International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 3, June 2020, pp. 3235~3243
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i3.pp3235-3243

An enhanced lossless compression with cryptography hybrid mechanism for ECG biomedical signal monitoring

Mustafa Emad Hameed[1], Masrullizam Mat Ibrahim[2], Nurulfajar Abd Manap[3], Ali A. Mohammed[4]
[1,2,3]Centre for Telecommunication Research and Innovation (CeTRI), Faculty of Electronic and Computer Engineering, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia
[1]Department of Computer Techniques Engineering, Bilad Al-rafidan University College, Iraq
[4]Faculty of Information and Communications Technology (FTMK), Universiti Teknikal Malaysia Melaka (UTeM), Malaysia

Article Info

Article history:

Received Aug 6, 2019
Revised Oct 13, 2019
Accepted Oct 25, 2019

Keywords:

Adaptive Huffman coding
AES
CBC mode
Diffie-Hellman
ECG signal
RSA

ABSTRACT

Due to their use in daily life situation, demand for remote health applications and e-health monitoring equipment is growing quickly. In this phase, for fast diagnosis and therapy, information can be transferred from the patient to the distant clinic. Nowadays, the most chronic disease is cardiovascular diseases (CVDs). However, the storage and transmission of the ECG signal, consumes more energy, bandwidth and data security which is faced many challenges. Hence, in this work, we present a combined approach for ECG data compression and cryptography. The compression is performed using adaptive Huffman encoding and encrypting is done using AES (CBC) scheme with a 256-bit key. To increase the security, we include Diffie-Hellman Key exchange to authenticate the receiver, RSA key generation for encrypting and decrypting the data. Experimental results show that the proposed approach achieves better performance in terms of compression and encryption on MIT-BIH ECG dataset.

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.
Department of Computer Techniques Engineering,
Bilad Al-rafidan University College, Diyala, Baqubah, Iraq.
Email: mihhh221@gmail.com

1. INTRODUCTION

Due to several problems such as unhealthy lifestyle and genetic inheritance of the patient, the medical health-related problems are growing daily. These problems contribute to the development of several chronic diseases such as cancer, diabetes, Alzheimer's and cardiovascular diseases, etc. A survey was submitted by the World Health Organization revealing that cardiovascular disease is the most chronic disease [1]. Thus, efficient diagnosis of cardiovascular disease has become a prominent research topic in the field of biomedical applications. Electrocardiogram (ECG) signals are considered as the promising non-invasive technique to measure the Heart-related activities, functionality and also provides structural information of the heart which helps to analyze the heart-related diseases [2]. Figure 1 shows atrial and ventricular depolarization and repolarization of heart by representing the ECG signal as a series of waves which are known as P, Q, R, S and T waves. The time interval between these peaks provides several critical information which is useful for Heart analysis. There exist several types of intervals which are important for medical analysis. These intervals are known as PQ interval, RR interval, QRS duration, ST segment, and QT interval which can be identified based on the P, QRS complex and T waves [3]. Consequently, ECG signals are widely adopted for remote health monitoring systems using advanced telemedical applications where

patients can be diagnosed and treated from remote assistance [4]. In this type of process, the signal is transmitted over a wireless channel where the original signal gets contaminated.

Moreover, the challenges of ECG signal are require more space for storage and bandwidth requirement for data transmission and also these signals are transmitted over the unsecured channel hence security also becomes a crucial task for the research community [5]. To mitigate the data storage requirement and security, ECG compression, and cryptography-based schemes. As well as, the privacy issue without limiting trading features to avoid data collection attacks and to keep correct open transaction record [6]. During signal transmission for remote monitoring systems, the channel conditions affect the ECG signal quality. Though, a few complexities arise here due to the improper transmission rate or low bandwidth in communication channel. Often, continuous flow of signal may lead to an increase in sheer volume of data [7]. Therefore, the size of data in the communication channel substantially affects the unsuitable transmission rate or low bandwidth [8, 9]. Continuous ECG signal flow can often lead to packet fall and important information loss. However, the compression with the elimination of redundancy in data, which is necessary to optimize storage space and reduce the time needed for data transmission [10, 11]. Furthermore, the improvement of compression mechanism which is depend on a performance evaluation criterion. Though, the most important thing is the new proposed compression algorithm work a high compression ratio (CR), which usually needs a low percentage root mean square difference (PRD). Also, the ECG biomedical signals contain sensitive private health information as well as details that serve to individually distinguish patients, hence must be encrypted prior to transmission across public media so as to prevent unauthorized access by adversaries from cyber-attacks [12, 13].

