# Using Modified Gorti-enhanced Homomorphic Cryptosystem to Improve Security of ECG Signal

Fatma Zohra Besmi, Samia Belkacem, and Noureddine Messaoudi

*University of Boumerdes, Boumerdes, Algeria*

https://doi.org/10.26636/jtit.2025.2.2002

**Abstract — While offering vast data storage capabilities, cloud computing poses numerous security- and privacy-related challenges. This requires robust security measures, particularly for sensitive data, such as electrocardiograms (ECG). Homomorphic encryption (HE) emerges as a promising solution by enabling secure computations to be performed directly on encrypted data. This study introduces a novel approach to enhance the security of ECG data. We modified the Gorti-enhanced homomorphic cryptosystem (MEHC) method by optimizing its key generation procedure and then applied the linear congruential generator (LCG) algorithm to create a list of huge prime integers. Furthermore, we increased the modulus value and enlarged the message space. These enhancements boosted overall security by substantially improving immunity to factorization attacks. We used quantization and fixed-point representation to enhance the encryption process. As an additional security layer, an evaluation process has been added to the proposed algorithm which performs various mathematical operations homomorphically on the encrypted data, rather than on the original data. This modified algorithm enables efficient and secure encryption of ECG data while preserving the ability to reliably identify arrhythmias, such as bradycardia and tachycardia. Using the MIT-BIH arrhythmia database, the proposed MEHC system demonstrated high accuracy (98.48%), sensitivity (99.10%) and positive predictive value (99.33%), while effectively safeguarding the ECG data. These results validate the efficacy of the MEHC system and confirm its suitability for secure and reliable ECG signal processing in healthcare applications.**

***Keywords — arrhythmia detection, cryptosystem, decryption, ECG, encryption, enhanced homomorphic cryptography***

## 1. Introduction

An electrocardiogram (ECG) is an important method commonly used in medicine to track electrical changes in a patient's body linked to the beating of their heart. The signals are measured using electrodes placed on 12 standard wires (also known as channels) and applied to specific areas of the patient's chest, arms, and legs [1]. There are three basic components to an ECG signal: the P-wave, the QRS wave, and the T-wave [2]. ECG signals are studies by assessing the locations or magnitudes of PR and ST segments, QRS, PR, QT, and ST intervals, as well as additional data [3].

Comprehending these waves and intervals is essential in detecting problems affecting the cardiovascular system and assessing the overall condition of the heart. The Pan-Tompkins approach is the predominant technique for the diagnosis of ECG abnormalities [4].

Due to the fact that ECGs contain patient information, solutions (such as encryption) are required to protect patient data and maintain its quality, in order to avoid risks that lead to erroneous diagnoses or treatment plans. One of the recommended methods for encrypting ECGs is fully homomorphic encryption (FHE).

This type of encryption allows for an infinite number of operations to occur at any given moment; mixed operators can perform any number of operations on the ciphertext. FHE may be of the additive, multiplicative, or mixed variety [5]. Therefore, it offers greater security for cloud data and services.

The Gorti-enhanced homomorphic cryptosystem (EHC), introduced by Gorti and Garimella in [6], is a specific type of fully homomorphic encryption (FHE). EHC offers secure indistinguishability under a chosen ciphertext attack (IND-CCA), implying that an attacker cannot discern the keys for a selected ciphertext [7].

This scheme is characterized by better performance than previous systems, as it discovers and utilizes two distinct keys for encryption and decryption: a secret key $q$, $p$ and a public key $m$ [8]. The security of the scheme relies on the difficulty of factoring the large number $m$ (at least 1024, preferably 2048 bits), and the random number $r$ adds an additional layer of security, making it harder to deduce the original message.

This research introduces a novel approach to enhancing the security of ECG signals in healthcare applications. Initially, the Pan-Tompkins approach is used to examine and process an electrocardiogram (ECG) signal in order to identify the QRS complex. This method provides strong detection performance when used with precise clinical ECG signal data. However, ECG recordings made at outpatient clinics, low quality of the signals and the noise present limit the ability of this algorithm to identify QRS complexes [9].

To address this limitation, we increase the bandpass filter's upper cutoff frequency to 25 Hz (resulting in a 5 – 25 Hz passband), removing noise while retaining significant signal components. To improve the efficiency of the encryption

process, signal (X6) is initially converted to an integer representation using a fixed-point representation. Subsequently, quantization is applied to the integer values, optimizing the data representation without sacrificing signal fidelity.

The resulting quantized signal is encrypted using the proposed MEHC algorithm which employs a robust key generation mechanism combining a linear congruential generator (LCG) and the Miller-Rabin primality test [10], where the sender applies the newly generated secret key $p$, $q$, $Q$ to encrypt the ECG data. A key feature of this approach is the enabling of secure homomorphic operations, facilitated by a deterministic evaluation key derived via SHA-256 hashing of the secret key. This allows direct computation on the encrypted data through a linear polynomial function, a core characteristic of FHE.

After the encrypted evaluation is complete, the signal is decrypted using public key $g$. This ensures that the transmitted ECG data remains private and is protected against unauthorized access. The signal is re-quantized and converted back to its original floating-point representation after decryption, thereby preparing it for subsequent analysis and classification.

The proposed method improves robustness against factorization attacks, contributing to improved efficiency, reliability, and analysis of the transmitted ECG signal.

This study is structured as follows. Section 2 reviews related work, whereas Section 3 provides an in-depth description of the proposed algorithm. Section 4 analyzes the experimental findings and compares them with previous work, and Section 5 concludes the article.

## 2. Related Works

Before discussing the proposed approach, it is imperative that we first review the current methods used to protect the ECG signal. This section highlights relevant encryption techniques that allow calculations to be performed on encrypted data while maintaining secrecy, and discusses the strengths and limitations of these methods to provide context for our contributions.

To guarantee the security of medical data during their transmission, the authors of [11] suggest an encryption method for ECG signals based on the partial homomorphic encryption technique (PHE). To encrypt the signals, the study combines the Pan-Tompkins algorithms for QRS complex detection with the PHE-RSA method. This approach can detect cardiac abnormalities and calculating the heart rate while protecting sensitive data from unauthorized access.

The study was carried out using MIT-BIH arrhythmia data. Of 20 recordings, the results indicate that 18 of them had the same outcome. the method achieved a 90% accuracy rate and was quick, demonstrating its effectiveness in securing ECG signals. However, while focusing on enhanced security, the study lacks a deeper exploration of potential vulnerabilities or attack scenarios, which is crucial to understanding the system's robustness.

