Comparative study of several operation modes of AES algorithm for encryption ECG biomedical signal

Mustafa Emad Hameed[1], Masrullizam Mat Ibrahim[2], Nurulfajar Abd Manap[3], Mothana L. Attiah[4]
[1,2,3,4]Centre for Telecommunication Research and Innovation (CeTRI),
Faculty of Electronic and Computer Engineering (FKEKK), Universiti Teknikal Malaysia Melaka (UTeM), Malaysia
[1]Department of Computer Techniques Engineering, Bilad Al-rafidan University College, Diyala, Baqubah, Iraq

Article Info

Article history:

Received Feb 27, 2019
Revised Apr 9, 2019
Accepted Jun 26, 2019

Keywords:

AES algorithm
Decryption
ECG signal
Encryption
Security

ABSTRACT

Biomedical signal processing provides a cross-disciplinary international forum through which research on signal and images measurement and analysis in clinical medicine as well as biological sciences is shared. Electrocardiography (ECG) signal is more frequently used for diagnosis of cardiovascular diseases. However, the ECG signals contain sensitive private health information as well as details that serve to individually distinguish patients. For this reason, the information must be encrypted prior to transmission across public media so as to prevent unauthorized access by adversaries. In this paper, the proposed the use of the Advanced Encryption Standard algorithm (AES), which is one of a symmetric key block cipher with lightweight properties for enhances confidentiality, integrity and authentication in ECG signal transmission. However, some of the challenges arising from the use of this algorithm are computational overhead and level of security, which occur when handling more complex.The AES algorithm has different operation modes using three different key sizes which can be utilized in encrypting the whole sample of ECG biomedical signal in electronic healthcare. The experiments in this research, exhibit comparative study of using five modes of operation in AES algorithm, which are coupled with three key sizes based on the execution time and security level for the encryption of ECG biomedical signals in electronic healthcare application. Thus, we reported that the CBC mode of the AES algorithm is suitable to be applied of security purpose.

Corresponding Author:

Mustafa Emad Hameed,
Department of Telecommunication Engineering,
Faculty of Electronic and Computer Engineering,
Universiti Teknikal Malaysia Melaka,
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
Email: mihhh221@gmail.com

1. INTRODUCTION

The biomedical Signal places emphasis on contributions to research in association with practical and applications with regard to the application of ways and devices in clinical diagnosis, tracking of patients and management [1]. Electrocardiogram (ECG) is broadly used in medicine to monitor minute electrical changes on the skin of a patient's body which arise as a result of human heart activities measured using electrodes placed on standard 12-leads (also referred to as channels) [2]. This is a simple technique and noninvasive measurement which easily indicates a number of heart diseases and the medical industries have built a dedicated equipment that aids in diagnosis of the signal [3]. Contrary, to other biotech authentication methods, the patient can wear the system, and as long as it is worn, authentication can be sustained. Therefore, the violation of the information confidentiality, integrity and accessibility may cause the damage to its owner and have significant undesirable consequences [4]. However, this results in a new challenge in terms of the security for transmission of an ECG signal template [5]. Thus, it is vital that huge amounts of data traffic [6], with a variety of security requirements be easily handled in the healthcare systems and be transmitted and stored while ensuring a high level of security [7, 8]. The cryptography technology is a science of data secueity, which includes the use of a cipher, describes a process of encrypting information so that its meaning is hidden and thus, remain securing from unauthorized access, and network hacking [9, 10]. Accordingly the encryption is quite important for a protection and security environment for the Internet [11]. This therefore, brings in suitability of the symmetric key cryptosystems in comparison with the public-key solutions for effective processing of this type of data [12]. The advanced encryption standard (AES) has become a de-facto standard when talking about symmetric key cryptosystems. The AES algorithm is being adopted by many organizations across the world [13]. It is mostly applicable to governments for different levels of data protection (e.g. the use of AES-128, AES-192 or AES-256) hence suitability for sensitive data storage related to healthcare [14]. Thus, the AES algorithm has been used with Lightweight Cryptography properties in Internet of things (IoT) [15].

Nonetheless some of the challenges arising from the use of this algorithm are computational overhead and level of, security, which occur when handling more complex. Furthermore the configuration modes like operation of block ciphers enable those ciphers to deal with large data streams, at no risk of security compromisation [16-18]. The AES is an algorithm for block encryption, with extensive use in public media communication especially the Internet of things (IoT) [19]. The five standardized AES modes of operation include: ECB (Electronic Code Book), CBC (Cipher Block Chaining), CFB (Cipher FeedBack), OFB (Output FeedBack) and CTR (Counter) [20].

In this paper, exposure comparative study of the usage the Advanced Encryption Standard algorithm (AES), which is a symmetric key block cipher for encryption and decryption process. The five modes of operation in AES will be presented, coupled with three key sizes for respective parameters. For each security level, the execution times for the whole sample of ECG biomedical signals in electronic healthcare will be presented. This paper is organized as follows; Section 2 entails the AES algorithm. The details of modes AES operation are introduced in Section 3. Section 4 explains the signal of electrocardiogram (ECG). Experimental results and discussion aspects are shown in Section 5 and conclusions of this paper in Section 6.