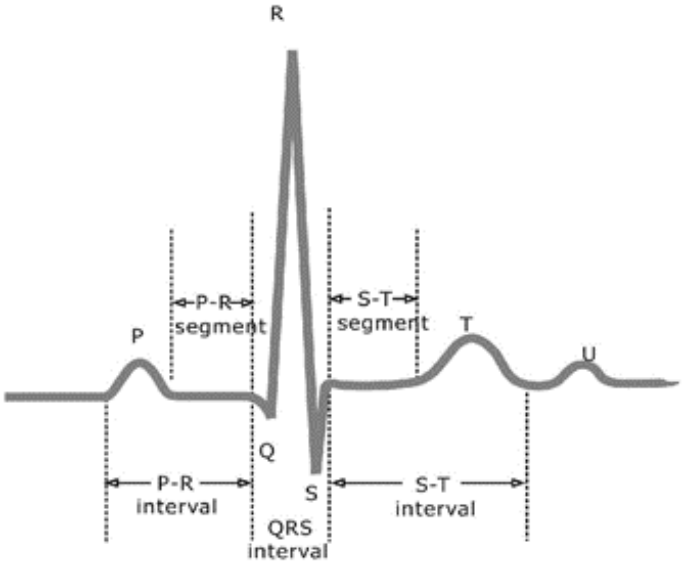

Figure 1. ECG signal representation- P, Q, R, S, T

Therefore, the combination between the compression and cryptography mechanisms its attracted researchers' attention in recent times. In the paper [14] proposed the concept of compressed sensing (CS), one of the newest signal processing techniques which applied to compress the ECG signals with the advantage of very low computational complexity at compression stage to encrypt signals for transmission over insecure channels. As well as, a novel electrocardiogram (ECG) compression method for e-health applications by adapting adaptive Fourier decomposition (AFD) algorithm hybridized with symbol substitution (SS) technique have been presented in [15]. This method as achieves averaged CR of 17.6 to 44.5 and PRD of 0.8% to 2.0% with a highly linear and robust PRD-CR relationship. Another research [16] have propose a scheme that can compress the data without any loss of important information and also apply cryptographic scheme to preserve confidentiality from unauthorized access. In their work, they use mobile computing devise to eliminate usage of computers. They perform preprocessing such as removal of gaussian and baseline noise, detect peaks, do heart rate analysis and compress the ECG signal. At the compression they apply 3 level wavelet transformation (db04) and use threshold mechanisms. Next, Huffman coding technique is used to compress and encrypt the signal. They get the compression rate of 97.72% which is quite decent

for any compression scheme. Further, the ECG signals are transmitted over TCP/IP to telemedicine clinic for specialist' assessment. Otherwise, the existing of encryption-then-compression (ETC) approaches for processing ECG data proposed in [17], which can protect data privacy and also provide the same quality of the reconstructed signals without sacrificing the compression efficiency. Furthermore, another research [18] proposed schemes for compression-then-encryption of the MIT-BIH Arrhythmia ECG signals. Their scheme involves complexity sorting (Beat detection, 2D ECG array formation, Period Normalization, Dc Equalization, Complexity Sorting, Codec Quantization and JPEG2000 codec) and coupled chaotic map mutation. In their scheme, they assume wireless transmission (using Rayleigh fading wireless channel) of ECG through OFDM (Orthogonal Frequency Division Multiplexing) and enhance it to correct impair samples using MMF (Moving Median Filtering). They show storage space minimization through 2D compression mechanism and combined it with chaotic based on mutation scheme to randomize ECG vector for maintaining shield to data confidentiality thus prevent from eavesdropping. Consequently, the study shows that, most of the previous works concentrate more on quality of signal based on peak detection but lacks security aspect. Though few works are found with security model along with compression schemes, but those schemes are not so efficient in terms of lossless compression or hybrid of the encryption scheme is incorporated to provide the security. We propose a new approach based on lossless scheme such as Adaptive Huffman for compression so that there is no information loss upon reconstruction. Also, to avoid the chances of data tampering we make use hybrid between symmetric key and asymmetric key of ciphering based on the AES-CBC, RSA and Diffie-Hellma algorithms with 256-bit key size.

2. RESEARCH METHOD

This section presents the proposed solution for ECG signal encoding & decoding using proposed weighted adaptive Huffman approach with AES-CBC, RSA for key generation and Diffie-Hellma key exchange based ECG data encryption. The complete process is divided into the following phases which are as shown in Figure 2.

