





Article

Fused Multi-Domains and Adaptive Variational Mode Decomposition ECG Feature Extraction for Lightweight Bio-Inspired Key Generation and Encryption

Israel Edem Agbehadji ^{1,*}, Richard C. Millham ^{2,*}, Emmanuel Freeman ³, Wanqing Wu ⁴ and Xianbin Zhang ⁴

¹ Honorary Research Fellow, Faculty of Accounting and Informatics, Durban University of Technology, P.O. Box 1334, Durban 4000, South Africa

² ICT and Society Research Group, Department of Information Technology, Durban University of Technology, P.O. Box 1334, Durban 4000, South Africa

³ Centre for Augmented Intelligence and Data Science, School of Computing, University of South Africa, Johannesburg 1709, South Africa; efreeman@gctu.edu.gh

⁴ School of Biomedical Engineering, Sun Yat-sen University, Guangzhou 510275, China; wuwangqing@mail.sysu.edu.cn (W.W.); zhangxb55@mail2.sysu.edu.cn (X.Z.)

* Correspondence: israeldel2006@gmail.com (I.E.A.); richardM1@dut.ac.za (R.C.M.)

Abstract: Security is one of the increasingly significant issues given advancements in technology that harness data from multiple devices such as the internet of medical devices. While protecting data from unauthorized user access, several techniques are used including fingerprints, passwords, and others. One of the techniques that has attracted much attention is the use of human features, which has proven to be most effective because of the difficulties in impersonating human-related features. An example of a human-related attribute includes the electrical signal generated from the heart, mostly referred to as an Electrocardiogram (ECG) signal. The methods to extract features from ECG signals are time domain-based; however, the challenge with relying only on the time-domain or frequency-domain method is the inability to capture the intra-leading relationship of Variational Mode Decomposition signals. In this research, fusing multiple domains ECG feature and adaptive Variational Mode Decomposition approaches are utilized to mitigate the challenge of losing the intra-leading correlations of mode decompositions, which might reduce the robustness of encryption algorithms. The features extracted using the reconstructed signal have a mean (0.0004), standard deviation (0.0391), skewness (0.1562), and kurtosis (1.2205). Among the lightweight encryption methods considered, Chacha20 has a total execution time of 27 μ s. The study proposes a lightweight encryption technique based on the fused vector representation of extracted features to provide an encryption scheme in addition to a bio-inspired key generation technique for data encryption.

Keywords: time-domain feature extraction; lightweight encryption; adaptive variational mode decomposition; ECG feature extraction; bio-inspired key generation



Citation: Agbehadji, I.E.; Millham, R.C.; Freeman, E.; Wu, W.; Zhang, X. Fused Multi-Domains and Adaptive Variational Mode Decomposition ECG Feature Extraction for Lightweight Bio-Inspired Key Generation and Encryption. *Sensors* **2024**, *24*, 7926. <https://doi.org/10.3390/s24247926>

Academic Editor: Georg Fischer

Received: 5 September 2024

Revised: 30 November 2024

Accepted: 4 December 2024

Published: 11 December 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Feature extraction is one of the topical issues in medical diagnosing. In order to have a proper diagnosis, one needs to understand the nature of feature extraction and its role in determining a diagnosis. The typical features used in a medical diagnosis include an Electroencephalogram or Electrocardiogram; while many techniques have been applied to feature extraction in the context of an Electrocardiogram (ECG), the effectiveness of these techniques has constantly been enhanced. Research has proven that using human features to create an encryption algorithm provides a much stronger approach notwithstanding the anticipated challenge it may have. Nonetheless, human biometric information are a promising alternative for cryptographic key generation to the traditional use of passwords as cryptographic keys. Cryptographic keys generated from biometrics are difficult to forge

and thus expand the frontiers of research into the use of different biometric key generation approaches. Keys can be extracted from biometric features, in raw ECG signals, which can be reliable despite the noise in ECG signals or abnormalities [1]. ECG-based biometric systems are much more reliable than other present biometric systems, e.g., fingerprints [2]. Furthermore, the widespread adoption of ECG technology in some clinical or hospital facilities and the ease of deploying ECG sensors in consumer settings in wearable devices [3] makes ECG signal encryption more imperative. Security-related application domains, when equipped with ECG signal encryption, provide many strong features to secure data on devices.