2. DESCRIPTION OF AES ALGORITHM

AES is a symmetric block cipher which entails a 128 bits block length. It can accommodate three dissimilar key lengths 128,192 and 256 bits. 128 key bits in the process of encryption requires 10 processing rounds while 192-bit keys need 12 rounds and 256-bit keys 14 rounds as shown in Table 1. AES is therefore an algorithm that is round based. Apart from the last round, encryption and decryption has four functions for each round. Only three functions are needed for the last round. The four-round functions for the encryption algorithm are SubByte, ShiftRows, MixColumn and AddRoundKey. Moreover, the same number of rounds apply for the decryption algorithm with reverse transformation, with a difference in order of round function i.e. InvShiftRow, InvSubByte, AddRoundKey and InvMixColumn [21]. Figure 1 show details encryption and decryption procedures of the Advanced Encryption Standard algorithm. A brief discussion of the four steps involved in the operation of the AES Algorithm.

2.1. AES encryption algorithm

In the Encryption process there exist various contrasting transformations that are successively utilized over the data block bits in iterations that are specific in number referred as rounds. The length of the key used determines how many rounds will occur for the encryption procedure [22]. 10 iterations are necessary for 128 bits key length, 12 for 192 bits and 14 for 256 bits. A brief discussion of the steps involved in the operation of the AES Algorithm is as follows:

1. KeyExpansions: Using Rijndael's key schedule, derivation of round keys from the cipher key is done. Separate 128-bit round key block are required by AES for every round plus another one.
2. InitialRound
   a. AddRoundKey: A combination of every byte of the state to a round key block is done using bitwise XOR.
   b. SubBytes: A non-linear replacement step with each byte used instead of another as per the lookup table.
   c. ShiftRows: A transposition step which entails shifting cynically a certain number of steps of the last three rows of the state.

d. MixColumns: A mixing operation which entails bringing together four bytes of each column and it functions on the columns of the state.

3. Final Round (No MixColumns) SubBytes, ShiftRows and AddRoundKey. The steps for encrypting the 128- bit block are:
   a. The set of round keys from the cipher key.
   b. Initialize state array and add together the initial round key and the starting state array.
   c. Circular performance = 1 to 9: execute usual round.
   d. Final round execution.
   e. Correlating cipher text chunk output of last round step.

Table 1. AES Parameters for the various AES versions

AES Algorithm	Number of Round	Key Size	Block Size
128-Bit	10	4	4
192-Bit	12	6	4
256-Bit	14	8	4

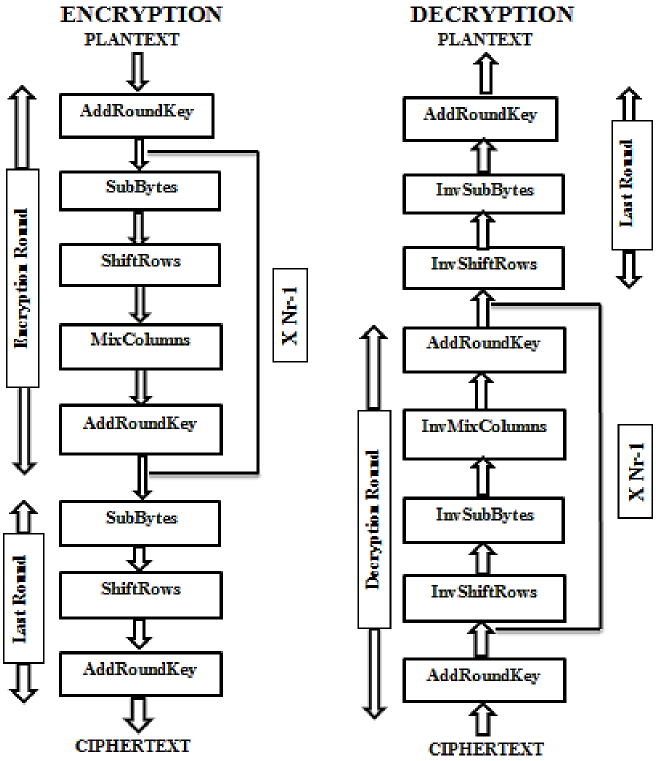


Figure 1. Block diagrams of AES algorithm

2.2. AES decryption algorithm

Extraction of the plaintext from a cipher text is what describes decryption process. The reverse of encryption is done where 128 bits of a cipher text are converted back to plain text using the inverse of the four operations. It details about a reverse of the process of encryption by the application of the following inverse functions [23]. The steps are:

a. Inv-SubBytes
b. Inv-Shiftrows
c. Inv-Mix-Column
d. AddroundKey

A key expansion routine is used to bring out a key schedule. The Inv-Mix-Column reverse operation requires matrix elements similar to the Mix-Column step. If the two constant matrices are inverse of each other, it is easy to prove that the two transformations are inverse of each other.

3. MODES OF AES OPERATION

Block ciphers operate using methods of configuration where the ciphers can use data streams that are huge with no risk of manipulation of the security of data [24]. However with block ciphers, there is a possibility for the use of secret key bits that are the same for similar plaintext parts for encryption. There can be a generation of the same ciphertext blocks for input data that is identical if one of the deterministic algorithm. Hence, for an intruder who knows the message parts that are identical, it would be easy to have access to much information. Conveniently, there is an existence of ways on how to blur the cipher output [25]. The point here is to have a combination of known plaintext blocks with generated ciphertext blocks, and then for the next blocks, use the result as the cipher input. Therefore in 2001 the NIST standardized five modes of operation: ECB (Electronic Code Book), CBC (Cipher Block Chaining), CFB (Cipher FeedBack), OFB (Output FeedBack) and CTR (Counter), applied to AES [25]. There exist a parameter for each mode which is significant and provides necessary security for the algorithm. An initialization vector (IV) is required for all these modes (except ECB), which is a sort of 'dummy block' to start the process for the initial real block, and for provision of some randomization for the process. In most cases there is no need for the secrecy of IV, but it is of benefit for it not to be used again with the same key. For CFB, there is spilling out of information about the initial plaintext block if an IV is reused, and about sharing of any common prefix between the two messages. The use of an IV again for OFB and CTR, entirely does away with the security.