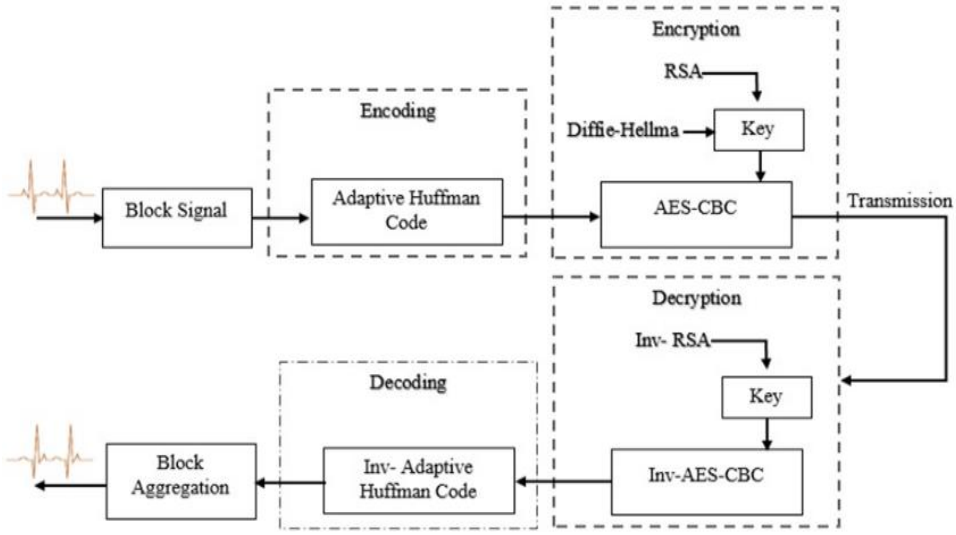

Figure 2. Block diagram of proposed system

An ECG signal is considered from a publicly available data known as "MIT-BIH". In this signal, we consider that ECG signal divide into four blocks with the same size to maintain the processing time and security i.e. the complete signal will be processed into different parts and finally, it can be combined at the receiver end. This process helps to maintain the anonymity in the signal and prevents the outsider attack on the signal. However, in the next phase, we consider each block and perform the weighted Adaptive Huffman encoding to achieve the compressed ECG signal. After compression, we apply AES-CBC, 256-bit key incorporate RSA algorithm for the key generation with Diffie-Hellma key exchange-based encryption scheme to encrypt of each compressed block. At this stage, this data is ready for transmission over unsecured channels. Later, we apply AES based decryption scheme to each received block to decrypt the data into its compressed or encoded form. Therefore, in the next phase, we apply an Adaptive Huffman decoding scheme

to reconstruct the data into its original form for each block and all blocks are combined to form the actual signal vector. Finally, we evaluate the performance of compression and creyptography in terms of PRD, compression ratio and security analysis.

2.1. Signal block creation

Let noisy signal be NS, length of it is L, number of blocks required to be NB, thus, the block size

$$\mathcal{BS} = \mathcal{L}/\mathcal{NB} \quad (1)$$

Now, $\mathcal{B}(i)$ is the set of signal $|\mathcal{NS}|_i$, that can be computed as:

$$\mathcal{B}(i) = |\mathcal{NS}|_i = (\mathcal{NS}_{((i-1)*\mathcal{BS})+1}, \mathcal{NS}_{((i-1)*\mathcal{BS})+2}, .., \mathcal{NS}_{\mathcal{BS}*\mathrm{i}}) \quad (2)$$

where $\mathcal{B}$, is the ECG signal block.

2.2. Adaptive huffman encoding

According to the proposed flow, in this stage, we perform ECG data compression using adaptive Huffman encoding scheme. The Huffman coding is widely adopted for data compression or encoding, according to this process a set of values of fixed coder words are replaced by the optimal set of code words [19]. The Huffman coding considers any input data as an input stream and performs frequency distribution of the data. This frequency distribution is later considered to compress the data. In the first phase, data is compressed with the help of dynamic bit reduction technique and in second phase Huffman coding is used to compress the data further to produce the final output. In the first phase, when a user enters an input text data, the system will find out the occurrence of the number of unique symbols in the input text string and then numeric code will be assigned to these unique symbols. For each numeric code, corresponding binary codes will be generated dynamically to obtain the (compressed) binary output. Then the ASCII code will be generated from the binary output obtained which will serve as the input to the second phase of the system. In the second phase, Huffman Coding will be applied to the output of the first phase to further compress the data and improve the performance of dynamic bit reduction algorithm.