Currently, most Internet of Things (IoT) devices are championing the use of human features in encrypting data from medical devices. These IoT devices used in the context of medical diagnosing are so small that using traditional encryption algorithms on these devices may require more energy for computation [4]. Though most consider the use of a cloud computing framework to provide the needed encryption, it also requires that devices are constantly connected to the internet for data encryption [5]. The efficiency and security for privacy are often very distinct leading to the proposition of an image privacy protection scheme that ensures high-quality reconstruction using the discrete cosine transform compression and nonlinear dynamics [6]. When IoT devices use ECG signals for feature extraction, then the amplitude and intervals are used, which are further processed [7]. Here, it is the case that IoT devices are used to capture and monitor ECG features. It is very common these days to have wearable ECG devices attached to the human skin to continuously monitor ECG signals. This development demonstrates how IoT devices have evolved. Again, it is common to have IoT devices and smart watches equipped with ECG sensors to monitor a person's heartbeat. The integration of IoT in these areas suggests easy-to-collect ECG features; however, the challenge is the computation algorithm to ensure encryption using ECG features. Therefore, crafting any algorithm based on an ECG signal should be very lightweight. One of the key phases in the integration of IoT with ECG is the security of data being transmitted.

Feature extraction in the context of an ECG requires the identification and analysis of features in ECG data. When dealing with ECG feature extraction, the amplitude and intervals are very time-dependent. Thus, time-domain feature extraction may have to deal with the intra-leading relationship within the sequence of multiple ECG signals from the same person. Mostly, statistical and machine learning techniques play a leading role in analyzing these intra-leading correlations and thus model accuracy in analyzing these is imperative. Again, these intra-leading relationships are key for a comprehensive understanding of the heart's electrical activity and for making accurate diagnoses based on ECG data. One will expect that while these electrical activities are happening, the approach to encrypting these data should be robust, taking into account the intra-leading correlations. This research seeks to develop a lightweight encryption algorithm that considers these intra-leading relationships using a time-domain feature, frequency-time domain, and adaptive variational model decomposition-based technique. Existing cryptographic schemes are complex, such that the key generation consumes a large computation time and a large amount of energy [8]; thus, encryption schemes need a suitable lightweight approach to encryption. Thus, this study contributes to the introduction bio-inspired algorithm based on the Kestrel-based search algorithm as it randomizes searching with its half-life component, which adds layers of randomization for a more secure key generation for encryption. The advantage of the Kestrel-based approach is the ease of formulation, which does not add more computational cost in the search for an optimal key.

The remainder section is organized as follows: Section 2 (literature review), Section 3 (methods and materials), Section 4 (results), Section 5 (discussion), and the conclusion in Section 6.

2. Literature Review

This section focused on reviewing articles on multiple domain feature extraction techniques and also lightweight encryption mechanisms. The review is necessary to know what has been performed and the gap that needs to be filled through our research. These sections are aligned with the research topic, thus helping the crystallization of articles along the thematic domains.

2.1. Model-Based and Multi-Fusion Domain Bio-Signals Techniques

ECG signals are electrical impulses generated by the heart's activity, and these signals are recorded in series of waves (P, Q, R, S, T), representing the varied phases of the electrical activities of the heart's cycle from its starts (P wave) to the end of the sequence (T wave). The intermediate waves are the time to transition from one wave to another wave. Thus, the regular and timing features are very relevant in diagnosing any heart-related condition. In this regard, the ECG is very crucial in diagnosing heart-related issues. To capture these electrical activities, electrodes are placed on the skin of an individual and then the waves are monitored, which helps to differentiate people based on these waves [2].

The time-domain approach quantifies changes in ECG signal over time. Among the time domain features include average heart rate variations, R-R intervals, and Shannon entropy [9,10].