3.1. Electronic codebook (ECB)

This is a straightforward mode of encryption which entails dividing the message to form blocks and encrypting every block as separate entities. However in this method, encryption of the identical plaintext blocks results into identical ciphertext blocks; hence, difficult in hiding of data patterns. Therefore, it lacks provision of confidentiality in a message, and it is not recommended for use in cryptographic protocols at all [26]. Figure 2(a) and Figure 2(b) show the encryption and decryption procedures of the ECB mode operation.

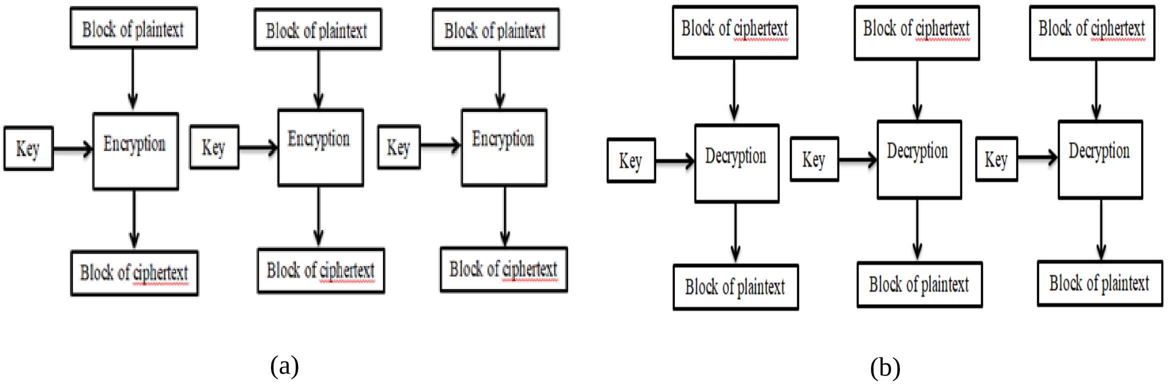


Figure 2. (a) Encryption in the ECB mode, (b) Decryption in the ECB mode

3.2. Cipher block chaining (CBC)

To each ciphertext block produced earlier, an XOR is added to each plaintext block. Figure 3(a) and Figure 3(b) show the encryption and decryption procedures of the CBC mode operation. Encryption of the result is then performed by a cipher algorithm. The outcome of each succeeding ciphertext block relies on the preceding one [27]. The initial plaintext block is added XOR to an unsystematic initialization vector (IV).

The size of the vector and that of the plaintext block are similar. Only a single thread is used to perform encryption in CBC mode. However with this demerit, this method is widespread when using block ciphers. CBC mode is used in many applications such as email or web data. Addition of XOR from the output data of the decryption algorithm to the previous ciphertext block should be done in the process of performing decryption of a ciphertext block. Because the ciphertext block in known to the receiver after obtaining the encrypted message, which enables decrypting the message by the use of a number of threads concurrently.

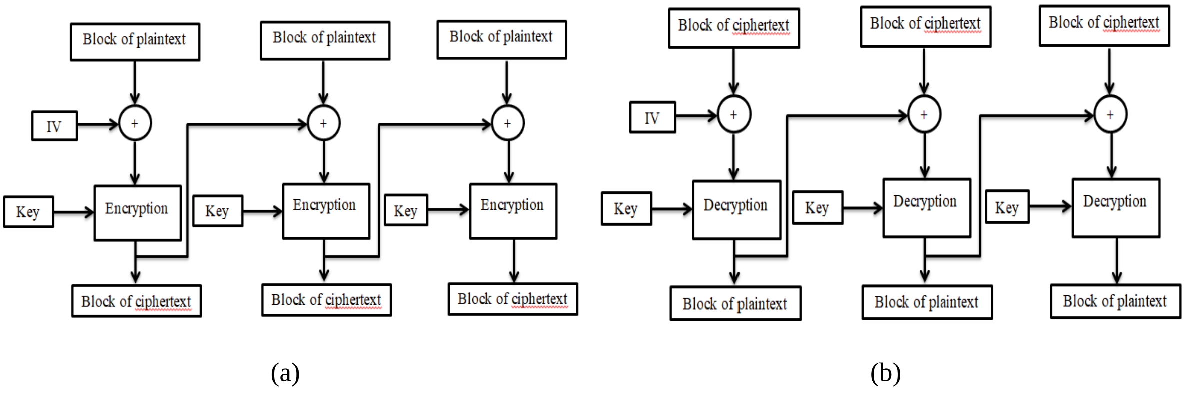


Figure 3. (a) Encryption in the CBC mode, (b) Decryption in the CBC mode

3.3. Cipher feedback (CFB)

There is similarity between the CFB mode and the CBC mode as detailed above. The major contrast comes as a result of encrypting the ciphertext data from the preceding round (not the plaintext block) and then combining with the outcome to the bits of the plaintext. It does not affect the cipher security, however the outcome is that the same encryption algorithm (as was applied in the plaintext encryption data) ought to be used when performing the decryption activity [28]. Figure 4(a) and Figure 4(b) show the encryption and decryption procedures of the CFB mode operation.