Huffman coding follows a top-down approach means the binary tree is built from the top to down to generate an optimal result. In Huffman Coding the characters in a data file are converted to binary code and the most common characters in the file have the shortest binary codes, and the characters which are least common will have the longest binary code. In a similar way method of decompression works in reverse order. Compressed data is first decompressed by Huffman Decoder and then by dynamic text compression decoder to get back the original data. Following are the steps to compress the data with the help of our proposed system. According to the proposed approach, initially, the occurrence of unique symbols is identified, and a unique numeric code value is assigned to the identified group of symbols. In the next stage, a binary codeword is generated for each symbol assigned initially. This binary codeword represents the compressed data. Huffman coding is based on the top-down computation approach where a binary tree is constructed to generate the optimal solution for data compression. According to the concept of Huffman coding, the data which is converted into binary code is considered for analysis where most common characters of input stream as assigned shortest binary code and least common characters are assigned longest binary codes. Similarly, the data decompression is performed by applying the reverse process of Huffman encoding.

2.3. Hybrid cryptography for ECG signal

In this section, we present the cryptography model to secure the ECG signal while transmitting over the unsecured channel. In order to perform this task, we use AES 256-bit key, based encryption model to generate the ciphers which are obtained using the Cipher Block Chaining (CBC) method. The AES approach is a symmetric key algorithm which takes 128-bit block input data for the given specified times [20]. In this approach, encryption and decryption modules use the same keys which are assigned by the user. In this work, we incorporate RSA based key generation model which is described later in this section. The size of an encrypt-decrypt key may vary as 128, 192 and 256 bits for the input block of 128 bit. Encryption module generates the cipher data from the input ECG data block and decryption process reconstructs the original data from cipher blocks of ECG signal. However, encrypt–decrypt key plays an important role in this field because the number of rounds to be performed on the input block depends on the size of the key. The initial round of AES encryption scheme performs “Add Round Key” in which the input ECG data is XOR’ed with RSA generated cipher key. The Figure 3 shows a flow chart of AES based encryption and decryption methodology.

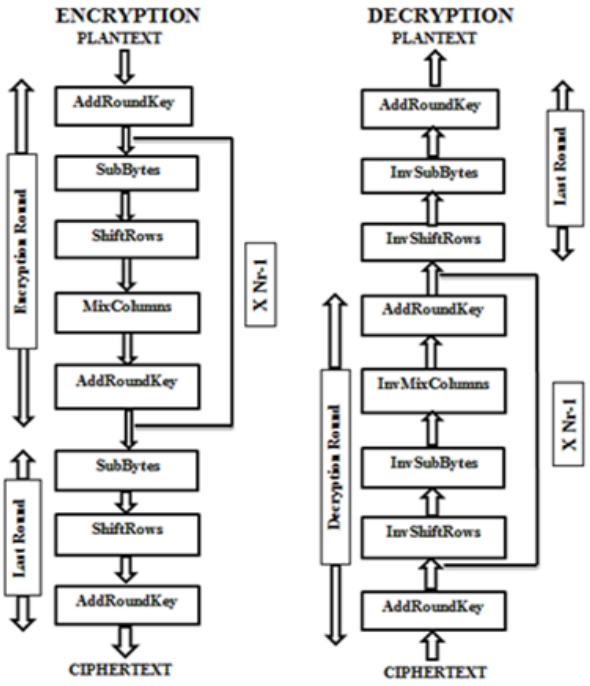

Figure 3. Block diagrams of the AES algorithm

In order to perform the encryption, we use Cipher Block Chaining (CBC) Mode of AES algorithm. According to this scheme chaining of input data is applied with the previous ciphertext blocks [21]. In order to do this, it requires an initialization vector (IV) which is not secure but unpredictable. According to CBC, initially, the first block of an input signal is XOR-ed with the initialization vector which generates the first cipher block. The generated cipher block is then XOR-ed with the next plain text or input ECG signal. Thus, the cipher blocks are created by performing the XOR operation between the cipher block and plaint text. Figure 4 depicts the CBC mode of encryption. The decryption of CBC mode can show in Figure 5. The Encryption process can be presented as:

$$\mathcal{C}(\mathcal{S})_{\mathcal{J}} = \mathcal{E}\left(\mathcal{K}, \left[\mathcal{P}(\mathcal{S})_{\mathcal{J}} \oplus \mathcal{C}(\mathcal{S})_{\mathcal{J}-1}\right]\right), \mathcal{J} = 1,2,..,\mathcal{N} \quad (3)$$

where $\mathcal{E}$ denotes the encryption function which considers $\mathcal{K}$ as the secret key, XOR operation between plain signal block $\mathcal{P}(\mathcal{S})_{\mathcal{J}}$ with the cipher of the previous block, this process is repeated for all blocks [22]. Similarly, the decryption process is performed as:

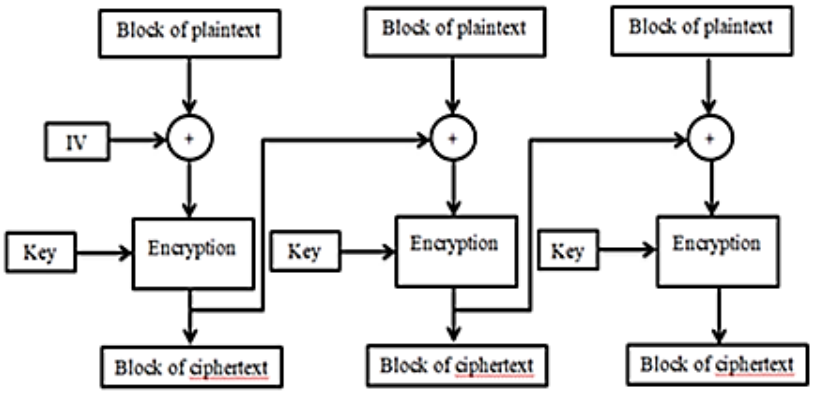

Figure 4. Encryption in the CBC mode

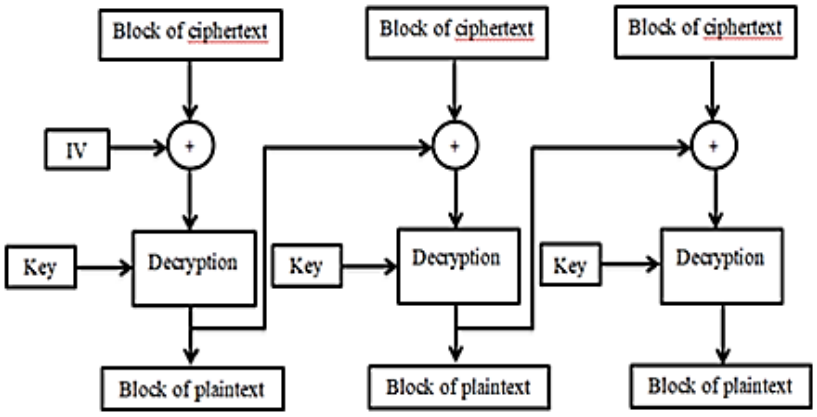

Figure 5. Decryption in the CBC mode

$$\left.\begin{aligned}\mathcal{D}\left(\mathcal{K},\mathcal{C}(\mathcal{S})_{\mathcal{J}}\right)&=\mathcal{D}\left(\mathcal{K},\mathcal{E}\left(\mathcal{K},\left[\mathcal{P}(\mathcal{S})_{\mathcal{J}}\oplus\mathcal{C}(\mathcal{S})_{\mathcal{J}-1}\right]\right)\right)\\ \mathcal{D}\left(\mathcal{K},\mathcal{C}(\mathcal{S})_{\mathcal{J}}\right)&=\mathcal{P}(\mathcal{S})_{\mathcal{J}}\oplus\mathcal{C}(\mathcal{S})_{\mathcal{J}-1}\end{aligned}\right\} \quad (4)$$

$$\mathcal{D}\left(\mathcal{K},\mathcal{C}(\mathcal{S})_{\mathcal{J}}\right)\oplus\mathcal{C}(\mathcal{S})_{\mathcal{J}-1}=\mathcal{C}(\mathcal{S})_{\mathcal{J}-1}\oplus\mathcal{C}(\mathcal{S})_{\mathcal{J}-1}\oplus\mathcal{P}(\mathcal{S})_{\mathcal{J}}=\mathcal{P}(\mathcal{S})_{\mathcal{J}}$$

Where D represents the decryption function secret key and cipher blocks and returns the plain block. In order to generate the public key, we use the RSA algorithm and the generated key is used in the aforementioned process of encryption and decryption [23]. The RSA key generation algorithm is as follows:

RSA KeyGen()
Input: Provide two large prime numbers as p and q
Output: Public and private keys for encryption and decryption.
Step 1: compute n as $n \leftarrow p * q$
Step 2: compute Euler phi value as $\varphi(n) \leftarrow (p-1) * (q-1)$
Step 3: select a random number which satisfies the condition $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$
Step 4: compute d as $d \leftarrow e^{-1} mod(\varphi(n))$
In this work, we use the DH key exchange protocol. Below given Figure 6 shows a sample representation of Diffie-Hellma key exchang.