Zhao, Li [11] segmented and extracted ECG features into a time-domain matrix. Then, the periodic signal was transformed into a wavelet to output the frequency domain features in the matrix structure. Furthermore, a nature-inspired algorithm such as particle swarm optimization (PSO) was utilized to fine-tune parameters to optimize the extraction of ECG features. To address the accuracy of ECG feature identification from different domains, such as time, frequency, or time–frequency; the multi-feature fusion method was proposed, which combined Variational Mode Decomposition (VMD) and the Convolutional Neural Network (CNN) [12]. On one hand, the VMD technique was used for feature decomposition while the CNN was used to extract feature information from the ECG signal. Furthermore, the features extracted were weighted and fused for ECG signal recognition. Machine learning models have been leveraged for ECG feature extraction to help in cardiac evaluation and treatment decisions [13]. It has been indicated that ECG signals are time domain-reliant, leading to the conversion to spectrogram signals using a Short-Time Fourier Transform (STFT) [14]. Thus, different signals of heartbeat were segregated into a deep learning model for training. While using an open dataset, the six best P-QRS-T fragments were extracted based on priority and the normalization of positions using the non-fiducial symlets and non-fiducial daubechies [15]. Unfortunately, the accurate identification of fiducial points is a very challenging task in ECG signals if not well addressed: it can degrade the performance of the ECG-based biometrics [16]. This leads to the proposition of a framework based on ECG signal for user authentication, which does not need the detection of fiducial points. This framework utilized data-adaptive Variational Model Decomposition for noise removal and feature extraction from the ECG signal. Pradhan, Neelappu [17] suggested that mode decomposition approaches (e.g., empirical mode decomposition) are effective in signal analysis.

Physiological signals can be linked to emotions because both provide unconscious responses, suggesting that ECG features can help recognize people's emotions, which can influence their physiological responses at any given time [18]. The ubiquity of wearable ECG devices helps to recognize people's emotions; however, there are high chances of ECG signal contamination, which is caused by motion artifacts, thus leading to a decline in distinguishing ECG features [19]. The feature extraction algorithm for coronary heart disease detection using photoplethysmography used three algorithms that are respiratory rate (RR) interval, HRV Features, and Time Domain Features [20]. A photoplethysmograph (PPG) is a biomedical signal capable of detecting blood volume changes in the microvascular bed of tissues [21]. Myocardial infarction, also known as heart attack, was detected using 21 time-domain features that are extracted from 12-lead ECG signals [22]. Gender

classification based on ECG signals has also been proposed using time and frequency domain features [23]. The Time Multiplexed Fast Fourier Transform (TMFFT) approach was used to extract features for categorization into the frequency domain for Arrhythmia classification [24]. An Electrocardiogram (ECG) is broadly utilized for monitoring and diagnosing cardiac arrhythmia, which is an irregularity of the heartbeat that can potentially cause difficulties that create an instantaneous life risk [25]. In this regard, the Selective Opposition (SO)-based Artificial Rabbits Optimization (SOARO) strategy was applied to extract different features on time, time–frequency, entropy, and nonlinearity features of ECG [25]. In the context of the Autism Spectrum Disorders screening method, an acoustic method was employed in speech processing, where the acoustic features are constructed based on time–frequency domain independent component analysis (TF-ICA). In this approach, three methods used are, firstly extracting and combining the rows of the unmixing matrix of each frequency point to build the feature vector; secondly, entailing the separation of results on each frequency point as a time–frequency feature; and lastly, entailing the extraction of time-domain features from the outputs of TF-ICA [26]. When time-domain (TD) and frequency–time-domain (TFD) features are used together in a movement classification, it improves efficiency [27]. The Singh and Krishnan [28] approach leads to the extraction of the time domain, frequency domain, and time–frequency domain features in addition to the use of decomposition and sparse domain for ECG signal processing.

In the context of person identification, different EEG features like time domain, frequency domain, and time–frequency domain features were extracted and fused, in which a supervised learning approach was applied and evaluated in terms of accuracy rate, specificity, sensitivity, and F-score, and it was determined that the fusing method is efficient for user authentication [29].

Deep learning models such as the spatiotemporal deep learning technique have been applied to learn time-domain features, which are extracted into a matrix structure [30]. Furthermore, Khushaba, Phinyomark [31] proposed a simple time-domain feature extraction technique that leverages the capability of waveform length, zero crossings, and root mean squared to capture the relation between any number of channels.

In some instances, multiple domain feature extraction approaches were used combined with ensemble machine learning methods for classification and prediction [32]. Wavelet packet transform (WPT) and Short-Timed Fourier Transform (STFT) approaches were used to extract features from EEG signals. It has been indicated that using a single feature does not yield better performance compared to the fusion of multiple features [33]. In these regards, model-based approaches have been applied for both ECG and EEG feature extraction, and examples of such models include CNN and supervised learning. Again, fusing multiple different ECG features can provide an effective way to develop an encryption algorithm for the Internet of Medical Things. The feature normalization approach proposed used a binary classifier based on a support vector machine to classify features for high classification accuracy [34].

2.2. Lightweight Encryption Mechanisms

The unique properties of ECGs described in the previous section demonstrate the reason why it is preferred for user identification rather than the use of more traditional methods, such as passwords, etc. [35]. This section mainly focuses on the encryption mechanism.