On one hand, only a single thread can be used to perform the encryption of CFB mode. On the other hand, as in CBC mode, numerous threads can be used to decrypt ciphertext blocks simultaneously. Similarly, damage of one ciphertext bit denotes that damage will only be done to two received plaintext blocks. As opposed to the previous block cipher modes, extension of the encrypted message is not necessary till the size is equal to an integer multiple of a single block length [28].

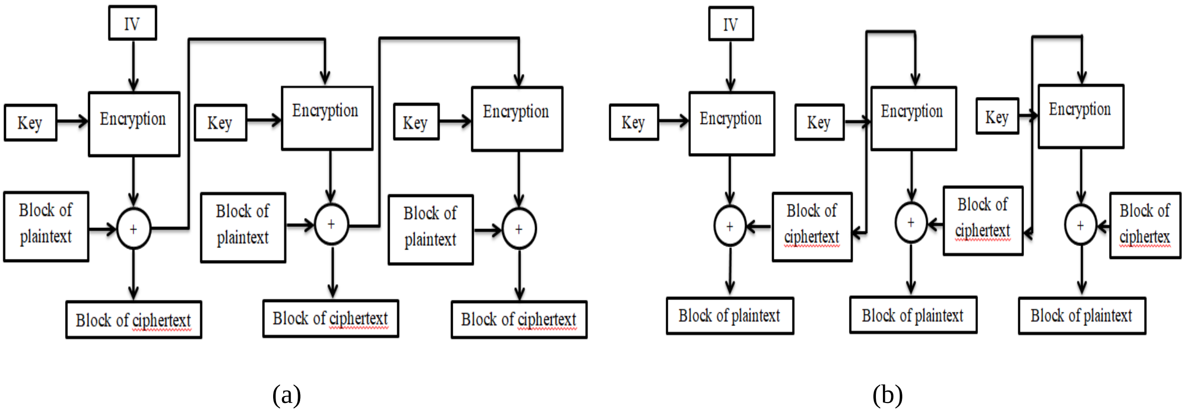


Figure 4. (a) Encryption in the CFB mode, (b) Decryption in the CFB mode

3.4. Output feedback (OFB)

Keystream bits meant for encryption of successive data blocks are generated by the algorithms that work in the OFB mode. Incidentally, there is some similarity between the block cipher way of working and the typical stream cipher way. Thus, Figure 5(a) and Figure 5(b) show the encryption and decryption procedures of the OFB mode operation.

The encryption and decryption procedures can be made possible if a single thread is applied every single time owing to the fact that there is continuous creation of keystream bits. Similarly, a similar cipher encryption algorithm is applied to both encryption and decryption in the CFB mode. The disadvantage of OFB is that a repetition of encryption of the initialization vector may result in the same state that has previously occurred. It is unusual, however if it does happen, encryption of the plaintext as done by the same data earlier, will be done [28].

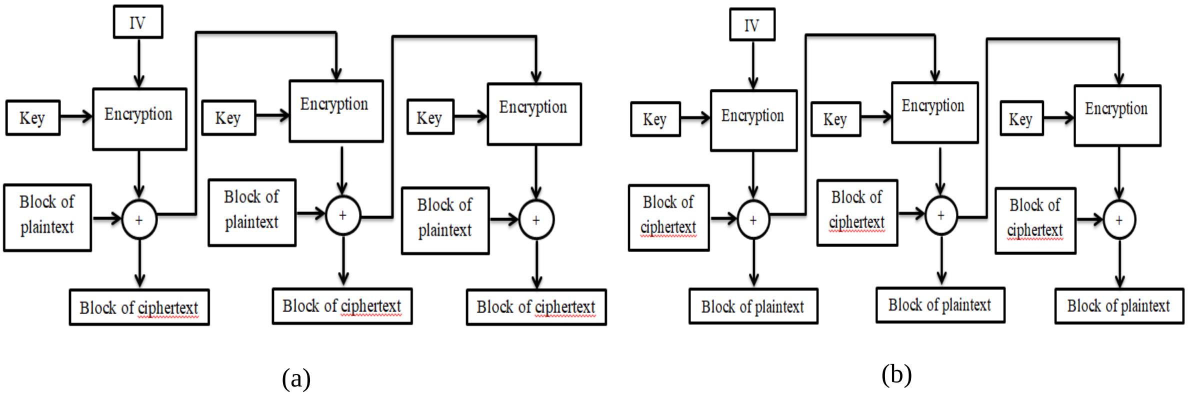


Figure 5. (a) Encryption in the OFB mode, (b) Decryption in the OFB mode

3.5. Counter (CTR)

In this mode, the operation of the block cipher is the same as to a stream cipher. Just like in the OFB mode, creation of keystream bits is done without regard to the encrypting data blocks content. In this mode, additions to a nonce value are the subsequent values of an increasing counter. The nonce means a digit that is distinct: a digit applied once and the encryption of the outcome is as usual. Therefore, the role of the nonce is similar to the role of initialization vectors in the previous modes (ECB, CBC, CFB and OFB) [17]. The encryption and decryption strategies of the CTR mode operation as shown in Figure 6(a) and Figure 6(b). A number of threads can be used to perform both encryption and decryption concurrently. However, damage from one bit of a plaintext or ciphertext, results in damage of only one corresponding output bit. Thus, there is a possibility to apply a variety of correction algorithms to take back the earlier value of corrupted parts of messages that were accepted [29]. The CTR mode is one of the accepted block ciphers mode of operation [30].

