SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Cloud Security System for ECG Transmission and Monitoring Based on Chaotic Logistic Maps

Rajasree Gopalakrishnan[1,*], Retnaswami Mathusoothana Satheesh Kumar[1]

[1] Department of Information Technology, Noorul Islam Centre for Higher Education, Tamil Nadu, India

ARTICLE INFO

Article history:
Received 8 September 2023
Received in revised form 17 November 2023
Accepted 23 January 2024
Available online 12 February 2024

Keywords:

Cloud computing; Chaos theory; Chaotic logistic map; Electrocardiogram; Fingerprint; Biometric; Cryptography

ABSTRACT

Biomedical data or information must be transmitted securely via the internet for smart healthcare. The Electrocardiogram (ECG) signal is amongst the most essential clinical signals which must be delivered to hospital facilities. Prime focus of this research is on the encryption of ECG for secure transmission. Chaos theory is used for the development of deterministic nonlinear systems, that can be used to create random numbers for the Chaotic Logistic Map (CLM) based encryption. This study describes a cryptographic algorithm for encrypting ECG signals that uses a mix of the CLM and fingerprint data. The common factor between the patient section and monitoring section is the operation on sample data points of ECG. The choice of proper encryption and decryption theme can save more amount of time and is invulnerable both to noise-based attacks and hacking instances. The proposed framework is implemented on Dropbox based cloud storage and access is possible from any given locations. Simulation tests are used to assess the system performance in terms of Structural Similarity Index Matrix (SSIM), Histogram, Spectral Distortion (SD), Correlation and Log-Likelihood Ratio (LLR). The incorporation of complex layers of CLM encryption increases security.

1. Introduction

As computers and information technology advance, digital information is widely being utilized in practical systems. The quality of health treatment might be enhanced if a doctor could be brought to the patient's house using telecommunication technology. Biomedical engineers are working on a computing environment that is capable of collecting medical data and securely store it on a remote server. The ECG signal is the representations of electrical events occur in a heart. It is being used to diagnose cardiovascular disorders. The myocardial muscles in the heart are responsible for the contractions in a rhythmic manner and subsequently drive blood flow throughout the system. This distribution of current is not arbitrary and it is well organized. As an outcome, the systole is strong and coordinated. These continuous processes results in ECG. The major variables that impact ECG are oxygen deficiency in the myocardium and defect in heart structure. Cloud technology is becoming

* *Corresponding author.*
E-mail address: rajasreegrni@gmail.com

https://doi.org/10.37934/araset.39.2.118

increasingly popular over the years. Many key characteristics distinguish a cloud-based healthcare professional [1]. For instance, it is possible to be viewed from anywhere by healthcare professionals. Customers are not required to set up programs locally. Because of the charge-per-utilization model, the expense of cloud services is substantially lowered. Similarly, for healthcare applications, remote transfer of biological data or information should be secure.

The Electrocardiogram (ECG) signal is a most essential medical signal that must be delivered to healthcare facilities. For the automated diagnosis of cardiac condition and disorders, ECG signals must be evaluated. The ECG signals need to be transferred from the handheld measuring device to the processor for further analysis and extraction of information. During the transmission procedure, the ECG signals must be secure. It is for this reason that ECG signal encryption is critical [2]. Encryption based on the patient's or doctor's biometrics can be used in healthcare systems which may be vulnerable to hacking attempts. ECG signal encryption can be utilized to create deflectable variations of ECG signals. Because of the increase demand in the security of biometric signals, the ECG signal encryption issue is discussed in this study. Fingerprint is unique for all human beings and it has been used in various literatures for the encryption and decryption of biomedical data and images. The hardware required for acquiring the fingerprint is economical and integration is easy with embedded systems. The features extracted from fingerprint cannot be used as a key for encrypting ECG signal. There is a necessity for the generation of separate key based on the features extracted from biometric fingerprint image. The fingerprint positions may vary while acquiring fingerprint of the same person at different scenario. So, a combination of fingerprint, generated key and ECG are required for ECG encryption. Since cloud computing is incorporated, the key required for encryption and decryption can be shared through a common channel and authentication can be performed for remote access. The fundamental model of a patient monitoring system with Body Sensor Network is depicted in Figure 1.

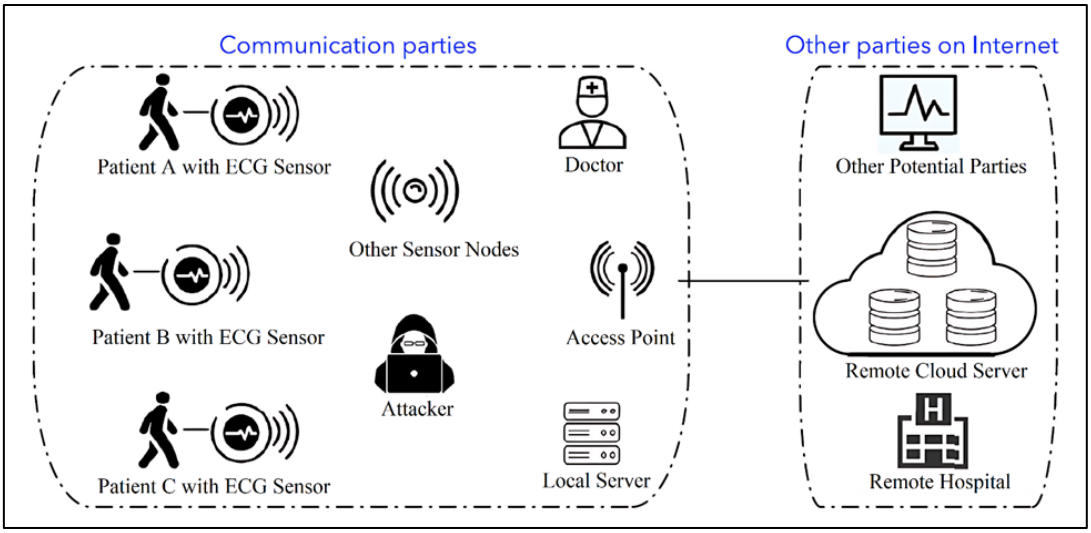

Fig. 1. Basic Structure of Patient Monitoring System

The Advanced Encryption Standard (AES) is an extensively used public-key cryptographic algorithms for both data and picture encryption. Hameed *et al.,* [3] have extended it to ECG encryption. The effectiveness and complexity in computational of AES encryption are well-known to be highly dependent on the operational mode. Mathivanan *et al.,* [4] created an encryption framework for ECG focused on converting ECG data into binary counterparts of decimal. These binary sequences are translated to QR codes, which are subsequently reassigned to decimal. In a noise-free environment, this procedure is considered to function well. A multifunctional method for masking

the data in ECG was published by Bhalerao *et al.,* [5]. To protect the privacy of the patients' information, a hashing technique was used to the ECG signals for watermark embedding, and a prediction model utilizing deep learning. McGregor *et al.,* [6] introduced a paradigm for web services in remote and local Neonatal Intensive Care (NIC) that allows real-time biological data transfer. They created a cloud-oriented service and was demonstrated it using a NIC unit case study. Pandeya *et al.,* [7] developed a cloud-oriented platform for offering ECG analysis services that is both extensible and cost-effective. It was created to gather ECG using handheld gadgets and send the information to distant mainframe for simple evaluation. For demonstration purposes, a prototype system was created. However, substantial difficulties must be rectified before such a system can be put into practice.