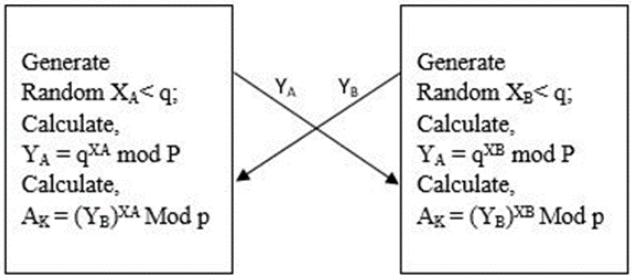

Figure 6. Diffie-hellma key exchange model

3. RESULTS AND DISCUSSIONS

In this section, we present the experimental result and are of the proposed approach to perform ECG signal filtering, compression, and encryption. The complete experimental study is carried out using MATLAB tool and validated on publicly available MIT-BIH arrhythmia dataset. This database contains 48 signal records (360Hz) of 47 unique patients and with a length of 30 minutes each. To compare the results with the methods in, the experimental performance using the signals numbered as 101, 102, 108, 202, 205, 209, 219 and 223 are reported.

3.1. Compression performance

Then, in the next phase, the purpose of the ECG signal compression is to achieve high compression rates without changing the quality of the signal. The compression rate should be checked with the other parameters to evaluate the experimental results of the quality of the reconstructed signal. Therefore, the compression parameters are selected to validate the dynamic compression mechanism, we evaluate the performance in terms of compression ratio and PRD. The compression ratio (CR) is the measure of compression achieved in signal through encoding mechanisms. It doesn't provide information on compressed signal quality but measures the efficiency of an algorithm in reducing storage space [17].

$$CR = \frac{\sum_{n=1}^{N}(bit(\overline{S[n]}))}{\sum_{n=1}^{N}(bit(S[n]))} \quad (5)$$

Here, the encoded signal (S[n])¯and original signal S[n] is converted to bits and then the length of encoded bits is divided with original signal length to fin CR value. The lower the CR, the better is the efficiency. However, the Percentage Root-mean-square Difference (PRD) is a measure to evaluate error or difference between the original S[n] and reconstructed signal (S˜[n]), where N is the length of signal S. The process can be defined as [16]:

$$PRD = \sqrt{\frac{\sum_{n=1}^{N}(S[n]-\hat{S}[n])^2}{\sum_{n=1}^{N}S[n]^2}} \times 100 \quad (6)$$

The above process may not give an accurate measurement of performance as PRD relies much on the mean value of the original signal. Researchers previously established that there should be extra efforts taken to clean the baseline or reduce the DC level. To overcome this issue a modified and advanced version of PRD equation is described in the past which is independent of mean value:

$$PRD\_New = \sqrt{\frac{\sum_{n=1}^{N}(S[n]-\hat{S}[n])^2}{\sum_{n=1}^{N}(S[n]-\acute{S}[n])^2}} \times 100 \quad (7)$$

Here, S´[n] indicate the mean value of the original signal S[n]. Since, the distortion increases as the CR ratio increases, a compression ratio suitable for the type of service and wireless channel environment should be selected. In order to compress and decompress the signal, we have developed an adaptive Huffman approach to achieve a better compression ratio. Any increase in CR may result in a decline in the quality of the signals reconstructed. The quality score (QS) is used to assess compression efficiency while taking into consideration the reconstruction mistakes that have been compromised [24]. The definition of the QS is:

$$QS = \frac{CR}{PRD} \quad (8)$$

A high QS value corresponds to a high quality of compression in a lossy compression method. Therefore, Table 1 illustrates CR, PRD and QS parameters for different ECG records of the MIT-BIH arrhythmia database. All depicted curves are of similar nature (as CR increases PRD also increases) which assures the working ability of the proposed method on different ECG records.

Table 1. Results obtained with proposed adaptive huffman coding for 8 records

Dataset	CR	PRD (%)	QS
100	21.68	0.22	98.54
102	37.6	0.15	237.76
108	18.25	0.20	91.25
117	32.13	0.24	129.58
118	23.8	0.18	129.32
209	24.45	0.18	128. 88
219	21.69	0.19	109.09
223	29.06	0.16	175.45

The proposed compression scheme achieves important compression ratios with a very low PRD rate. It reaches a mean compression ratio of 23.91 for the adaptive Huffman coding. thus, the mean PRD is the same for the different data set and is equal to 0.2%. Table 2 presents a comparison with a different state of the art techniques. It's obvious that our compression algorithm outperforms the state-of-the-art techniques in term of accuracy and efficiency.

Table 2. Performance of different ECG signal compression schemes for record no. 100

Algorithm	CR	PRD (%)	QS
Proposed Algorithm	21.68	0.22	98.54
CS [25]	17.76	5.60	-
Static Low coding	37.5		-
Dynamic Low coding	40.82	0.50	
Dynamic with minimum window size [26]	42.13		
CAE [27]	32.25	1.47	-
SVD [17]	40.1	0.42	95.47
QLV- Skeleto Haffman [28]	16.91	0.64	29.36

However, we notice that no significant distortion is introduced between the original and reconstructed signals. The proposed ECG compression/decompression algorithm is very low complexity and very highly efficient compared with other approaches. In addition, there no need for huge memory resources.