In article [12] a new system based on fully homomorphic encryption (FHE) methods was proposed. The strength of this approach lies in its ability to achieve a high sensitivity of 92.59% and a positive predictive accuracy of 90% for detecting arrhythmias, while simultaneously maintaining data privacy. This method faces some limitations, including computational complexity, in addition to a lack of detailed comparison with other FHE schemes, which makes it difficult to evaluate the advantages and disadvantages of the proposed approach. Addressing these limitations is critical to realize the full potential in secure healthcare data sharing.

In [13], a new fully homomorphic encryption algorithm with an advanced encryption standard (FHEAES) was introduced to encode electrocardiogram (ECG) signals for improved security and data privacy. The ECG measurements were processed using the Pan-Tompkins algorithms, followed by encoding using the FHEAES algorithm. The proposed algorithm integrates an evaluation process as an additional security layer, enabling mathematical operations to be performed on encrypted data without decryption.

The algorithm was evaluated using various ECG signals obtained from the MIT-BIH database and demonstrated a 95.8% accuracy rate in classifying heart rates and 100% accuracy in decryption, highlighting the effectiveness of homomorphic encryption in securing ECG signals. In general, while FHEAES offers robust security and privacy features, its computational complexity and key management requirements present challenges that need to be addressed for optimal implementation in real-world applications.

Paper [14] presents a new approach to secure transmission of ECG signals over the Internet by combining set partitioning in hierarchical trees (SPHIT) with RSA encryption. The approach aims to address bandwidth and security issues related to the transmission of sensitive medical data while maintaining the quality of the ECG signal. The use of RSA encryption provides a strong foundation for protecting confidentiality of patient data and ensuring secure communication. However, it is not appropriate for large signals or for real time use. Instead, the FHE encryption algorithm is capable of performing simultaneous addition and multiplication operations, thus adding further security to the signal.

The authors of [15] tested the feasibility of analyzing ECG data in the cloud using FHE, aiming to secure patient privacy while enabling remote healthcare services. The suggested technique is based on Gentry's FHE and BGV techniques. The findings indicate that while FHE is promising, it suffers from major performance constraints, especially since decryption time dominates addition operations and every bit of encryption necessitates a large amount of storage.

These limitations, as exemplified by the 800 000-fold increase in storage space needed by Gentry's FHE scheme for one hour of patient data, highlight the need for further exploration of alternative secure computation methods that are capable of balancing security with practical efficiency for real-world healthcare applications.

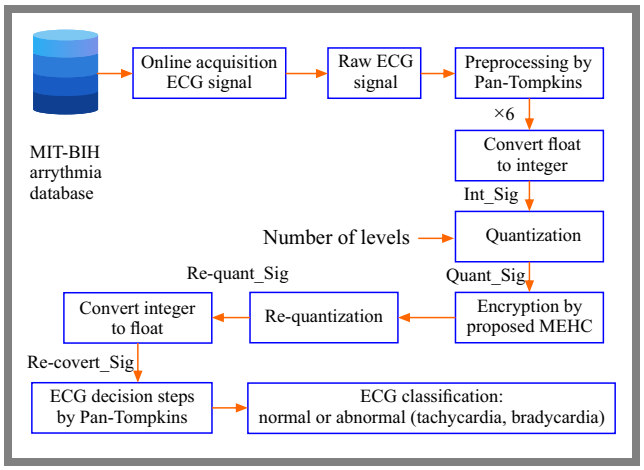


**Fig. 1.** Flow chart of the proposed approach.

# 3. Proposed Method

This research is divided into four steps: preprocessing, encryption, decision-making, and classification. Initially, the Pan-Tompkins technique was used for signal pre-processing. Subsequently, the signal (X6) was transformed into an integer representation and quantized to enhance the representation of the data while preserving signal fidelity.

In the second part, the proposed MEHC algorithm was used to encrypt the ECG signal, which improves security and makes it more difficult for attackers to gain access. Subsequently to decryption, the signal underwent re-quantization and was restored to its original format. In the decision-making stage, this resulting signal was analyzed to detect QRS complexes, a prominent feature in ECG assessments.

The characteristics of these features are used to calculate the heart rate, which is then classified. This ensures the privacy and integrity of sensitive medical information, improving the efficiency and reliability of ECG signal transmission and analysis.

Figure 1 shows the methodology of this study presented in the form of a flowchart. We use raw ECG data from the MIT-BIH database [16]. Details regarding the specific dataset used are provided in Subsection 4.1.

## *3.1. Preprocessing Signal*

The pre-processing stage (Fig. 2) involved several steps to prepare the ECG signal for subsequent encryption and analysis. The Pan-Tompkins algorithm was applied for initial detection of the QRS complex [17]. To improve the algorithm's robustness against noise and low-quality signals, we increased the bandpass filter's upper cutoff frequency to 25 Hz. This specific bandpass was chosen to ensure effective noise removal while preserving critical signal components, thus striking a necessary balance for reliable QRS detection under various recording conditions.

The processing of the ECG signal within this methodology is conducted in the following manner: the raw ECG signal (X1) is subjected to a bandpass filter, comprising a low pass (X2) and a high-pass (X3) stage, with a passband of 5 – 25 Hz.

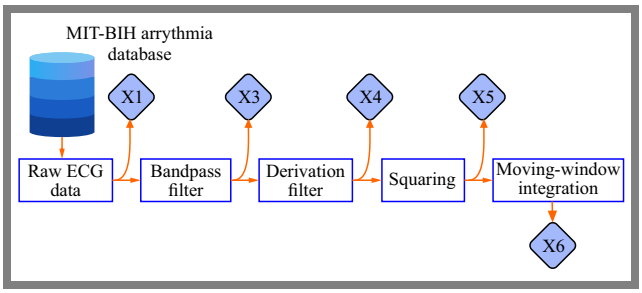


**Fig. 2.** Preprocessing ECG signal diagram.

Following the bandpass filter (X3), the signal-to-noise ratio is improved, consequently enhancing the overall sensitivity of the detector. Subsequently, the filtered signal undergoes a series of transformations, including differentiation (X4), a squaring function (X5), and integration of the moving window (X6).

## *3.2. Fixed-point Representation and Quantization*

After receiving the output of the moving window coordinates (X6), a two-step transformation (fixed-point representation and quantization) is performed to optimize it for the encryption process. By adopting these transformations, the system can efficiently manage the data without sacrificing its integrity.