Liu *et al.,* [8] suggested that, existing compression after encryption methods for ECG that use cutting-edge encryption algorithms often trade compression efficiency or quality. Shaikh *et al.,* [9] conceived and built a security-enhanced ECG system for ECG diagnosis and visualization that is both safe and private. The QRS complex approach will be utilized to diagnose the obtained ECG data in this study. The outcome of the QRS complex technique is utilized to show if a patient is healthy or unwell. If the condition is critical, the system will send an alarm for further diagnostics, which will aid medical practitioners in the identification of arrhythmias and medical researchers in their study. The system's security and privacy features use security-enhancing approaches to preserve the validity and confidentiality of the patient's medical data. The suggested Fully Homomorphic Encryption (FHE) technology will be used to encrypt the signals, which will fix the problem. The contributions of this research are demonstrated by applying these concepts to two classic challenges in natural algorithm computation and signal processing.

Since the constant heart rate recordings and important parameter to store, ECG data requires a big memory storage device. Before transmitting it to the telemedicine centre for monitoring and analysis, it is compressed using effective compression algorithms. In addition, the acquired ECG signals are compressed after being processed using several filtering algorithms to reduce unwanted noise. The usage of buffer blocks was proposed by Hameed *et al.,* [10], which is a first in this sector. The use of highly efficient technologies for peak identification, noise reduction, compression, and encryption ensure that the ECG signal is sent from the sensor to the monitor in a secure way. This work also makes advantage of the AES 256 CBC mode, which is rarely utilized in embedded systems but is incredibly powerful and efficient at encrypting data. The suggested work has a PRD of 0.41% and a Compression Ratio of 0.35%, which is much superior than existing systems. On five different signal recordings in MIT-BIH datasets, experimental findings implicate that the suggested strategies are effective.

Hameed *et al.,* [11] presented a technique that uses encryption and compression to provide smooth and safe ECG transfer from sensing location to monitoring location. The reconstructed signal's quality acquired by utilizing the suggested technique, which employs DWT and Huffman algorithm are superior to that achieved with unencrypted compression, according to this research. Security is tested against wiretapping and passive tracking. With a growing requirement for confidentiality in data gathering techniques that store personal data concealed in useable information, privacy problems in healthcare have gotten a lot of attention recently. Impio *et al.,* [12] created a multi-level encryption technique based on compressive sensing for ECG signals in order to disguise probable heart rate irregularities from semi-authenticated users and keeps the beat pattern for heart rate visualization. The suggested multi-level encryption approach can reduce heartbeat anomaly classification accuracy by an average of 50% while retaining a high R-peak identification efficiency. The usability of the ECG data produced is a major problem. Artifacts and electrode misplacements can make ECG data difficult to understand, especially if the individual collecting the

data is inexperienced. The major objective of this work is to develop an efficient ECG encryption algorithm for cloud computing applications.

2. Methodology

A secure ECG transmission and reception system consists of strong encryption algorithm, which is capable of altering the structure of ECG based on the key generated. The acquisition of fingerprint is widely facilitated by optical sensors. The quality provided by acquired fingerprint determines the efficiency of encryption as well as decryption processes. A key generator is used for the generation of key corresponding to the scanned fingerprint. The matching and authentication are performed by incorporating K-Nearest Neighbor (KNN) Classifier. Chaotic Logistic Map algorithm is the ultimate choice for the encryption of ECG because of its complexity and robustness against various types of attacks. The cloud application used in this work is based on Dropbox which is compatible with MATLAB for the simulation of the proposed framework. The system administers access of the ECG data to the respective doctor and patient for maintaining secrecy of diseases. Figure 2 depicts the overall design of the proposed cloud-based ECG acquisition and monitoring system.

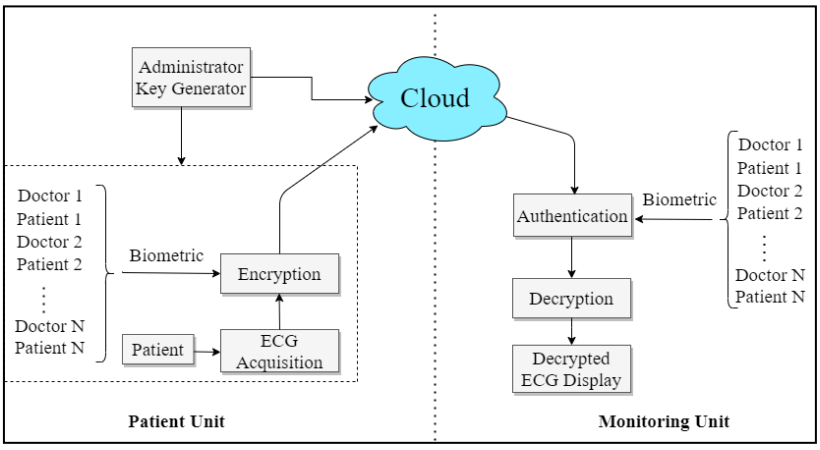

Fig. 2. Flow Diagram of Proposed ECG Monitoring System

The entire system is divided into two section named patient unit and monitoring unit. Both these units are interlinked using the cloud server. The fingerprint biometric is used to generate the key required for encrypting the ECG signal. The patient unit is a handheld unit which is connected to the cloud server via internet for real time update of ECG, biometric and key. The detailed process flow along with all the components of the patient unit is given in Figure 3.

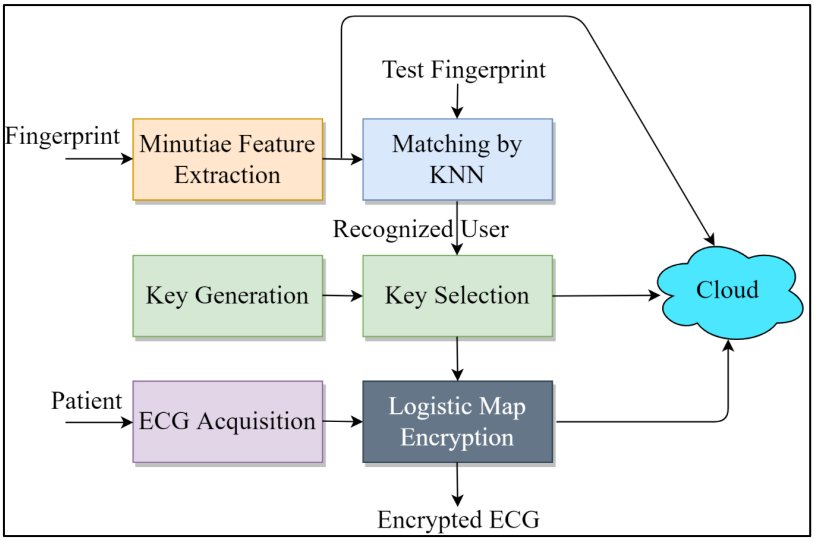

Fig. 3. Flow Diagram of Patient Unit

2.1 Fingerprint Feature Extraction

Identification of suitable pixel or block characteristics is the initial stage in developing an algorithm for fingerprint image segmentation. The pixel characteristics are retrieved for every pixel or block in the fingerprint images, and each block is categorized based on collected feature attributes. Computation of the ROI, elimination of false minutiae, finding ridge ending points, and detection of bifurcation are part of the feature extraction step. The existence of noise in fingerprint pictures has been proven to cause erroneous minutiae. To solve this issue, feature extraction was used to efficiently identify the minutiae points in fingerprints. The detailed process flow of feature extraction along with feature fusion is delineated in Figure 4.

