grant Putra [GP/2018/9667300].

## REFERENCES

Afonso, V. X., Tompkins, W. J., Nguyen, T. Q., & Luo, S. (1999). ECG beat detection using filter banks. *IEEE Transactions on Biomedical Engineering, 46*(2), 192-201. doi: 10.1109/10.740882

Hameed, M. E., Ibrahim, M. M., Manap, N. A., & 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), 4850-4859. doi:10.11591/ijece.v9i6.pp4850-4859

Jati, G., Rachmasari, A. R., Jatmiko, W., Mursanto, P., & Sediono, W. (2018, September 23-24). An efficient secure ECG compression based on 2D-SPIHT and SIT algorithm. In *2017 International Workshop on Big Data and Information Security (IWBIS)* (pp. 155–160). Jakarta, Indonesia.

Li, J., Song, D., Chen, S., & Lu, X. (2013, October 30 – November 1). A simple fully homomorphic encryption scheme available in cloud computing. In *IEEE 2nd International Conference on Cloud Computing and Intelligence Systems (*pp. 214-217). Hangzhou, China.

Lin, B. S., Wong, A. M., & Tseng, K. C. (2016). Community-based ECG monitoring system for patients with cardiovascular diseases. *Journal of Medical Systems, 40*(4), 1-12. doi:10.1007/s10916-016-0442-4

Michalek, P. J. (2006). *An authentic ECG simulator*. (Master thesis). University of Central Florida, Florida.

Moody, G. B., & Mark, R. G. (2001). The impact of the MIT-BIH arrhythmia database. *IEEE Engineering in Medicine and Biology Magazine, 20*(3), 45-50. doi:10.1109/51.932724

Motwani, P., & Chaudhari, D. (2014). Encrypted data concealment in electrocardiogram signal using chaos encryption method. *International Journal for Research in Emerging Science and Technology, 1*(5), 60–63.

Pan, J. & Tompkins, W. J. (1985). A real-time QRS detection algorithm. *IEEE Trans Biomed Eng. 32*(3), 230-236. doi: 10.1109/TBME.1985.325532.

Park, J., & Lee, D. H. (2018). Privacy preserving k -nearest neighbor for medical diagnosis in e-health cloud. *Journal of Healthcare Engineering 2018,* 1-11. doi:10.1155/2018/4073103

Qin, Q., Li, J., Yue, Y., & Liu, C. (2017). An adaptive and time-efficient ECG R-peak detection algorithm. *Journal of Healthcare Engineering, 2017,*1-14. doi:10.1155/2017/5980541

Shaikh, M. U., Ahmad, S. A., & Wan Adnan, W. A. (2019, December 3-6). Investigation of data encryption algorithm for secured transmission of electrocardiograph (ECG) signal. In *2018 IEEE EMBS Conference on Biomedical Engineering and Sciences* (pp. 274-278). Sarawak, Malaysia

Sivaranjani, B. & Radha, N. (2017, October 19-20). Securing patient's confidential information using ECG steganography. In *2017 2nd International Conference on Communication and Electronics Systems* (pp. 540-544). Coimbatore, India.

US Department of Health and Human Services. (2013). 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. *Federal Register, 78*(17), 5566-5702.