It is a technique used to represent floating-point numbers using integers [18]. In this study, the signal (X6) is transformed into a discrete integer representation using a scaling factor. This requires selecting appropriate scale factors for each data point based on its magnitude. By scaling the values, we can preserve precision while decreasing the number of bits necessary for representation.

Once the relevant scale factors are determined, each floating-point value in the (X6) signal is multiplied by its corresponding scale factor and rounded to the nearest integer. This results in an integer signal (Int_Sig) that precisely describes the (X6) signal.

To further optimize data representation, quantization is performed for integer values. This approach attempts to enhance the retention of essential signal properties while lowering distortion, thereby boosting performance of subsequent analytical tasks [19]. This technique is widely applied in audio and voice compression, image processing, and biological signal analysis, particularly in ECG signal evaluation. The following formulae were applied to determine the signal after quantization (Quant_Sig) [20]:

$$Y_i = \left\{ \frac{X_i - X_{min}}{X_{max} - X_{min}} \right\} \times 2^{n-1} , \tag{1}$$

where $Y_i$ and $X_i$ represent the $i$-th sample in quantized array $Y$ and original signal $X$. $X_{max}$ and $X_{min}$ represent the maximum and minimum values of signal $X$ (here the original signal is Int_Sig).

Following acquisition of the quantization signal (Quant_Sig), encryption is performed using the proposed MEHC system.

### *3.3. Modified Enhanced Homomorphic Cryptosystem (MEHC)*

Based on the Gorti-enhanced homomorphic cryptosystem (EHC), we incorporate a modified MEHC scheme. This fully homomorphic public-key encryption scheme utilizes a pair of public and private keys.

Key modifications implemented to enhance security include using a larger modulus value (related to public key $g$), which strengthens immunity to factorization attacks, and incorporating a prime number $Q$ into the secret key to enlarge the message space. The robust key generation process integrates the Miller-Rabin primality test and the linear congruential generator. This modified scheme ensures data privacy by executing various computational operations (addition and multiplication) on the ciphertext without necessitating decryption, enabled by a deterministic evaluation key derived via SHA-256 hashing of the secret key. These changes aim to improve the performance and enhance security, making it particularly beneficial for applications demanding enhanced data privacy and security.

The approaches used in this study are presented below.

The most common approach for obtaining random numbers is a technique known as the linear congruential generator (LCG). We utilized it to create a massive list of odd integers for a subsequent primality test [21].

$$X_{n+1} = (aX_n + C) \mod m \ , \ n \in \mathbb{Z}^+ \ . \tag{2}$$

The seed value of the series is $X_0$, while the multiplier is $a$, the increment is $C$, the created modulus is $m$, and the random numbers are denoted by $X_n$. The quality of the generated sequence depends heavily on the choice of $a$, $C$, and $m$ parameters. To ensure a long period and good statistical properties, the following conditions should be met:

$$gcd(C, m) = 1 \ , \tag{3}$$

$$a \equiv 1 \mod p \quad \text{for every prime } p \text{ dividing } m \ , \tag{4}$$

$$a \equiv 1 \mod 4 \quad \text{if } m \text{ is a multiple of 4} \ . \tag{5}$$

With $m = 2^k$; $a = 4b - 1$; $C$ as an odd number ($b$; $k > 0$). A satisfactory result can be obtained by setting the increment $C$ to zero [22].

The Miller-Rabin primality-testing algorithm is a primality test that assesses if a specific number is likely to be prime. This test is based on Fermat's little theorem [10].

The proposed MEHC algorithm consists of four processes, as described below.

The proposed algorithm generates three keys: public key $pk$, private key $sk$, and evaluation key $ek$. The algorithm follows the following steps to create these keys:

1) Generate two large prime numbers $p$ and $q$ using LCG, such that $p > q$. The primality of these numbers is verified using the Miller-Rabin test.
2) Calculate modulus $m = p \times q$
3) Calculate $g = m^2 + 1$

**Algorithm 1** Miller-Rabin primality test to verify the primality of an odd number $n$

```
Find integers r and m such that n − 1 = 2 r × m
Choose randomly any integer a ∈ [1, n − 1]
Compute: b_0 = a^m mod n
Compute b_i, k times b_i = b_i − 1
The result must b_e = ±1
if the result is 1 then
    n is a composite number
end if
if the result is –1 then
    n is a prime number
end if
```

4) Select a prime number $Q$ that satisfies the condition $Q|_2^p|\_$. The primality of this number is verified by the Miller-Rabin test.

Based on these generated values, the keys are defined as follows:

- Public key $g$. This value is designed to obscure the original value $m$.
- Private key $p$, $q$, $Q$.
- Evaluation key $ek$ is derived by computing the SHA-256 hash of the combined parameters $p$, $q$, and $Q$, and then reducing the resulting hash value modulo $g$.

The encryption procedure takes the quantized ECG signal (Quant_Sig) as input and generates the corresponding ciphertext $C$. This process utilizes scheme parameters $Q$ and $g$, along with a random vector $r$ for probabilistic security. The encryption is calculated using the following formula:

$$C = (Quant\_Sig + r \times Q + r \times g) \mod g \ . \tag{6}$$

The evaluation process receives ciphertexts $C$ that originate from the encryption process as input and creates new ciphertexts $C'$ as output, which will be termed evaluated ciphertexts. An assessment procedure is performed on the server side before decryption. This fundamental procedure was suggested to be added to the MEHC algorithm in order to accomplish homomorphic encryption. It conducts mathematical operations homomorphically on the ciphertext.

Our approach converts the generic evaluation function $f$ into a linear polynomial. This decision is driven by the simplicity of linear polynomials, which improves performance, as well as its ability to provide better security. A linear polynomial is characterized by constant real values and has a degree of one [23]. The suggested evaluation function generates evaluated ciphertexts $C'$ using three parameters: random integer $N$, evaluation key $ek$ and new modulo $g$. The following formula represents the procedure:

$$(C') \leftarrow Eval_{N,ek,g}(f, C) \ , \tag{7}$$

$$C' = (N \times C + ek) \mod g \ . \tag{8}$$

$N$ was chosen in the MEHC algorithm to be a variable number rather than a constant number to increase the level of security by making it more difficult to hack or break. Such a higher

degree of protection results from the fact that the variable number itself costs the hacker or third party. Before putting it in the encryption equation, the user must first ascertain whether the integer is variable or not.

This requires an additional effort to crack the encryption.

The proposed algorithm is fully homomorphic, which implies that it can handle both multiplicative and additive homomorphic properties, as demonstrated in Eq. (8). The correct decoding of the ciphertext is essential for the success of homomorphic encryption.