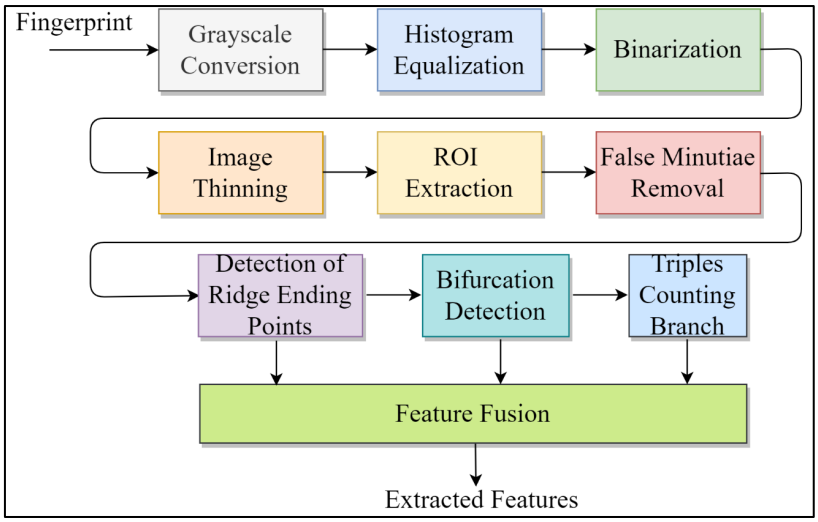

Fig. 4. Flow Diagram of Fingerprint Feature Extraction

The fingerprint images captured by the scanner are RGB images that have to be transformed to a grayscale image for further processing [13]. Grayscale conversion may be as simple as averaging. The average of three colours is all that is required. Since it is an RGB image, it is required to add the R value by the G value and the B value and then divide by 3 to get the necessary grayscale image. Histogram Equalization is an image enhancement technique that transforms the intensity of a

fingerprint to boost contrast. The cumulative density function straightens the histogram and expands the dynamic selection of intensity levels in Histogram Equalization. Histogram Equalization draws attention to the boundaries and borders between items, but it may obscure local features, making it ineffective for local improvement. The grey values histogram for image *I* (*x*, *y*) with *K* discrete level is calculated using the occurrence probability of grey level *i*. The number of total pixels in an image is *N*, the overall pixel count with same pixel intensity is *n*, and the total number of grey levels in an image is *K*. Eq. (1) gives the likelihood of a pixel of a particular level *I* appearing in the picture, and Eq. (2) gives the Cumulative Distribution Function (CDF) for histogram equalization.

$$P_i = \frac{n_i}{N},\ 0 \le i < L \tag{1}$$

$$cdf_x(i) = \sum_{j=0}^{i} P_x,\ x = j \tag{2}$$

The next stage is image binarization, which involves transforming the 8-bit grey level fingerprint into a single bit binary image representing valley as 1 and ridge as 0. Ridges and valleys are outlined with black and white hue after the image binarization process. The grey scale fingerprint image is binarized using a locally adaptive technique. This technique involves the conversion of a pixel's intensity to 1, when the original value is higher compared to the mean intensity of selected 16x16 block. The thinning method employs a hit-miss transformation to determine the structure of a series of pixels. This method uses a pattern set *S* to strike pixels in the image set *X*. If the image is viewed of as a set, the output indicates that the hit operation produced a set of pixels that should be removed.

$$X \otimes S = X - \left(X \oplus S\right) \tag{3}$$

The region of interest (ROI) must be extracted after thinning. A fingerprint threshold is specified for ROI extraction to reject the background from the whole region. The ROI, which is employed to assess the fingerprint image, is the remaining region created as an outcome of the thresholding process. The ridge's redundant pixels are eliminated using the thinning method, resulting in a ridge of single pixel wide. Then minutiae labelling is performed utilizing a window (3x3). Crossing Number (CN) technique is utilized for minutia labelling. While considering bifurcation, the value of CN(p) is 3, while for termination, the value is 1. In minutia marking, a real branch is thrice counted, and it is considered as a peculiar case. The topmost and rightmost pixels in the specified 3x3 window with a neighbour outside the 3x3 frame are designated as branches. However, when just one branch is available in a limited area, a check mechanism is necessary to ensure that none of the branches' neighbours are added, as illustrated in Figure 5. The features of ridge necessary to indicate a person's identification are bifurcation, termination, and triples count. Each of these characteristics has a set of feature points, and the relevant features will be chosen solely on the basis of their quality. These characteristics are fused (mixed) to produce a collection of relevant features for fingerprint recognition [14].

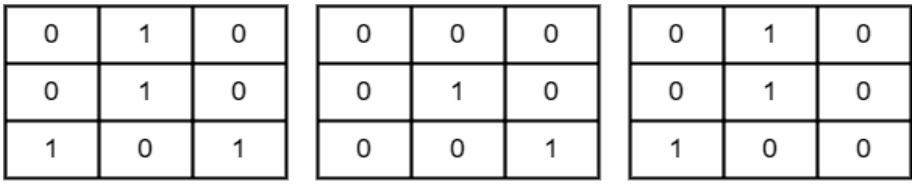

Fig. 5. 3x3 windows for (a) bifurcation (b) termination (c) triples count

2.2 Fingerprint Matching

KNN algorithm is ultimately a methodology for the classification of entities in a feature map depending on their proximity to training samples. Generally, fingerprints are categorized by considering the labels of its K number of closest neighbours by calculating the predominant vote. K value equal to 1 indicates that the object can be categorized as a closest object class. For just 2 classes in the image, then the value of k must be an odd integer. Nevertheless, there are possibilities of occurrence of ties for odd vales of K in multi-class scenario [15]. The Euclidean distance between two pixels is given by Eq. (4). Consider *x* and *y* as the histograms in $X = R^m$.

$$d_e(x,y) = \sqrt{\sum_{i=1}^{m}(x_i - y_i)^2} \tag{4}$$

The key generator is an important part of the cryptosystem. Each patient and doctor will be allotted with a random secret key. This key is generated using a 128-bit Pseudo Random Number Generator (PRNG). The major component of a PRNG is the deterministic algorithm where a seed is supplied as an initial input to generate random numbers that can be used as key. The basic requirements for the computation of PRNG are modulus (*m*) greater than *0*, a multiplier (*m*), an increment (*c*) and seed value X_0. The equation for PRNG is given by,

$$X_{n+1} = (aX_n + c) \bmod m \tag{5}$$

The key is selected and assigned to doctors and patients based on the identification of individual using fingerprint features. After assigning a 128-bit key to a particular person, the key is uploaded to cloud. The key and fingerprint will be linked and the ECG can be accessed from any location where internet is available. This computation utilizes 16 rounds for a 128-bit key size, as compared to standard 10 rounds. The raise in rounds' count will increase the computing complexity and computational time. The system's security is improved by raising the rounds' count, which provides privacy to authorized users. The ECG is fed to the encryption algorithm in the form of a text. The size of input ECG is an important factor that determines the computational time of the proposed algorithm.

2.3 ECG Cryptography with Chaotic Logistic Map

This work intent to increase the secrecy and security administered by chaotic map-based signal encryption. In this study, a N-array synthesizer for key stream is presented. The dynamic matrix is created by utilizing a Linear Feedback Shift Register (LFSR), and the cryptographic keys are based on multi-level logistic maps. This process increases the randomness of the signal. Chaos is an unpredictably disordered state. A chaotic system is a non-predictable system that displays

randomness and entirely unexpected behaviour [16]. It is utilized in cryptography because of randomness and aperiodicity. It is employed to generate random numbers. The generated series are entirely different and can be made to differ just slightly in their starting values. Several inferences regarding the properties of chaotic systems may be made using this definition. Since the system is dynamic and nonlinear, it is susceptible to the influence of the initial conditions. The system's output is not directly proportional to the input. The basic principles of the system are deterministic (as opposed to probabilistic), and they allow for discrete changes. There is no random component in the system since the states must abide by these criteria.