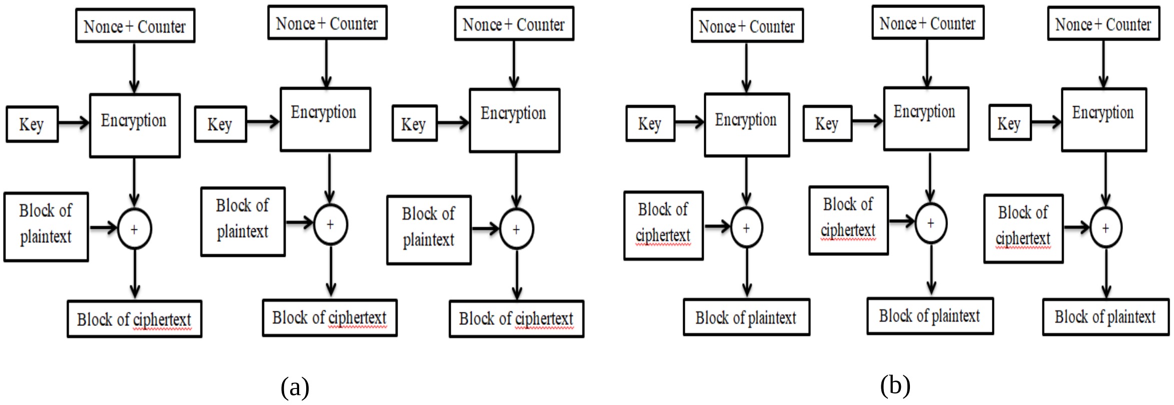


Figure 6. (a) Encryption in the OFB mode, (b) Decryption in the OFB mode

4. ELECTROCARDIOGRAM (ECG)

The ECG is a recorded electrical current whose results are gotten from the heartbeat. ECG waveforms are dependent upon the anatomic characteristics of the human heart and body. The QRS complexes, P and T waves extracted from the ECG are the constituents of ECG fragments. QRS is the ECG deflection which is a representation of ventricular depolarization. The atrial depolarization is substituted by P wave where atrial repolarization happens when ventricular depolarization occurs and is unknown. The ventricular repolarization is substituted by the T wave as shown in the Figure 7. The multiple individual factors govern their morphology and amplitudes resulting in an assumption about the uniqueness of the human aspects, specifically by the heart shape and position. For instance, the QRS complexes in an ECG have various structures easy to distinguish in different cases [31]. The ECG signals used in this study were obtained from the MIT-BIH Arrhythmia database that is made up of 48 half-hour excerpts of two-channel ambulatory ECG recordings [32].

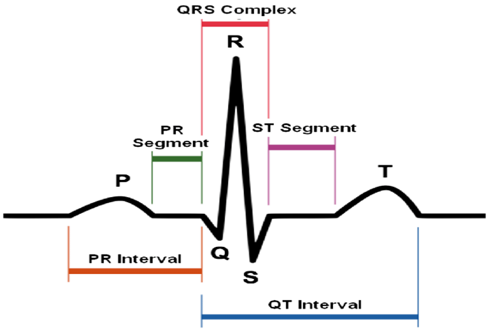


Figure 7. Display of the ECG signal

5. RESULTS AND ANALYSIS

This portion reports and deliberates the results of the conducted investigations. The experiments are, to evaluate the effectiveness of the utilization impact of different operation modes of the AES algorithm under three key sizes for encryption ECG biomedical signal in electronic healthcare. The conducted experiments are performed on a computer with specifications (processor Intel(R) Core (TM) i3-3110M @ 2.40GHz(CPUs),~2.4GHz, RAM 4GB, under windows 10 professional 64-bit using MATLAB (R2013a). The original ECG biomedical signal can show in Figure 8, which is encrypted with the AES algorithm using three key magnitudes (128-bit, 192-bit and 256-bit) and five AES mode operation (ECB, CBC, CFB, OFB and CTR). Figure 9(a) and Figure 9(b) show the encryption and decryption of ECG biomedical signal. The execution of the proposed method was assessed using some parameters, timely execution and security level.