3.2. ECG signal security analysis

In this section, we describe the various types of attacks which can be mitigated using the proposed mechanism. Hence, the security of the data produced mainly depends on the security of the key generator. Furthermore, the only attack model that can be applied to the proposed encryption scheme is the attacks on privacy, as described in [29]. Additionally, according to the security management aspect, we have used DH key exchange, AES cryptography and partitioning the entire ECG signal into 4 bocks. Therefore, the proposed approach can be used for avoiding the following attacks such as user data privacy in this approach, we do not transmit the data in the plain-text form. The original data is encrypted using AES-CBC mechanism with a 256-bit key. Hence, private data information can be secured. The Mutual authentication before transmitting the data over an unsecured wireless channel, we use the DH key exchange to authenticate the receiver module. This authentication process helps to avoid eavesdroppers. However, the mutual authentication using DH key exchange process helps to avoid the man-in-the-middle attacks. The session Key management during transmission of the data, we perform DH key exchange which is limited for the current session. Hence, the false data cannot be transmitted i.e. user 1 data can only be transmitted for user 1's session by using the particular session key. On another hand, the phishing attack: the authentication process helps to avoid the false receiver module hence, the phishing attacks can be avoided using this approach. Consequently, the AES-CBC with a 256-bit key based encryption scheme helps to secure the data while sending the data into the encrypted form [21]. Moreover, we divide the original signal into multiple blocks which increases the security to various attacks. The proposed approach also restricts the eavesdropping attacks by using an encrypted key exchange mechanism.

4. CONCLUSION

In this work, we focus on the development of a secured and efficient mechanism for ECG processing where ECG signal compression, and encryption are the main tasks. However, The ECG signal compression task is done using an adaptive Huffman coding scheme and data encryption is achieved using the AES encryption process. In order to increase security, we incorporate RSA key generation and DH key exchange protocols. The performance of the proposed approach is measured in terms of PRD, CR and security efficacy. the obtained performance is compared with the existing techniques, the comparative analysis shows that the proposed approach achieves better performance. Thus, the results of this paper approve the applicability of the proposed method, for the compression mechanism, and cryptographic technique. This method is then believed to serve as a novel system model for the high compression ratio with minimum reconstruction error and a high level of security.

REFERENCES

[1] E. Yulianto, A. Susanto, T. S. Widodo, and S. Wibowo, "Classifying the EEG Signal through Stimulus of Motor Movement Using New Type of Wavelet," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 1, no. 3, pp. 139–148, Sep.2012.

[2] J. S. Sahambi, S. N. Tandon, and R. K. P. Bhatt, "Using wavelet transforms for ECG characterization. An on-line digital signal processing system," in *IEEE Engineering in Medicine and Biology Magazine*, vol. 16, no. 1, pp. 77-83, Jan.-Feb. 1997.

[3] A. Alesanco and J. Garc´ıa, "Automatic Real-Time ECG Coding Methodology Guaranteeing Signal Interpretation Quality," in *IEEE Transactions on Biomedical Engineering*, vol. 55, no. 11, pp. 2519-2527, Nov. 2008.