The decryption process involves using the inverse of the evaluation function (a linear polynomial function) followed by the MEHC decryption algorithm with the secret key to recover the plaintext from the ciphertext in the following manner:

$$C = \left((C' - ek) \times N^{-1}\right) \mod g\,, \tag{9}$$

$$Dec\_Sig = C \mod Q\,. \tag{10}$$

### 3.4. Decision Making

Once decrypted, the signal is converted back to its original floating-point representation, preparing it for this decision phase. This step involves labeling signal peaks as QRS complexes by applying several thresholds, distinguishing them from noise peaks, which may include muscle noise and T waves. Figure 3 presents a diagram that illustrates the decision-making phase. To be identified as a QRS complex, a peak must be recognized as such a complex in both the decrypted signal and the bandpass-filtered waveforms. Specifically, the following threshold values were used [24]:

$$SPK = 0.125 \times Peak + 0.875 \times SPK\,, \tag{11}$$

$$NPK = 0.125 \times Peak + 0.875 \times NPK\,, \tag{12}$$

$$Threshold\,1 = NPK + 0.125 \times (SPK - NPK)\,, \tag{13}$$

$$Threshold\,2 = 0.5 \times Threshold\,1\,. \tag{14}$$

SPK and NPK are the peak values of the running estimates of the signal and noise, respectively. Value threshold 2 is used only if threshold 1 fails to find a QRS complex within a certain distance from the detected one.

The thresholds were automatically changed to adapt to changes in QRS shape and heart rate. Once the QRS complex is detected, the $R$ position is specified, leading to the RR interval, and computing the heart rate (HR) according to the equation [21].

$$HR = \frac{\text{Number of } R \text{ peaks}}{\text{Time of ECG signal [s]}} \times 60\,. \tag{15}$$

The heart rate was classified as normal or abnormal HR. Normal heart rate varies from 60 to 100 bpm, but irregular heartbeats indicate arrhythmia (either bradycardia or tachycardia), which helps the physician to make the appropriate

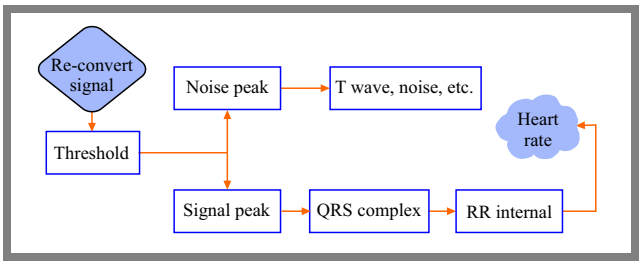


**Fig. 3.** Diagram of the decision-making phase.

inference. It also helps the analyst to perform further analysis and detection-related steps.

### 3.5. Parameter Estimation

The reference annotation and the WFDB toolbox provided by the Python suite were used for this evaluation [15]. Several values are introduced to assess the effectiveness of the presented algorithm, including:

- True positive (TP) – correctly identified QRS complexes.
- False positive (FP) – peaks incorrectly identified as QRS complexes.
- False negative (FN) – missed QRS complexes.
- True negative (TN) – peaks correctly identified non-QRS peaks.

Performance of the algorithm is evaluated by calculating its accuracy, sensitivity, positive prediction, and detection error rate, with all of the aforementioned terms defined as follows.

- Accuracy (Acc) assesses the algorithm's overall correctness in identifying both QRS complexes and non-QRS peaks.

$$Acc = \frac{TP + TN}{\text{Total beats}} \times 100\,[\%]\,. \tag{16}$$

- Sensitivity (Se) is its ability to accurately identified QRS:

$$Se = \frac{TP}{TP + FN} \times 100\,[\%]\,. \tag{17}$$

- Positive prediction represents the probability of QRS identified among the true QRS.

$$+P = \frac{TP}{TP + FP} \times 100\,[\%]\,. \tag{18}$$

- Detection error rate (DER) is a measure that indicates the overall error rate of the algorithm.

$$DER = \frac{FP + FN}{\text{Total beats}} \times 100\,[\%]\,. \tag{19}$$

## 4. Results and Discussion

This section presents the results obtained by applying the proposed MEHC scheme to process ECG signal in a secure manner. We detail the results achieved at various stages of our approach – from preprocessing, to encryption and secure classification of the decrypted signal. The effectiveness of the encryption method and the overall effectiveness in identifying cardiac abnormalities are evaluated using various indicators.

The ECG signals were obtained from the MIT-BIH arrhythmia database containing 48 heartbeat signal recordings, with