Proposed model is developed to design encryption algorithm for ECG signals by using CLM. When different equations are used, CLM sequences are produced that appear completely random to an outside observer [17]. Since they are sensitive to initial conditions, the sequence formation is predictable, hence this article solely examines the logistic map. A complicated chaotic system based on polynomial mapping is the logistic map. The behaviour of logistic map can be represented using nonlinear dynamic equations. The 1-D coupled logistic map is explained using Eq. (6).

$$X_{n+1} = rX_n(1 - X_n) \tag{6}$$

As the number of iterations increases, the complexity of CLM increases and it will be difficult for the attacker to extract information. Initial iterations of the CLM are defined using Eq. (7) to Eq. (9).

$$X_1 = rX_0(1 - X_0) \tag{7}$$

$$X_2 = rX_1(1 - X_1) \tag{8}$$

$$X_2 = r^2X_0(1 - X_0)(1 - rX_0 + rX_n^2) \tag{9}$$

Here, X_n is the state variable, that creates values in the interval [0,1] and n is the iteration count. r is the control parameter and its value is present in the range $0 < r \leq 4$. The bifurcation map depicted in Figure 6 displays the period splitting in the stable orbits from 1 to 4.

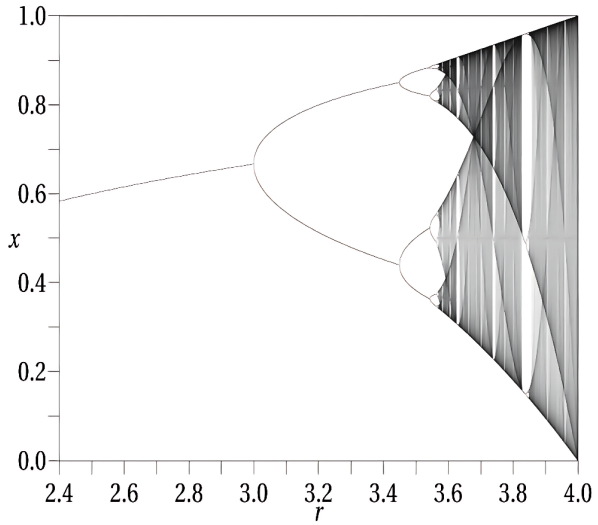

Fig. 6. Bifurcation Diagram of the Logistic Map

These locations of bifurcation are all periods-doubling bifurcations. The first Feigenbaum constant converges to the ratio of the lengths of successive intervals between values of r when bifurcation occurs [18]. Different values of r will provide quite different signals as illustrated in Figure 7.

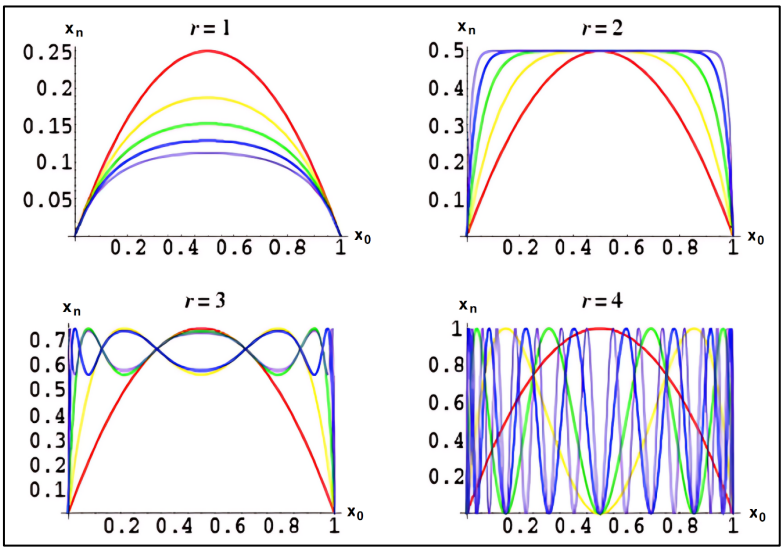

Fig. 7. Bifurcation Parameters of Logistic Map

The ECG signal obtained from the patient is given as the input to the CLM algorithm. At first the signal is sampled and divided into wavelets at every 100ms. The key is generated using the features extracted from the biometric image. Two LMs are involved in the key generation to increase the complexity of the algorithm. The biometric feature-based key is given as the seed key for LM1. A random 128-bit number is given as the seed for LM2. A Linear Feedback Shift Register (LFSR) is used to combine these two keys and generate the final key [19]. The key is then XOR operated with the sampled signal to obtain the encrypted signal. Decryption can be performed simply by XOR operating encrypted signal with the key. The process flow of proposed CLM algorithm is depicted in Figure 8.

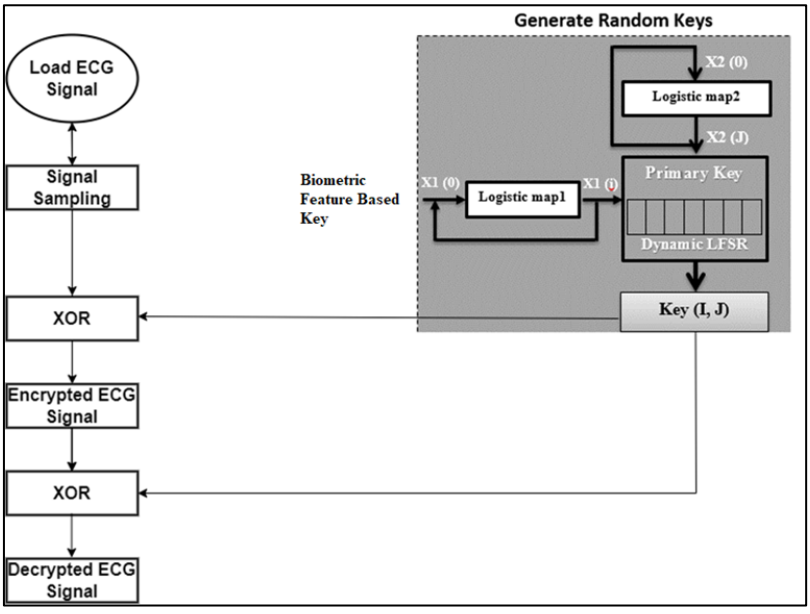

Fig. 8. Process Flow of Chaotic Logistic Map

In order to encrypt an ECG signal, the CLM should perform a sequence of steps that are explained in Algorithm 1.

Algorithm 1: CLM Encryption
Input: ECG signal *X(t)* from the patient, Primary key K_1 based on biometric features.
Output: Encrypted ECG signal $X_E(t)$.
Step 1: Sample the ECG signal X(t) at 100 ms.
Step 2: Obtain the primary key K_1
Step 3: Convert K_1 into bit stream.
Step 4: Convert K1 into equivalent 1-D binary array called BinK1 [M].
Step 5: Initialize the parameters of LM (X_0, R), where, $X_0 \in [0, 1]$ & $R \in [0, 4]$.
Step 6: Apply LM to generate the factors (Increment, Max, Values, Ranges, Min).
Based on BinK1,
Increment = (Max values / Number of samples).
Step 7: The resultant of the Eq. (5) represents [M] in BinK1.
Step 8: The resultant of the Eq. (9) represents [M] in BinK2.
Step 9: Apply LFSR to each [M] in BinK1 and BinK2 to generate the key K.
Step 10: Perform the encryption (using XOR operations) on the signal X(t)

$$X_E(t) = X(t) \oplus K$$

In order to decrypt the received ECG signal at the doctor's end, the CLM performs a sequence of phases that are explained in Algorithm 2.

Algorithm 2: CLM Encryption
Input: Encrypted ECG signal $X_E(t)$, Primary key K_1 based on biometric features.
Output: ECG signal *X(t)* from the patient
Step 1: Obtain the encrypted ECG signal $X_E(t)$
Step 2: Generate the keys K1 and K2 as explained in Algorithm 1.
Step 3: Apply LFSR to each [M] in BinK1 and BinK2 to generate the key K.
Step 4: Perform decryption on the sequences:

$$X(t) = X_E(t) \oplus K$$

Step 5: Create the decrypted ECG signal.