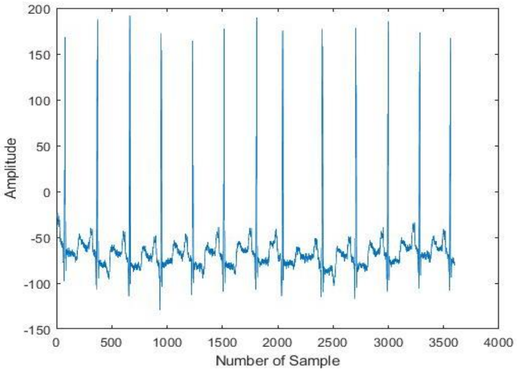
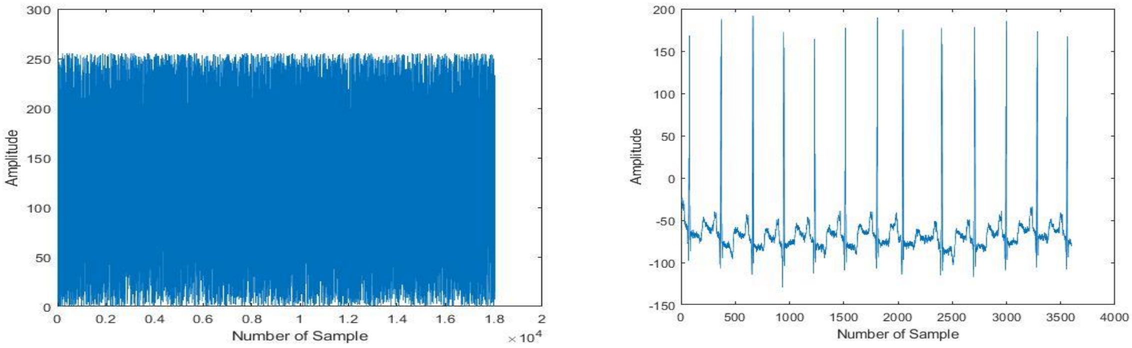


Figure 8. Original ECG Biomedical Signal

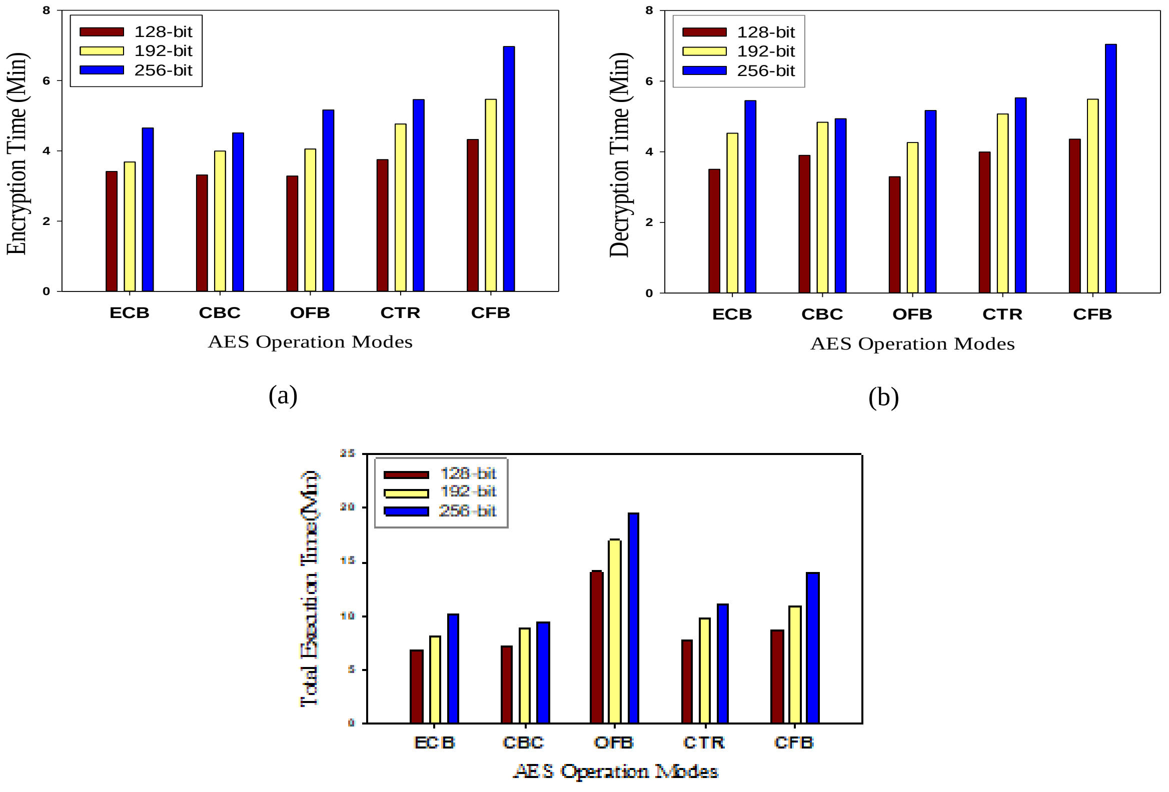


(a) (b)

Figure 9. (a) Encryption ECG biomedical signal; (b) Decryption ECG biomedical signal

5.1. Time execution

The execution time of encryption and decryption operations of the AES algorithm for ECG biomedical signal is shown in Figure 10. Accordingly, during different ciphering modes operation (ECB, CBC, OFB, CFB and CTR) three key sizes are used. From the conducted experiments, the result is that, the encryption and decryption processes of AES algorithm that were applied in ECG biomedical signal showed that, when using the CFB mode operation, there is a need for high computational time compared with the other mode operation.



(a)

(b)

(c)

Figure 10. (a) Histogram of Time Execution for Encryption Process, (b) Histogram of Time Execution for Decryption Process, (c) Histogram of Total Time Execution for Encryption and Decryption Processes in AES Algorithm

However, there was a minimum time in execution the ECB mode operation with 128-bit and 192-bit key sizes, while the CBC mode of operation had a low time execution within 256-bit key size as compared to other modes operation. Figure 10(a) and Figure 10(b) show the histogram of the timely execution of encryption and decryption processes in the AES algorithm for ECG biomedical signal.