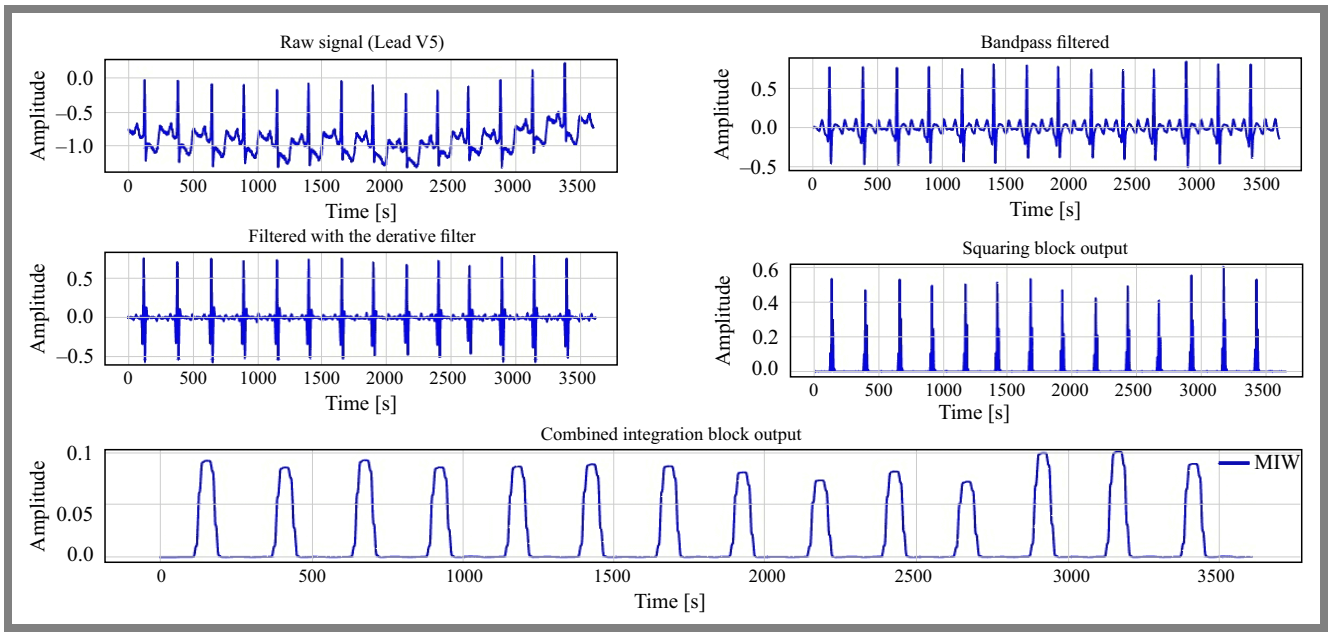


**Fig. 4.** ECG processing results involving record no. 112.

a sampling rate of 360 Hz. In each recording, the first channel represents the modified lead II (MLII), while the subsequent channel is designated as one of the leads v1, v2, v4, or v5, depending on a specific recording. Given that MLII is consistently present in all recordings and demonstrates great accuracy [25], we used MLII data for this investigation.

### *4.1. Pre-processing Signal*

This stage consists of two main processes: data acquisition and pre-processing. Figure 4 shows the procedures used in processing record no. 112. To remove the noise and existing artifacts, bandpass filtering was employed. The following phase involved the use of differentiation to determine the high slope to differentiate QRS complexes from other ECG waves. To make all the data positive and highlight the higher frequencies of the signal, the sample was first squared gradually. After this square, the waveform passed through the moving window integrator.

### *4.2. Encryption/Decryption Process*

To prepare the ECG signal for encryption, a two-step transformation procedure is applied. First, the signal is transformed into an integer representation using fixed-point arithmetic. This involves scaling the signal values to make sure that they fit within a certain integer range. Subsequently, adaptive quantization is performed on the scaled integer values, dividing the signal range into 256 discrete levels to maximize the representation of data.

Following quantization, the ECG signal is encrypted using the proposed MEHC scheme. The scheme relies on parameters derived from two large 512-bit prime numbers $p$ and $q$, so the public key component $g$ is approximately 2048 bits. The substantial size of these parameters, particularly of $g$, contributes significantly to the security of the scheme. Figure 5

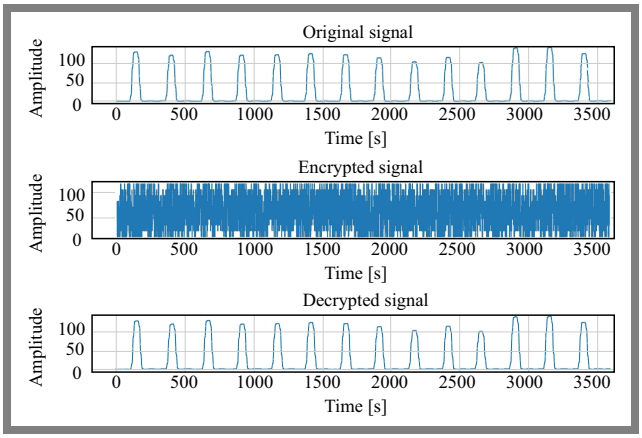


**Fig. 5.** ECG encryption/decryption results (record no. 112)

illustrates the signal at different stages, including the preprocessed signal (X6) and the resulting encrypted and decrypted signals after applying the MEHC scheme.

We noticed that the original signal is completely different from the encrypted signal. Nevertheless, upon decryption, we acquire a signal that is identical to the original signal. This observation highlights the effectiveness of the encryption process in protecting data while maintaining its integrity. To complement this visual assessment and further validate security against statistical attacks, we performed a detailed analysis.

### *4.3. Analysis of Statistical Attacks*

Using signal diffusion in the encrypted signal, intruders attempt to anticipate the original signal and secret keys in a statistical attack. The histogram, the correlation coefficient, and the mean square error (MSE) are analyzed for verification of the statistical attack. To evaluate the effectiveness of the encryption scheme in preventing statistical attacks, we ana-

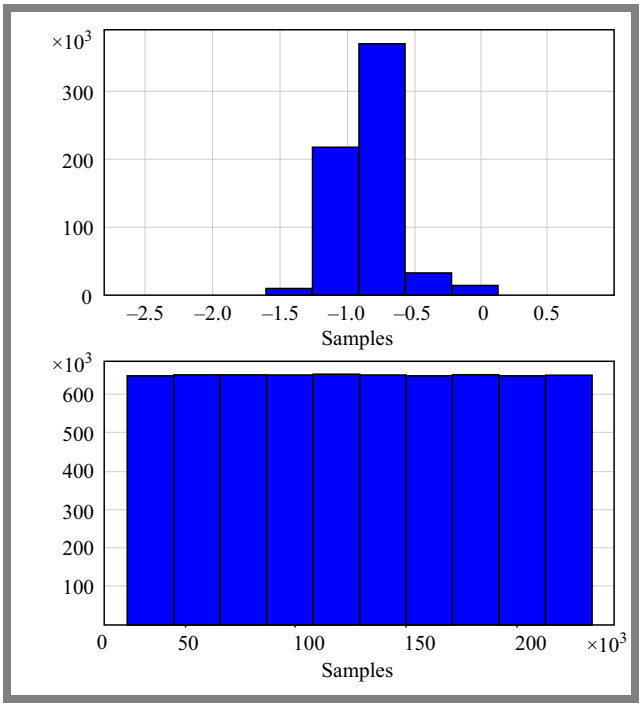


**Fig. 6.** Analysis of original and encrypted signal of sample no. 112.

lyzed the histogram of the encrypted signal. A well-encrypted signal should exhibit a uniform distribution that resembles random noise.

Figure 6 clearly demonstrates that the proposed approach meets this criterion. The histogram of the encrypted ECG signal is significantly different from that of the original signal and displays a uniform distribution. This indicates that the encrypted signal is statistically indistinguishable from random noise, making it resistant to statistical attacks.

The correlation coefficient is a statistical metric that assesses the degree and direction of the linear association between two variables. In cryptography, it can be used to evaluate the security of an encryption algorithm and its ability to fend off statistical attacks.

A correlation value of –1 signifies a perfect negative linear connection, 1 signifies a perfect positive linear relationship, and 0 signifies the absence of a linear link.

We assessed the security of the proposed encryption scheme by calculating the correlation coefficients between the original and encrypted ECG signals. We analyzed all possible column and row pairings involving raw and encrypted ECG data [26]. The findings shown in Tab. 1 indicate that the correlation coefficients between the raw and encrypted signals are markedly low. This means that the encrypted signal is considerably different from the original signal, making it very resistant to statistical attacks. Consequently, the proposed technique is successful in ensuring the security and confidentiality of ECG data.