2.4 Monitoring Unit

The monitoring unit consists of a fingerprint scanner to identify the user. The fingerprint image obtained by the scanner will undergo feature extraction and classification process to verify the authenticity of current user. The features extracted will be matched using KNN algorithm and the equivalent key will be selected [20]. This key will be used for the decryption of the ECG which is extracted from the cloud. The detailed flow diagram of monitoring unit can be visualized in Figure 9.

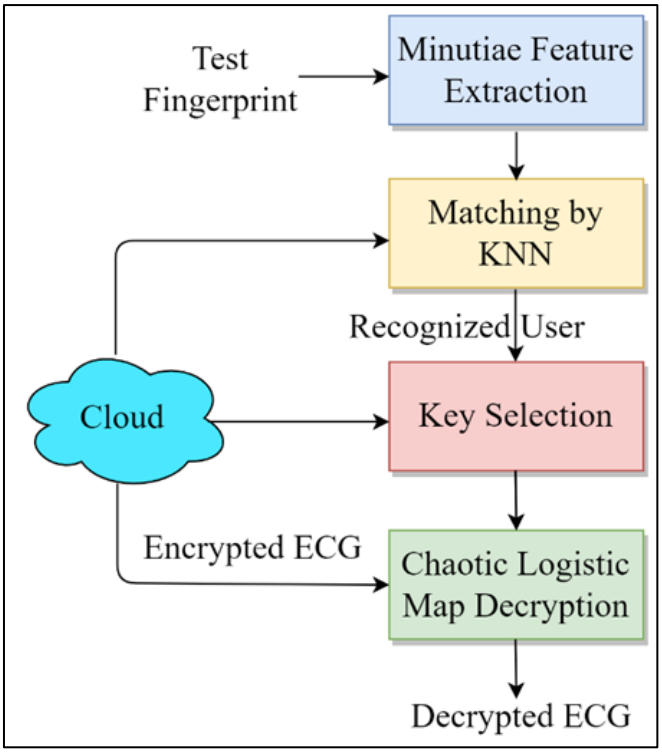

Fig. 9. Flow Diagram of Monitoring Unit

3. Results

Simulation testing is performed to determine the proposed cryptosystems' performance. MATLAB is used to implement all of the suggested cryptosystems (R2018a). The CLM algorithm is used for encryption of the initial ECG signals and to test the efficiency. The ECG data used for experiment were taken from MIT-BIH dataset of arrhythmia [21]. Each signal in the database has a length of roughly 30 minutes and a sampling frequency rate of approximately 360 Hz. Nearly 48 ECG signals may be found in this dataset. The performance review method took into account a variety of measures and views [22]. The fingerprint obtained from fingerprint scanner undergoes all the steps explained in the process flow to obtain the features required to identify a person. Fine details from the fingerprint are extracted to evaluate its structure for identification purpose. These detailed evaluation increases the efficiency of matching algorithm. The results obtained during the feature extraction process are depicted in Figure 10.

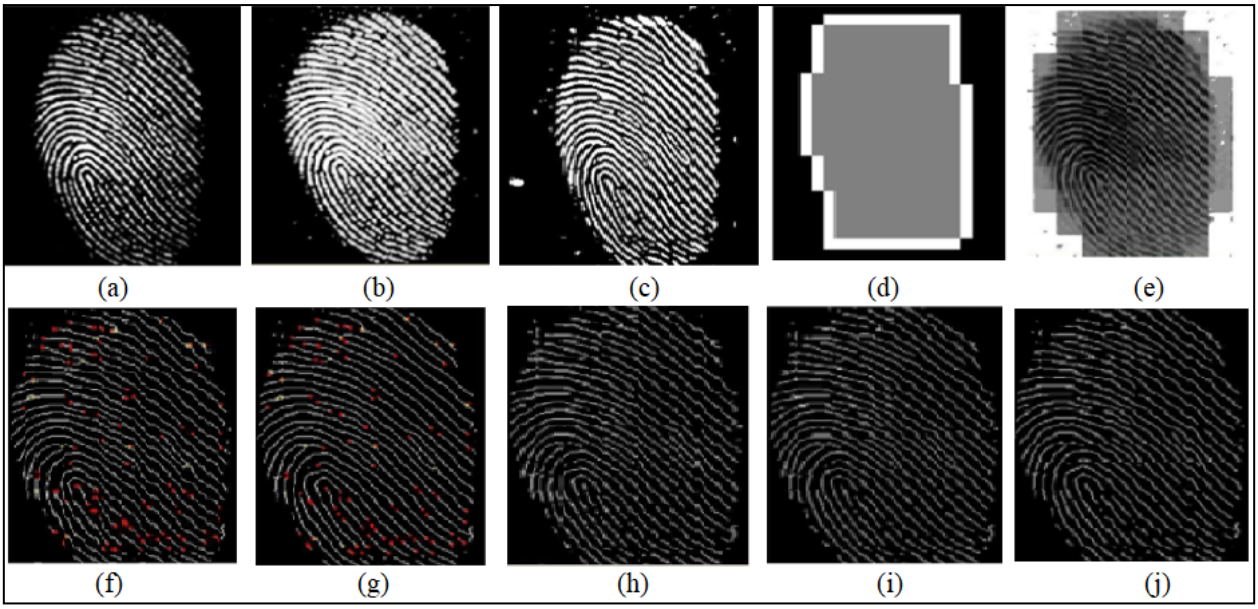

Fig. 10. Fingerprint feature extraction results (a) input fingerprint image (b) Enhanced fingerprint (c) Binarized (d) ROI mask (e) ROI (f) Minutiae marked (g) Minutiae removed (h) Ridge bifurcation (i) Ridge ending (j) triples counting branch

These features are utilized to generate key for the encryption of ECG signals. The original ECG signal, the ECG encrypted using CLM algorithm and the decrypted ECG signal are depicted in the Figure 11. Here it is possible to observe the difference in amplitude and frequency of the ECG due to the encryption process [23,24].

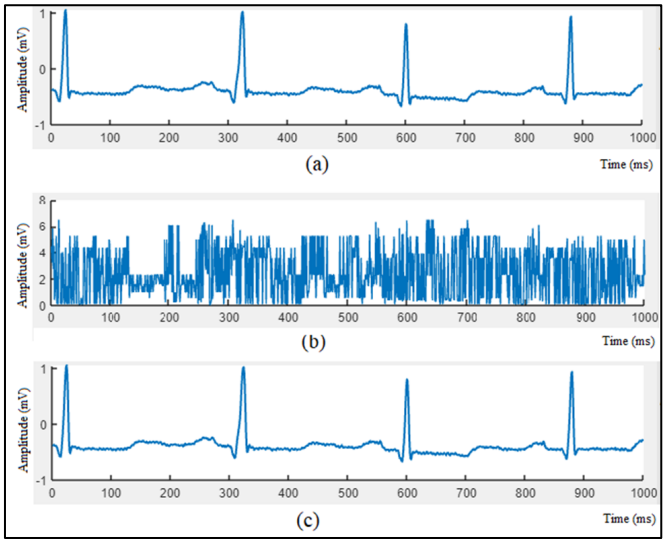

Fig. 11. ECG encryption (a) Input ECG (b) Encrypted ECG (c) Decrypted ECG

The performance of proposed encryption system for the improvement of security in biomedical signal transmission is evaluated in a qualitative and quantitative manner. The execution time of the proposed encryption algorithm decreases due to decrease in the number of rounds in key generation. The execution time depends on the size of the ECG file used for testing. If the file size is increased, the execution time also increases. The execution time is computed and compared with the execution

time of standard encryption algorithms. Table 1 and Figure 12 explains the variation in execution time with respect to various input file size.