The total time of execution of encryption and decryption processes in the AES algorithm for ECG biomedical signal shown in Figure 10(c). However, the minimum value of execution time for encryption process is 3.28 minutes and 3.29 minutes for decryption process. The maximum value of execution time for encryption process is 6.96 minutes and 7.04 minutes for decryption process. Therefore, there is no significant variation in the time of execution of the encryption and decryption processes between ECB, CBC and OFB AES mode operation with three key sizes except CTR and CFB modes. Thus, the CFB and CTR operation modes for AES algorithm revealed high computation of the time execution for encryption and decryption processes.

5.2. Analysis of security level

The security level is used to analysis the strength of algorithm that a cryptographic primitive such as a cipher or hash function achieves. The security level is typically conveyed using "bits". Table 3 illustrates the security level for three key lengths in the AES algorithm. The symmetric cryptosystem with λ-bit keys does not allow a general attack that is faster than exhaustive keys where λ represents the value of the length of the key and which is also the security level. Therefore, an asymmetric cryptosystem with a key size of λ-bits cannot succumb to attacks faster than an exhaustive key search. As a result, the cryptosystem is described as having a security level of λ. An exhaustive key search that has λ- bit keys may demand for up to 2^λ different keys [33]. In general, with a successful general attack that requires effort approximately up to 2^λ, then a cryptographic system offers security level of λ. Moreover, the ensuing number from 2^λ represents the number of attempts required by the hacker to break the cryptographic key. On the other hand, to be able to know the period of time required by an attacker to breach a ciphertext, measurement of the security is needed. This is important as it provides computational security to the system. A cipher is said to be computationally secure if there is more benefit to the information in comparison to the cost of breaking or if there is much usefulness in the lifetime of the information in comparison to the time required in breaching the ciphertext [34].

Table 3. Illustrates security level of AES algorithm

AES Algorithm	Key Length	Key Block	Security Level
AES 128	128	128	$2^{128} = 3.4*10^{38}$
AES 192	192	128	$2^{192} = 6.2*10^{57}$
AES 256	256	128	$2^{256}= 1.1*10^{7}$

Consequently, an assumption in the present work is that the aptness of the attacker to breach the cipher has a low probability if there is a rise in the length of the block and the key. Hence, a physical argument reveals computational security in symmetric key against attacks. In Equation (1), the time to attack a cryptographic key where the possible combinations determines the security level of the key length can be calculated using Equation (2) to find the number of combinations checked per second and thereby the number of seconds in one year. Where a faster supercomputer is $10.51*10^{15}$Flops (Floating Point Operation) per second with the quantity of flops entailed per combination check is 1000.

$$\text{Time to attack} = \frac{\text{possible combination}}{\text{No.of combination} * \text{No.of sec}} \tag{1}$$

$$\text{No . of combination} = \frac{10.51*10\text{^}15}{1000} \tag{2}$$

The comparison, on the basis of the time to attack in the AES algorithm versus key length, such that AES-128, AES-192 and AES-256 show in Table 4.

Table 4. Time to attack of AES algorithm versus key size

AES Algorithm	Key Length	Time to Attack
AES 128	128-bit	$1.02*10^{18}$ Years
AES 192	192-bit	$1.87*10^{37}$ Years
AES 256	256-bit	$3.31*10^{56}$ Years

6. CONCLUSION

This paper exhibit comparative study of several operation modes of the AES algorithm for cryptographic ECG biomedical signal in an electronic healthcare application. The main objective was to find out the performance of the most common modes operation such as ECB, CBC, OFB, CFB and CTR of the algorithm and to underline the execution time of each mode of the AES algorithm. Based on the conducted analysis, the AES algorithm was highly computationally expensive, particulary for cryptography for the whole sample of the ECG biomedical signal. The conducted experimental results clearly showed that the security level in 256-bit key length of the AES algorithm is better than 128-bit and 192-bit. However, the OFB mode operation exhibits minimal time of execution within 128-bit (3.28m) in the encryption process (3.29m), the decryption process, and also regarding the cases of ECB and OFB within 192-bit. While the CBC mode operation revealed the lowest time execution in 256-bit (4.51m) encryption process and (4.93m) in the decryption process. Hence, the latency in transmission for these types of data must be fast and feasible in real time because it affects the patient's life within an electronic healthcare application. Therefore, the AES algorithm needs improvement to become more conformable and suitable for healthcare application in the Internet of Things (IoT). In addition, the CBC mode of operation with a 256-bit key size of the AES algorithm is suitable and better practically low processing time with hight level security to use for protection ECG biomedical signal compared to other modes of operation.

REFERENCES

[1] C. K. Chen, *et al*., "Personalized information encryption using ECG signals with chaotic functions," *Inf. Sci. (Ny).*, vol. 193, pp. 125-140, 2012.

[2] V. J. Naveen, *et al*., "Noise reduction in ECG signals for bio-telemetry," *Int. J. Electr. Comput. Eng.*, vol. 9, pp. 1028-1035, 2019.

[3] S. M. Jalaleddine, *et al*., "ECG data compression techniques--a unified approach," *Biomed. Eng. IEEE Trans.*, vol. 37, pp. 329-43, 1990.

[4] U. R. Saxena and S. P. Singh, "Multi-Party Security with SEP using Artificial Neural Networks," *IAES Int. J. Artif. Intell.*, vol. 1, pp. 121-126, 2012.