Mean squared error (MSE) was used to measure the distortion induced by encryption, homomorphic evaluation, and decryption stages [13]. The MEHC method produced a surprisingly low average MSE of roughly $3.43 \cdot 10^{-8}$. This tiny amount of error is a critical result, indicating that calculations performed fully inside the encrypted domain generate only minor numerical errors. Such a high degree of signal fidelity after decryption is a therapeutic need. It guarantees that crucial ECG properties, including the exact amplitudes and durations of the P waves, QRS complexes, and T waves, as well as the critical PR, QRS, and QT intervals, are retained. This preservation directly affects the accuracy of automated arrhythmia detection systems and the reliability of future clinical interpretation. Therefore, the proposed MEHC scheme efficiently reconciles the need for robust data security in cloud-based ECG processing with the need to preserve high signal quality that is necessary for accurate and reliable medical diagnosis.

### *4.4. Decision Making*

After decryption, the ECG signal undergoes dequantization followed by conversion to its original floating-point form. The QRS complex identification process is then performed on the restored signal. Figure 7 illustrates the QRS complexes on a filtered ECG signal. The QRS complexes are marked by purple circles. The graph includes a background noise level

**Tab. 1.** Results of the correlation coefficients of encrypted signals.

| Record no. | Correlation coefficient | Record no. | Correlation coefficient |
|---|---|---|---|
| 100 | 0.001151854 | 201 | 0.000885001 |
| 101 | –0.000578912 | 202 | 0.000250119 |
| 102 | –0.000669556 | 203 | 0000482145 |
| 103 | 0.001295191 | 205 | 0.000742561 |
| 104 | 0.001038385 | 207 | 0.001767004 |
| 105 | 0.000953979 | 208 | –0.001236361 |
| 106 | 0.000304367 | 209 | 0.00297388 |
| 107 | 0.000532022 | 210 | 0.000755799 |
| 108 | 0.0000125535 | 212 | 0.000441197 |
| 109 | 0.003018805 | 213 | 0.000711752 |
| 111 | 0.001969152 | 214 | 0.000676252 |
| 112 | –0.001360556 | 215 | 0.000885888 |
| 113 | 0.001442974 | 217 | 0.002380301 |
| 114 | 0.000284177 | 219 | 0.00088243 |
| 115 | –0.000108819 | 220 | 0.000449283 |
| 116 | 0.002244413 | 221 | –0.000336268 |
| 117 | –0.000393281 | 222 | 0.000473388 |
| 118 | 0.002158905 | 223 | 0.001647422 |
| 119 | 0.00126128 | 228 | 0.003093744 |
| 121 | 0.00087087 | 230 | –0.000017272 |
| 122 | 0.002106787 | 231 | 0.002384566 |
| 123 | 0.001947021 | 232 | 0.001998768 |
| 124 | –0.000769574 | 233 | 0.000740326 |
| 200 | 0.000891936 | 234 | 0.001472958 |

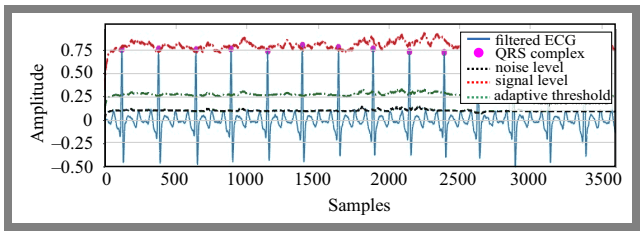


**Fig. 7.** Decision-making results (record no. 112).

line (black), a signal level line (red), and a dashed green line showing the adaptive threshold used to detect QRS complexes.

### *4.5. Heart Rate and Classification*

Table 2 highlights the analysis of heart rate results after using the MEHC algorithm. The 48 records were taken from the MIT-BIH arrhythmia database. We classified the results as normal or abnormal after comparing data collected after decryption with the heart rate range obtained from the database.

Our findings revealed that once the ECG signal was decrypted using the proposed method, 46 of 48 samples in the MIT-BIH database were classified correctly. For records 210 and 217, the results obtained were classified incorrectly because they contained significant amounts of noise. This suggests that the algorithm is mostly resilient and is capable of effectively classifying almost all samples despite the presence of noise in a couple of instances. Consequently, it underscores the possibility of practical implementation in real-world scenarios.

### *4.6. Performance Comparison*

To test the efficacy of the proposed system, we assessed each ECG sample in the MIT-BIH database using four essential metrics: accuracy, sensitivity, positive predictive value and detection error rate. The average values of these measures were calculated and compared with the findings of previous investigations, as shown in Tab. 3.

The results show competitive performance of the proposed solution when various metrics are compared with other ECG record encryption methods, demonstrating the effectiveness of the MEHC approach. Our method consistently achieves the highest levels of accuracy on various record counts, indicating reliable data preservation. We also obtained high rates of sensitivity, demonstrating the technique's decent efficacy in accurately detecting genuine positive instances of arrhythmia. Moreover, the proposed approach correctly classifies a vast majority of positive instances, as evidenced by the positive predictive values.

Moreover, the method boasts the lowest detection error rate (DER) among all studied approaches, demonstrating its exceptional stability and dependability.

## 5. Conclusions

The primary goal of signal security is to protect against unauthorized access, as well as tampering, disruption, alteration, and destruction of ECG signals. In this study, an altered ver-