Table 1
Execution Time Comparison

File Size of ECG (kB)	Execution Time for Encryption (ms)			
	DES	TDES	AES	CLM (Proposed)
16	2.25	2.32	2.20	1.82
43	6.32	7.29	6.18	4.32
91	8.64	9.43	9.31	7.31
156	11.57	12.89	11.46	10.04
302	14.68	15.37	16.13	12.14
415	17.32	17.93	18.72	14.83

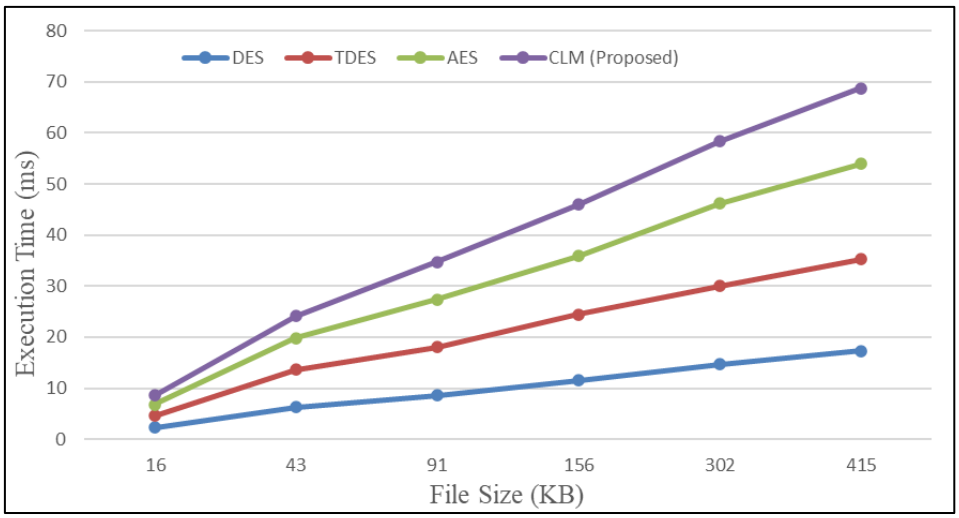

Fig. 12. Variation in execution time for various file sizes

The resilience of a system against statistical attacks is measured using a histogram. The encrypted ECG must have uniform distribution which has been represented in their histograms for an effective cryptosystem. Figure 13 (a and b) shows a sample ECG and its corresponding histogram. For quality assessment of encryption operations, histograms of encrypted signals are calculated. Figure 13 (c and d) shows the encrypted signal and its associated histogram. It is worth mentioning that the encrypted signals' histograms using suggested CLM cryptography are uniform, implying that the system is resistant to statistical attacks. While analysing two histograms, it can be visualized that the amplitudes are distributed throughout the entire range. The amplitude and range of the encrypted ECG is increased because of the new distribution. This indicates that the encrypted signal is not vulnerable to attacks.

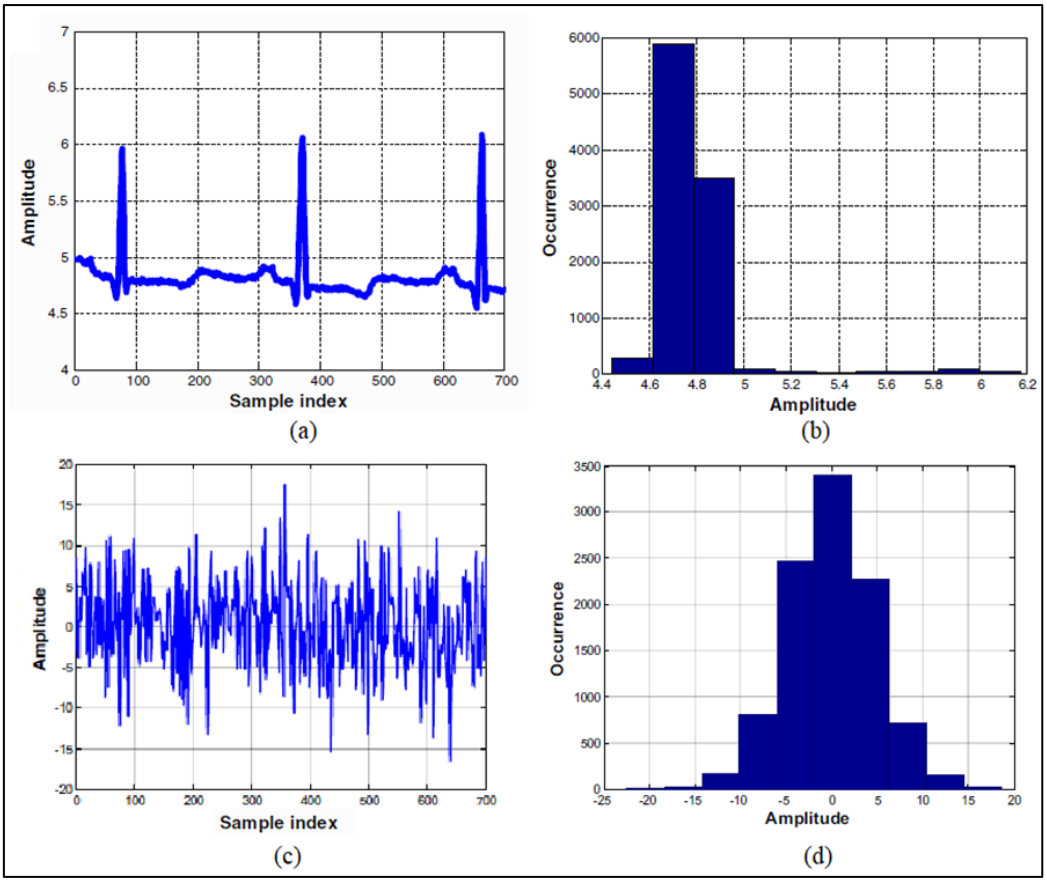

Fig. 13. Histogram Analysis (a) Original ECG input (b) Histogram of Original ECG (c) Encrypted ECG (d) Histogram of encrypted ECG

The SSIM is used to assess the original ECG signal and the encrypted ECG for resemblance. Eq. (10) is used to compute SSIM. Here μ_x is the mean of x (original) and μ_y is the mean of y (encrypted). δ_x^2 is the variance of x and δ_y^2 is the variance of y. δ_{xy} is the cross-covariance between x and y. c_1 and c_2 are small constants. SSIM indicates the resemblance of signals and it varies between 0 and 1. 0 indicate entirely different and 1 indicates exactly same.

$$SSIM = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\delta_{xy} + c_2\right)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\delta_x^2 + \delta_y^2 + c_2\right)} \tag{10}$$

It really is well understood that the encryption complexity of suggested security system is higher compared to existing algorithms. The CLM has the lowest SSIM value of 0.06. The AES cryptosystem gets an SSIM value of 0.1. The value of SSIM is 0.04 less compared to AES. There is more dissimilarity in the structure of the encrypted signal compared to the original ECG signal. The comparison of SSIM is illustrated in Figure 14. For greater encryption quality, higher value of Spectral Distortion (SD) as well as Log-Likelihood Ratio (LLR) will be obtained. The LLR is a measure that is based on the spatial distance between Linear Prediction Coefficients (LPC) vectors computed from original and encrypted signal as formulated in Eq. (11).

$$LLR = \left|\log\left[\frac{l_x R_x l_x^T}{l_y R_y l_y^T}\right]\right| \tag{11}$$

Here l_x and l_y are the LPCs for original ECG and encrypted ECG respectively. R_x represents autocorrelation matrix of input ECG and R_y represents autocorrelation matrix of encrypted ECG.