[4] D. M. Mirris and A. L. Goldberger, "Braunwald: Heart Disease: A Textbook of Cardiovascular Medicine," 6th ed., Copyright © 2001 W. B. Saunders Company, 2001.
[5] H. Kupwade Patil and R. Seshadri, "Big Data Security and Privacy Issues in Healthcare," *2014 IEEE International Congress on Big Data*, Anchorage, AK, pp. 762–765, 2014.
[6] K. Gai, Y. Wu, L. Zhu, and M. Qiu, "Privacy-preserving Energy Trading Using Consortium Blockchain in Smart Grid," *in IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3548-3558, Jun. 2019.
[7] J. Andreu-Perez, C. C. Y. Poon, R. D. Merrifield, S. T. C. Wong, and G. Z. Yang, "Big Data for Health," in *IEEE Journal of Biomedical and Health Informatics*, vol. 19, no. 4, pp. 1193-1208, Jul. 2015.
[8] S. K. Mukhopadhyay, S. Mitra, and M. Mitra, "An ECG signal compression technique using ASCII character encoding," *Measurement*, vol. 45, no. 6, pp. 1651–1660, Jul. 2012.
[9] M. K. Abdulhameed, Z. Zakaria, I. Ibrahim, and M. K. Mohsen, "Novel design of triple-band EBG Novel design of triple-band EBG," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 4, pp. 1683–1691, Aug. 2019.
[10] D. Gurve, B. S. Saini, and I. Saini, "An improved lossy and lossless combined ECG data compression using ASCII character encoding," *International Journal of Medical Engineering and Informatics*, vol. 8, no. 4, pp. 758–764, 2016.
[11] A.F. Hussein, S.J. Hashim, A.F.A. Aziz, F.Z. Rokhani, and W.A.W. Adnan, "A real time ECG data compression scheme for enhanced bluetooth low energy ECG system power consumption," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–14, Aug. 2017.
[12] K. Gai, M. Qiu, Y. Li, and X. Liu, "Advanced Fully Homomorphic Encryption Scheme Over Real Numbers," *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, New York, NY, pp. 64-69. 2017.
[13] H. Al-Hamadi, A. Gawanmeh, J. Baek, and M. Al-Qutayri, "Lightweight Security Protocol for ECG Bio-Sensors," in *Wireless Personal Communications*, vol. 95, no. 3, pp. 5097–5120, Apr. 2017.
[14] M. Fira, "Applications of compressed sensing: Compression and encryption," *2015 E-Health and Bioengineering Conference (EHB)*, Iasi, pp. 1-4, 2015.
[15] J. Ma, T. Zhang, and M. Dong, "A novel ECG data compression method using adaptive fourier decomposition with security guarantee in e-health applications," in *IEEE Journal of Biomedical and Health Informatics*, vol. 19, no. 3, pp. 986-994, May 2015.
[16] M. Raeiatibanadkooki and S. R. Quchani, "Compression and Encryption of ECG Signal Using Wavelet and Chaotically Huffman Code in Telemedicine Application," *Mobile Systems*, vol. 40, no. 3, pp. 1-8, Jan. 2016.
[17] T.Y. Liu, K.J. Lin, and H.C. Wu, "ECG data encryption then compression using singular value decomposition," in *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 3, pp. 707-713, May 2018.
[18] A. Pandey, B. S. Saini, B. Singh, and N. Sood, "Complexity sorting and coupled chaotic map based on 2D ECG data compression-then-encryption and its OFDM transmission with impair sample correction," *Multimedia Tools and Applications*, vol. 78, no. 9, pp. 11223–11261, May 2019.
[19] N. A. M. Mustafa Emad Hameed, Masrullizam Mat Ibrahim, "Compression and Encryption for ECG Biomedical Signal in Healthcare System," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 6, pp. 2826-2833, Dec. 2019.
[20] M. E. Hameed, M. M. Ibrahim, and N. A. Manap, "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*, vol. 10, no. 1, pp. 139–145, 2018.
[21] M. L. A. Mustafa Emad Hameed, Masrullizam Mat Ibrahim, Nurulfajar Abd Manap, "Comparative study of several operation modes of AES algorithm for encryption ECG biomedical signal," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 6, pp. 4850-4859, Dec. 2019.
[22] M. Vaidehi and B.J. Rabi, "Design and analysis of AES-CBC mode for high security applications," *Second International Conference on Current Trends in Engineering and Technology-ICCTET 2014*, Coimbatore, pp. 499-502, 2014.
[23] E.R. Arboleda, J.L. Balaba, and J.C.L. Espineli, "Chaotic rivest-shamir-adlerman algorithm with data encryption standard scheduling," *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 3, pp. 219–227, Sep. 2017.
[24] S. Lee, J. Kim, and M. Lee, "A real-time ECG data compression and transmission algorithm for an e-health device," in *IEEE Transactions on Biomedical Engineering*, vol. 58, no. 9, pp. 2448-2455, Sep. 2011.
[25] A. Singh, L. N. Sharma, and S. Dandapat, "Multi-channel ECG data compression using compressed sensing in eigenspace," *Computers in Biology and Medicine*, vol. 73, pp. 24–37, Jun. 2016.
[26] H. Anas, R. Latif, and M. Arioua, "Efficient electrocardiogram (ECG) lossy compression scheme for real time e-Health monitoring," *International Journal of Biology And Biomedical Engineering*, vol. 11, pp. 101–114, 2017.
[27] O. Yildirim, R. S. Tan, and U. R. Acharya, "An efficient compression of ECG signals using deep convolutional autoencoders," *Cognitive Systems Research*, vol. 52, pp. 198–211, Dec. 2018.
[28] H. Kim, R. F. Yazicioglu, P. Merken, C. Van Hoof, and H. J. Yoo, "ECG signal compression and classification algorithm with quad level vector for ECG holter system," in *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 1, pp. 93-100, Jan. 2010.
[29] M. Burhanuddin, A. Mohammed, R. Ismail, M. E. Hameed, A. N. Kareem, and H. Basiron, "A Review on Security Challenges and Features in Wireless Sensor Networks: IoT Perspective," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 10, no. 1–7, pp. 17–21, 2018.