**Tab. 2.** Heart rate results (in bpm) with classification.

| Record | Heart rate range | HR after using MEHC | Classification | |
|---|---|---|---|---|
| 100 | 70 – 89 | 75.5003 | Normal | ✓ |
| 101 | 55 – 79 | 62.0751 | Normal | ✓ |
| 102 | 72 – 78 | 72.6757 | Normal | ✓ |
| 103 | 62 – 92 | 69.2197 | Normal | ✓ |
| 104 | 69 – 82 | 71.6787 | Normal | ✓ |
| 105 | 78 – 102 | 86.1342 | Normal | ✓ |
| 106 | 49 – 87 | 65.7969 | Normal | ✓ |
| 107 | 68 – 82 | 70.5157 | Normal | ✓ |
| 108 | 44 – 78 | 64.9329 | Normal | ✓ |
| 109 | 77 – 101 | 83.9742 | Normal | ✓ |
| 111 | 64 – 82 | 70.5489 | Normal | ✓ |
| 112 | 74 – 91 | 84.3729 | Normal | ✓ |
| 113 | 48 – 87 | 59.616 | Bradycardia | ✓ |
| 114 | 51 – 82 | 59.4498 | Bradycardia | ✓ |
| 115 | 50 – 84 | 64.8997 | Normal | ✓ |
| 116 | 74 – 86 | 79.488 | Normal | ✓ |
| 117 | 48 – 66 | 51.0092 | Bradycardia | ✓ |
| 118 | 54 – 91 | 75.7329 | Normal | ✓ |
| 119 | 61 – 84 | 66.0295 | Normal | ✓ |
| 121 | 55 – 83 | 61.8757 | Normal | ✓ |
| 122 | 67 – 97 | 82.2794 | Normal | ✓ |
| 123 | 41 – 65 | 50.3446 | Bradycardia | ✓ |
| 124 | 47 – 64 | 53.4683 | Bradycardia | ✓ |
| 200 | 69 – 111 | 86.6658 | Normal | ✓ |
| 201 | 31 – 61 | 63.6702 | Normal | ✓ |
| 202 | 49 – 69 | 70.7483 | Normal | ✓ |
| 203 | 63 – 173 | 96.8345 | Normal | ✓ |
| 205 | 80 – 99 | 88.1612 | Normal | ✓ |
| 207 | 57 – 90 | 72.3434 | Normal | ✓ |
| 208 | 91 – 134 | 94.8738 | Normal | ✓ |
| 209 | 82 – 116 | 99.8585 | Normal | ✓ |
| 210 | 63 – 158 | 85.1372 | Normal | × |
| 212 | 63 – 108 | 91.3182 | Normal | ✓ |
| 213 | 101 – 113 | 107.4683 | Tachycardia | ✓ |
| 214 | 49 – 92 | 74.9354 | Normal | ✓ |
| 215 | 81 – 215 | 111.6222 | Tachycardia | ✓ |
| 217 | 69 – 103 | 73.2074 | Normal | × |
| 219 | 38 – 75 | 71.5126 | Normal | ✓ |
| 220 | 58 – 74 | 68.0566 | Normal | ✓ |
| 221 | 47 – 110 | 79.1225 | Normal | ✓ |
| 222 | 49 – 84 | 82.5785 | Normal | ✓ |
| 223 | 75 – 94 | 86.4 | Normal | ✓ |
| 228 | 54 – 80 | 69.6517 | Normal | ✓ |
| 230 | 63 – 99 | 74.9686 | Normal | ✓ |
| 231 | 49 – 69 | 52.2055 | Bradycardia | ✓ |
| 232 | 24 – 28 | 59.3169 | Bradycardia | ✓ |
| 233 | 98 – 110 | 102.0517 | Tachycardia | ✓ |
| 234 | 84 – 99 | 91.3514 | Normal | ✓ |

**Tab. 3.** Comparison with other studies.

| Method | Software | Record | Same record | Acc [%] | Se [%] | +P [%] | DER [%] |
|---|---|---|---|---|---|---|---|
| RSA [9] | Matlab R2019a | 20 | 18 | 90 | NR | NR | NR |
| Our study | Python | 20 | 19 | 99.11 | 99.19 | 99.9 | 0.89 |
| Gentry FHE [10] | Matlab R2019a | 27 | 25 | NR | 92.59 | 90 | 14.8 |
| Our study | Python | 27 | 26 | 98.58 | 98.89 | 99.45 | 1.65 |
| FHEAES [11] | Matlab R2018b | 48 | 46 | 95.8 | NR | NR | NR |
| Our study | Python | 48 | 46 | 98.48 | 99.10 | 99.33 | 1.52 |

sion of the EHC technique is used to build a secure ECG signal encryption system.

The effectiveness of the designed cryptosystem was assessed with the use of various signals taken from the MIT-BIH arrhythmia database.

Heart rate was calculated after using MEHC and classified as normal or abnormal, helping to diagnose arrhythmias, such as bradycardia and tachycardia. When compared with results from the original database, the suggested MEHC technique achieves a 98.48% degree of accuracy, a 99.10% sensitivity rate and a 99.33% positive prediction rate.

Furthermore, MEHC is considered a successful homomorphic encryption method, since it correctly decodes the encrypted data. This ensures the algorithm's suitability and clarity. It also guarantees a high degree of security and privacy in practical applications, such as encryption and decryption of signal data.

## Acknowledgments

This study was supported by the Algerian Ministry of Higher Education and Scientific Research through funding for the PRFU Project.

## References

[1] V.J. Naveen, K.M. Krishna, and K.R. Rajeswari, "Noise Reduction in ECG Signals for Bio-telemetry", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, pp. 505–511, 2019 (https://doi.org/10.11591/ijece.v9i1.pp505-511).

[2] M.A. Hashim, Y.W. Hau, and R. Baktheri, "Efficient QRS Complex Detection Algorithm Implementation on SOC-based Embedded System", *Jurnal Teknologi*, vol. 78, pp. 49–58, 2016 (https://doi.org/10.11113/jt.v78.9450).

[3] K.K. Patro and P.R. Kumar, "Effective Feature Extraction of ECG for Biometric Application", *Procedia Computer Science*, vol. 155, pp. 296–306, 2017 (https://doi.org/10.1016/j.procs.2017.09.138).

[4] H. Xiong, M. Liang, and J. Liu, "A Real-time QRS Detection Algorithm Based on Energy Segmentation for Exercise Electrocardiogram", *Circuits, Systems, and Signal Processing*, vol. 40, pp. 4969–4985, 2021 (https://doi.org/10.1007/s00034-021-01702-z).

[5] P. Dhiman *et al.*, "Secure Token-key Implications in an Enterprise Multi-tenancy Environment Using BGV-EHC Hybrid Homomorphic Encryption", *Electronics*, vol. 11, art. no. 1942, 2022 (https://doi.org/10.3390/electronics11131942).

[6] G. VNKV Subba Rao and G. Uma, "An Efficient Secure Message Transmission in Mobile Ad Hoc Networks Using Enhanced Homomorphic Encryption Scheme", *Global Journal of Computer Science and Technology*, vol. 13, pp. 21–33, 2013 [Online]. Available: https://computerresearch.org/index.php/computer/article/view/169.

[7] S. Zaineldeen and A. Ate, "Improve the Security of Transfer Data File on the Cloud by Executing Hybrid Encryption Algorithms", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, pp. 521–527, 2020 (https://doi.org/10.11591/ijeecs.v20.i1.pp521-527).