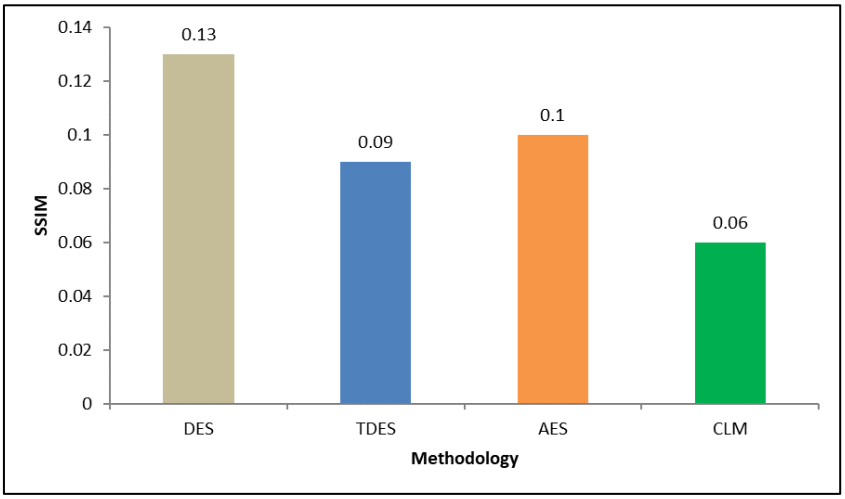

Fig. 14. Comparison of SSIM

While considering LLR, there is an increase of 0.17 as compared to normal AES. This indicates that the spatial distance between encrypted ECG and the original ECG is very high. The comparison of LLR is illustrated in Figure 15.

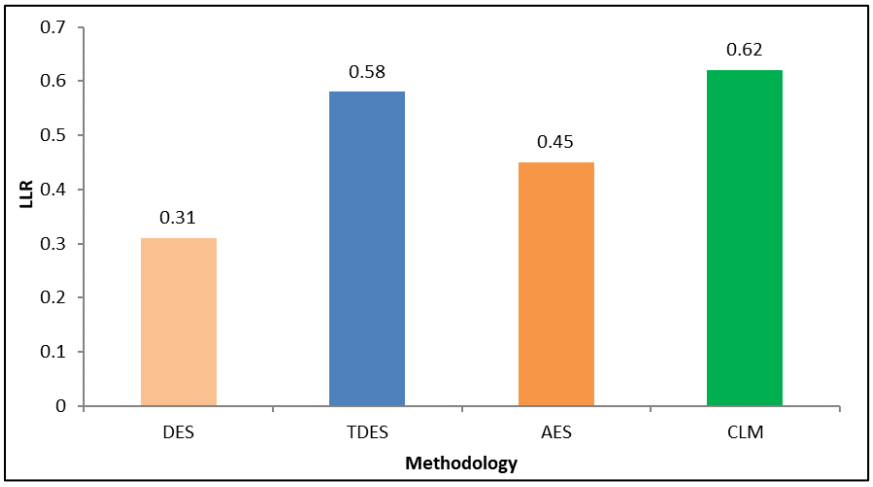

Fig. 15. Comparison of LLR

Spectral Distortion (SD) displays the distance between the spectrums of encrypted ECG and original ECG. This value is evaluated in frequency domain as given in Eq. (12).

$$SD = \frac{1}{M}\sum_{m=0}^{M-1}\sum_{i=Nm}^{Nm+N-1}\left|Q_x(i) - Q_y(i)\right| \tag{12}$$

There is a huge change of 75 in the SD value as compared to AES. This indicates large distance between the spectrums of original ECG and encrypted ECG. The comparison of SD is illustrated in Figure 16.

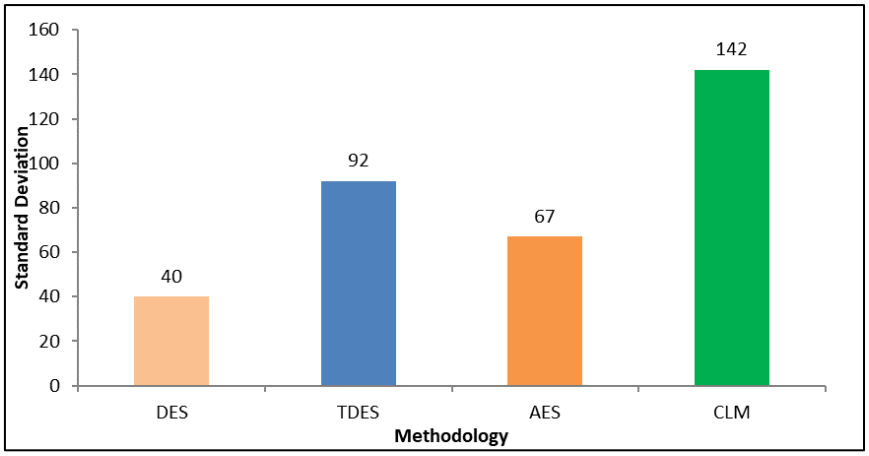

Fig. 16. Comparison of SD

Here, $Q_x(i)$ is the spectra of original ECG and $Q_y(i)$ is the spectra of encrypted ECG signal. Since it represents the largest spectral distortion, the SD of CLM is undoubtedly the best. To assess the performance of a cryptosystem, the correlation between input and resultant ECG are calculated as per Eq. (13). Here *cov*(*x,y*) is covariance, σ_x^2 and σ_y^2 are variances.

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sigma_x \sigma_y} \tag{13}$$

The value of r_{xy} is 0.035 less than that of AES. There is less relation between in the encrypted signal and the original ECG signal. This makes the encrypted signal robust against attacks. The comparison of correlation is illustrated in Figure 17. The addition of extra layers in the LM definitely improves the ECG encryption performance.

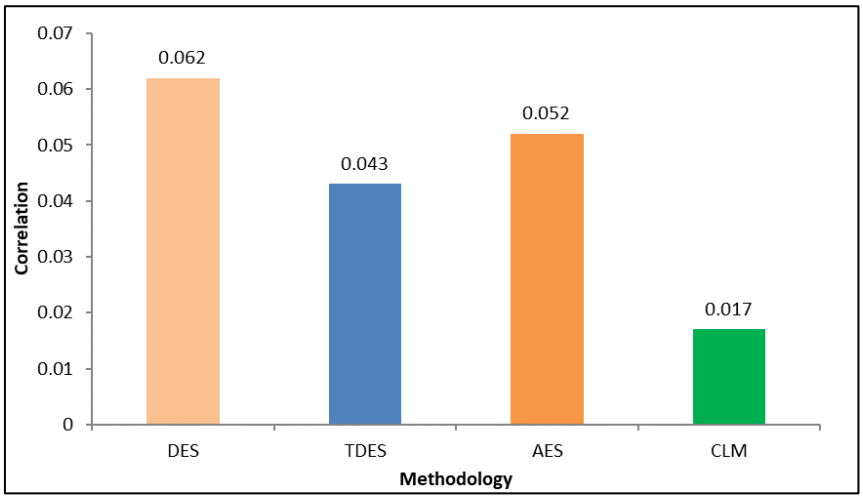

Fig. 17. Comparison of Correlation

4. Conclusions

This work described a cryptosystem for generating safe ECG signals for use in telemedicine applications. Initially, the fingerprint features were extracted and key was generated for performing CLM on ECG. The entire framework is divided into patient section and monitoring section for the operation on sample data points of ECG. The choice of CLM encryption and decryption improved the

security of ECG signal while transferring from patient unit to monitoring unit. The proposed framework is implemented on Dropbox based cloud storage and access is possible from any given locations. Computation of performance parameters such as structural similarity index matrix (SSIM), Histogram, Spectral Distortion (SD), Correlation and Log-Likelihood Ratio (LLR) indicated the efficiency of encryption algorithm over existing algorithms. According to the findings, using greater levels of encryption improves security. The proposed cryptosystems provide a very high level of security. According to the simulation outputs, the suggested cryptosystem based on additional layers has the greatest performance in terms of attack resilience. Deep learning will be utilized in the future to extract features from ECG data for diagnostic and authentication purposes.