[5] A. Ghazvini and Z. Shukur, "Security Challenges and Success Factors of Electronic Healthcare System," *Procedia Technol.*, vol. 11, pp. 212-219, 2013.

[6] M. L. Attiah, *et al*., "Adaptive Multi-state Millimeter Wave Cell Selection Scheme for 5G communications," vol. 8, pp. 2967-2978, 2018.

[7] H. K. Patil and R. Seshadri, "Big Data Security and Privacy Issues in Healthcare," *2014 IEEE Int. Congr. Big Data*, pp. 762-765, 2014.

[8] M. Burhanuddin, *et al*., "A Review on Security Challenges and Features in Wireless Sensor Networks: IoT Perspective," *J. Telecommun. Electron. Comput. Eng.*, vol. 10, pp. 17-21, 2018.

[9] P. Wanda and H. J. Jie, "Efficient Data Security for Mobile Instant Messenger," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 16, pp. 1426, 2018.

[10] E. R. Arboleda, *et al*., "Chaotic rivest-shamir-adlerman algorithm with data encryption standard scheduling," *Bull. Electr. Eng. Informatics*, vol. 6, pp. 219-227, 2017.

[11] A. K. Tripathy, *et al*., "Data cryptography based on musical notes on a fingerboard along with a dice," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 14, pp. 1286-1290, 2019.

[12] D. Elminaam, "Performance evaluation of symmetric encryption algorithms," *Int. J. Comput. Networks*, vol. 8, pp. 280-286, 2008.

[13] S. Rajkumar and R. Malaichamy, "Secure cryptographic algorithm for a fault tolerant model in unmanned aerial vehicles," *Int. Conf. Electr. Eng. Comput. Sci. Informatics*, vol. 1, pp. 105-110, 2014.

[14] M. E. Hameed, *et al*., "Review on Improvement of Advanced Encryption Standard (AES) Algorithm based on Time Execution, Differential Cryptanalysis and Level of Security," vol. 10, pp. 139-145, 2018.

[15] M. Katagi and S. Moriai, "Lightweight Cryptography for the Internet of Things," pp. 7-10, 2008.

[16] N. H. M. Ali, *et al*., "A novel multi modification in AES block cipher algorithm for complexity," *International Review on Computers and Software*, vol. 9, pp. 901-905, 2014.

[17] S. S. Priya, *et al*., "An Efficient Hardware Architecture for High Throughput AES Encryptor Using MUX Based Sub Pipelined S-Box," *Wirel. Pers. Commun.*, vol. 94, pp. 2259-2273, 2017.

[18] A. A. Thinn and M. M. S. Thwin, "Modification of AES algorithm by using second key and modified subbytes operation for text encryption," *Lect. Notes Electr. Eng.*, vol. 481, pp. 435-444, 2018.

[19] S. D. Putra, *et al*., "Revealing AES Encryption Device Key on 328P Microcontrollers with Differential Power Analysis," *Int. J. Electr. Comput. Eng.*, vol. 8, pp. 5144-5152, 2018.

[20] D. Blazhevski, "Modes of operation of the aes algorithm," pp. 212-216, 2013.

[21] NIST, "Announcing the ADVANCED ENCRYPTION STANDARD," *Fed. Inf. Process. Stand. Publ.*, vol. 197, 2001.

[22] M. Mohurle and V. V. Panchbhai, "Review on realization of AES encryption and decryption with power and area optimization," *1st IEEE Int. Conf. Power Electron. Intell. Control Energy Syst. ICPEICES 2016*, pp. 31-33, 2017.

[23] S. More and R. Bansode, "Implementation of AES with Time Complexity Measurement for Various Input," vol. 15, 2015.

[24] A. R. Reddy, "Revised aes and its modes of operation," vol. 5, pp. 31-36, 2012.

[25] M. J. Dworkin, "Recommendation for block cipher modes of operation," 2007.

[26] S. Srivastava, *et al*., "Inter Cipher Block Diffusion: A Novel Transformation for Proposed Parallel AES," *2Nd Int. Conf. Commun. Comput. Secur. {[}Icccs-2012]*, vol. 1, pp. 872-879, 2012.

[27] M. Vaidehi and B. J. Rabi, "Design and analysis of AES-CBC mode for high security applications," *2nd Int. Conf. Curr. Trends Eng. Technol. ICCTET 2014*, pp. 499-502, 2014.

[28] M. Dworkin, "NIST Special Publication 800-38G | Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption," *Natl. Inst. Stand. Technol. Spec. Publ. 800-38G*, pp. 1-28, 2016.

[29] P. Rogaway, *et al*., "CTR-Mode Encryption," 2013.

[30] B. Bakhache, *et al*., "Improvement of the security of ZigBee by a new chaotic algorithm," *IEEE Syst. J.*, vol. 8, pp. 1021-1030, 2014.

[31] H. Al-Hamadi, *et al*., "Lightweight Security Protocol for ECG Bio-Sensors," *Wirel. Pers. Commun.*, vol. 95, pp. 5097-5120, 2017.

[32] MIT-BIH, "MIT-BIH arrhythmia database," Available: http://physionet.org/physiobank/database/mitdb/.

[33] A. Lenstra, "Key lengths," *Handb. Inf. Secur.*, pp. 1-37, 2004.

[34] L. S. Models, "and P Erformance E Valuation of M Odels U Sed," pp. 3-7, 2010.