[8] H.M. Al-Mashhadi and A.A. Khalf, "Hybrid Homomorphic Cryptosystem for Secure Transfer of Color Image on Public Cloud", *Journal of Theoretical and Applied Information Technology*, vol. 96, pp. 6474–6486, 2018 [Online]. Available: https://www.jatit.org/volumes/Vol96No19/17Vol96No19.pdf.

[9] M.N. Imtiaz and N. Khan, "Pan-Tompkins++: A Robust Approach to Detect R-peaks in ECG Signals", *2022 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, Las Vegas, USA, 2022 (https://doi.org/10.1109/BIBM55620.2022.9995552).

[10] M. Ngendahimana and W. Shen, "RSA Cryptosystem Speed Security Enhancement (Hybrid and Parallel Domain Approach)", *Crypto and Information Security*, vol. 2, 2023 (https://doi.org/10.23977/crypis.2023.020101).

[11] M.U. Shaikh, W.A.W. Adnan, and S.A. Ahmad, "Secured Electrocardiograph (ECG) Signal Using Partially Homomorphic Encryption Technique-RSA Algorithm", *Pertanika Journal of Science and Technology*, vol. 28, pp. 231-242, 2020 (https://doi.org/10.47836/pjst.28.s2.18).

[12] M.U. Shaikh, W.A.W. Adnan, and S.A. Ahmad, "Sensitivity and Positive Prediction of Secured Electrocardiograph (ECG) Transmission using Fully Homomorphic Encryption Technique (FHE)", *2020 IEEE-EMBS Conference on Biomedical Engineering and Sciences (IECBES)*, Langkawi Island, Malaysia, 2021 (https://doi.org/10.1109/IECBES48179.2021.9398792).

[13] A.A. Ahmed, M.M. Madboly, and S.K. Guirguis, "Securing Data Transmission and Privacy Preserving Using Fully Homomorphic Encryption", *International Journal of Intelligent Engineering and Systems*, vol. 16, pp. 277–289, 2023 (https://doi.org/10.22266/ijies2023.0228.25).

[14] P. Vithya KP, "Secured ECG Distribution Using Compression and RSA Algorithm for Telemedicine Application", *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 3, pp. 2277–3878, 2014 [Online]. Available: https://api.semanticscholar.org/CorpusID:212557890.

[15] O. Kocabas and T. Soyata, "Medical Data Analytics in the Cloud Using Homomorphic Encryption", *E-Health and Telemedicine*, pp. 751–768, 2016 (https://doi.org/10.4018/978-1-4666-8756-1.ch038).

[16] G.B. Moody and R.G. Mark, "The Impact of the MIT-BIH Arrhythmia Database", *IEEE Engineering in Medicine and Biology Magazine*, vol. 20, pp. 45–50, 2001 (https://doi.org/10.1109/51.932724).

[17] W.L. Caldas, J.P.V. Madeiro, C.L.C. Mattos, and J.P.P. Gomes, "A New Methodology for Classifying QRS Morphology in ECG Signals", *International Joint Conference on Neural Networks*, Glasgow, UK, 2020 (https://doi.org/10.1109/IJCNN48605.2020.9206707).

[18] D. Menard, D. Chillet, and O. Sentieys, "Floating-to-fixed-point Conversion for Digital Signal Processors", *EURASIP Journal on Advances on Signal Processing*, vol. 2006, art. no. 096421, 2006 (https://doi.org/10.1155/ASP/2006/96421).

[19] K. Sayood, *Introduction to Data Compression*, 5th ed., Elsevier, 765 p., 2018 (https://doi.org/10.1016/C2015-0-06248-7).

[20] S. Banerjee and G.K. Singh, "A New Real-time Lossless Data Compression Algorithm for ECG and PPG Signals", *Biomedical Signal Processing and Control*, vol. 79, art. no. 104127, 2023 (https://doi.org/10.1016/j.bspc.2022.104127).

[21] B. Yogapriya *et al.*, "Accelerating Linear Congruential Generators with Carbon Nanotube Field-effect Transistors", *IOP Conference Series: Materials Science and Engineering*, vol. 1316, art. no. 012005, 2024 (https://doi.org/10.1088/1757-899X/1316/1/012005).

[22] S. Nisha and M. Farik, "RSA Public Key Cryptography Algorithm – A Review", *International Journal of Scientific & Technology Research*, vol. 6, pp. 187–191, 2017.

[23] A.A. Ahmed, M.M. Madboly, and S.K. Guirguis, "Securing Signal Encryption Based on Reduced Round Homomorphic AES", *International Journal of Intelligent Engineering and Systems*, vol. 16, pp. 440–454, 2023 (https://doi.org/10.22266/ijies2023.0630.35).

[24] V. Mondelo *et al.*, "Detection of Heart Beat Positions in ECG Recordings: A Lead-dependent Algorithm", *Journal of Information Systems Engineering & Management*, vol. 2, pp. 1–8, 2017 (https://www.jisem-journal.com/download/64NV7FMF.pdf).

[25] H. De Melo Ribeiro *et al.*, "ECG-based Real-time Arrhythmia Monitoring Using Quantized Deep Neural Networks: A Feasibility Study", *Computers in Biology and Medicine*, vol. 143, art. no. 105249, 2022 (https://doi.org/10.1016/j.compbiomed.2022.105249).

[26] B. Adithya and G. Santhi, "A DNA Sequencing Medical Image Encryption System (DMIES) Using Chaos Map and Knight's Travel Map", *International Journal of Reliable and Quality E-Healthcare*, vol. 11, pp. 1–22, 2022 (https://doi.org/10.4018/IJRQEH.308803).

---

**Fatma Zohra Besmi, Ph.D. Student**
LIST Laboratory, Department of Electrical Systems Engineering
https://orcid.org/0009-0007-8216-0831
E-mail: f.besmi@univ-boumerdes.dz
University of Boumerdes, Boumerdes, Algeria
https://www.univ-boumerdes.dz

**Samia Belkacem, Ph.D., Associate Professor**
Department of Electrical Systems Engineering
https://orcid.org/0000-0003-0912-3392
E-mail: s.belkacem@univ-boumerdes.dz
University of Boumerdes, Boumerdes, Algeria
https://www.univ-boumerdes.dz

**Noureddine Messaoudi, Professor**
LIST Laboratory, Department of Electrical Systems Engineering
https://orcid.org/0000-0002-7228-5784
E-mail: n.messaoudi@univ-boumerdes.dz
University of Boumerdes, Boumerdes, Algeria
https://www.univ-boumerdes.dz