Acknowledgement
This research was not funded by any grant.

References

[1] Baig, Mirza Mansoor, Hamid GholamHosseini, Aasia A. Moqeem, Farhaan Mirza, and Maria Lindén. "Clinical decision support systems in hospital care using ubiquitous devices: current issues and challenges." *Health informatics journal* 25, no. 3 (2019): 1091-1104. https://doi.org/10.1177/1460458217740722

[2] Zheng, Guanglou, Rajan Shankaran, Wencheng Yang, Craig Valli, Li Qiao, Mehmet A. Orgun, and Subhas Chandra Mukhopadhyay. "A critical analysis of ECG-based key distribution for securing wearable and implantable medical devices." *IEEE Sensors Journal* 19, no. 3 (2018): 1186-1198. https://doi.org/10.1109/JSEN.2018.2879929

[3] Hameed, Mustafa Emad, Masrullizam Mat Ibrahim, Nurulfajar Abd Manap, and Mothana L. Attiah. "Comparative study of several operation modes of AES algorithm for encryption ECG biomedical signal." *International Journal of Electrical and Computer Engineering* 9, no. 6 (2019): 4850. https://doi.org/10.11591/ijece.v9i6.pp4850-4859

[4] Mathivanan, P., A. Balaji Ganesh, and R. Venkatesan. "QR code–based ECG signal encryption/decryption algorithm." *Cryptologia* 43, no. 3 (2019): 233-253. https://doi.org/10.1080/01611194.2018.1549122

[5] Bhalerao, Siddharth, Irshad Ahmad Ansari, Anil Kumar, and Deepak Kumar Jain. "A reversible and multipurpose ECG data hiding technique for telemedicine applications." *Pattern Recognition Letters* 125 (2019): 463-473. https://doi.org/10.1016/j.patrec.2019.06.004

[6] McGregor, Carolyn, Jennifer Heath, and Ming Wei. "A web services based framework for the transmission of physiological data for local and remote neonatal intensive care." In *2005 IEEE International Conference on e-Technology, e-Commerce and e-Service*, pp. 496-501. IEEE, 2005. https://doi.org/10.1109/EEE.2005.25

[7] Pandey, Suraj, William Voorsluys, Sheng Niu, Ahsan Khandoker, and Rajkumar Buyya. "An autonomic cloud environment for hosting ECG data analysis services." *Future Generation Computer Systems* 28, no. 1 (2012): 147-154. https://doi.org/10.1016/j.future.2011.04.022

[8] Liu, Ting Yu, Kuan Jen Lin, and Hsi Chun Wu. "ECG data encryption then compression using singular value decomposition." *IEEE journal of biomedical and health informatics* 22, no. 3 (2017): 707-713. https://doi.org/10.1109/JBHI.2017.2698498

[9] Shaikh, Muhammad Umair, Siti Anom Ahmad, and Wan Azizun Wan Adnan. "Investigation of data encryption algorithm for secured transmission of electrocardiograph (ECG) signal." In *2018 IEEE-EMBS Conference on Biomedical Engineering and Sciences (IECBES)*, pp. 274-278. IEEE, 2018. https://doi.org/10.1109/IECBES.2018.8626640

[10] Hameed, Mustafa Emad, Masrullizam Mat Ibrahim, and Nurulfajar Abd Manap. "Compression and encryption for ECG biomedical signal in healthcare system." *TELKOMNIKA (Telecommunication Computing Electronics and Control)* 17, no. 6 (2019): 2826-2833. https://doi.org/10.12928/telkomnika.v17i6.13240

[11] Hameed, Mustafa Emad, Masrullizam Mat Ibrahim, Nurulfajar Abd Manap, and Ali A. Mohammed. "A lossless compression and encryption mechanism for remote monitoring of ECG data using Huffman coding and CBC-AES." *Future generation computer systems* 111 (2020): 829-840. https://doi.org/10.1016/j.future.2019.10.010

[12] Impiö, Mikko, Mehmet Yamaç, and Jenni Raitoharju. "Multi-level reversible encryption for ECG signals using compressive sensing." In *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 1005-1009. IEEE, 2021. https://doi.org/10.1109/ICASSP39728.2021.9414983

[13] Li, Yazhao, Yanwei Pang, Kongqiao Wang, and Xuelong Li. "Toward improving ECG biometric identification using cascaded convolutional neural networks." *Neurocomputing* 391 (2020): 83-95. https://doi.org/10.1016/j.neucom.2020.01.019

[14] Le, Ngoc Tuyen, Jing-Wein Wang, Duc Huy Le, Chih-Chiang Wang, and Tu N. Nguyen. "Fingerprint enhancement based on tensor of wavelet subbands for classification." *IEEE Access* 8 (2020): 6602-6615. https://doi.org/10.1109/ACCESS.2020.2964035

[15] Maltoni, Davide, Dario Maio, Anil K. Jain, and Salil Prabhakar. *Handbook of fingerprint recognition*. Vol. 2. London: springer, 2009. https://doi.org/10.1007/978-1-84882-254-2

[16] Pourasad, Yaghoub, Ramin Ranjbarzadeh, and Abbas Mardani. "A new algorithm for digital image encryption based on chaos theory." *Entropy* 23, no. 3 (2021): 341. https://doi.org/10.3390/e23030341

[17] Yousif, Sura F., Ali J. Abboud, and Hussein Y. Radhi. "Robust image encryption with scanning technology, the El-Gamal algorithm and chaos theory." *IEEE Access* 8 (2020): 155184-155209. https://doi.org/10.1109/ACCESS.2020.3019216

[18] Alsharman, Nesreen, Adeeb Saaidah, Omar Almomani, Ibrahim Jawarneh, and Laila Al-Qaisi. "Pattern Mathematical Model for Fingerprint Security Using Bifurcation Minutiae Extraction and Neural Network Feature Selection." *Security and Communication Networks* 2022 (2022). https://doi.org/10.1155/2022/4375232

[19] Koppanati, Rama Krishna, Krishan Kumar, and Saad Qamar. "E-MOC: an efficient secret sharing model for multimedia on cloud." In *Conference Proceedings of ICDLAIR2019*, pp. 246-260. Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-67187-7_26

[20] Xing, Wenchao, and Yilin Bei. "Medical health big data classification based on KNN classification algorithm." *IEEE Access* 8 (2019): 28808-28819. https://doi.org/10.1109/ACCESS.2019.2955754

[21] Apandi, Ziti Fariha Mohd, Ryojun Ikeura, and Soichiro Hayakawa. "Arrhythmia detection using MIT-BIH dataset: A review." In *2018 International Conference on Computational Approach in Smart Systems Design and Applications (ICASSDA)*, pp. 1-5. IEEE, 2018. https://doi.org/10.1109/ICASSDA.2018.8477620

[22] Mustafa, Wan Azani, Haniza Yazid, Mastura Jaafar, Mustaffa Zainal, Aimi Salihah Abdul-Nasir, and Noratikah Mazlan. "NAE, PSNR, ME."

[23] Nabil, Mohamed, Mohamed Helmy Megahed, and Mohamed Hassan Abdel Azeem. "Design and simulation of new one time pad (OTP) stream cipher encryption algorithm." *Journal of Advanced Research in Computing and Applications* 10, no. 1 (2018): 16-23.

[24] Rudwan, Mohammed Suleiman Mohammed, and Salah Eldin Deng Al-Jack. "Performance Analysis of Three Classical Encryption Algorithms, Simple Substitution, Caeser, and Periodic Permutation (the Three SCP) in Encrypting Database Transactions."