Hash function and DNA cryptography were used to implement the Triple Data Encryption Standard (Triple-DES) that combines Hash function and DNA cryptography to encrypt different bio-signals into the DNA format. Mathivanan, Ganesh [36] proposed a system to convert ECG signals into QR codes. Additionally, Karthikeyan and Martin Leo Manickam [37] introduced a secret key generation algorithm extracted from the parameters of the ECG signal to allow device authentication. A reversible bio-signal steganography method was applied using the Extended Binary Golay Code based on the error correction method [38].

A wavelet-based 128-bit key generator using the uniqueness and quasi-stationary biometric behavior of ECG signals of individuals was proposed: there were two stages: key generator on enroll and verify and another on key determination with an algorithm [39]. Many encryption algorithms that rely on the key size of the 256-bit key have also been proposed, which include the Chacha20 encryption scheme [40]. This scheme encrypts data a byte at a time leading to the generation of stream cipher for data encryption [41].

Heartbeat-based Random Binary Sequences (RBSs) that generate 128-bit RBSs using inter-pulse intervals (IPIs) of heartbeats incorporate a finite monotonic increasing sequence generation mechanism of IPIs and a cyclic block encoding procedure that extracts a high number of entropic bits from each IPI [42].

The generation of a security key using the R-R interval feature of ECG signals as an input for verification and identification occurs by generating a security key corresponding to an individual. The system comprises two independent stages: registration and authentication. The biometric security key, created in the registration stage, was generated using Hamming Distance and the extended version of the triple DES algorithm. Biometric security key generation, verification, authentication, and performance of the biometric security key have been assessed using the R-R interval of ECG signals taken from the standard MIT-BIH database [43]. The simulation results for 64-bit, 128-bit, and 256-bit biometric security keys indicate that the performance of the proposed biometric security key is reasonably good for a security system.

An energy-efficient and computationally less complex authentication technique for BSN, which is a biometric-based algorithm, is proposed, which utilizes Heart Rate Variability (HRV) for a simple key generation process. The proposed algorithm is compared with three data authentication techniques, namely Physiological Signal Key Agreement (PSKA), Data Encryption Standard (DES), and Rivest Shamir Adleman (RSA). The results suggest that the proposed algorithm is quite efficient in terms of transmission time utilization, average remaining energy, and total power consumption [8]. The RSA encryption algorithm is utilized to encrypt an ECG signal; however, the RSA algorithm only performs one operation on encrypted data, which can either be addition or multiplication [44].

Generation of the key without requiring the key pre-distribution solutions approach was proposed involving two different Interpulse Interval (IPI) features of ECG-based cryptographic key generation. The first approach is realized by using a pseudo-random number and consecutive IPI sequences. The second approach is realized by utilizing the Advanced Encryption Standard (AES) algorithm and IPI as the seed generator for the AES algorithm [45].

Due to intra-individual variability, bio-crypto keys (bio-keys), in the context of wearable devices, based on Electrocardiograms (ECGs), were proposed for flexibility and convenience to use bio-key using ECGs. This approach minimizes biosignal variability using normalization, clustering-based binarization, and the fuzzy extractor, enabling the generation of personalized seeds and offering ease of use with the accuracy of authentication [46].

Moosavi, Nigussie [45] combined two different bio-signals, such as ECG and EMG, to generate keys in cryptographic systems by initially using a “pseudo-random number” and consecutive IPI sequences, then followed by the use of an “Advanced Encryption Standard” (AES) algorithm and IPI as a seed generator for the AES algorithm. The advantage of this approach is that it avoids pre-key distribution and ensures ease of key generation. Karthikeyan and Manickam [47] proposed an authentication model for a low resource-constrained architecture where a secret key is generated from the ECG signal parameter and combined with the Secure Force (SF) algorithm in a wireless network.

The generation of a persistent key from an ECG signal to ensure symmetric encryption of data in a time-invariant key has been considered in [48]. Similarly, a time-invariant cryptographic key generation mechanism based on electroencephalogram (EEG) signals has also been proposed [49]. A key generation approach that uses a wavelet-based 128-bit key generator from ECG signals was proposed, which comprises two independent steps, that is, enrollment and verification generation [39].

The ECG signal is distinct to an individual such that it is very difficult to emulate; therefore, securing these features of ECG so that only an authenticated person can assess these signals for diagnosis purposes is imperative [50]. Furthermore, the processing of the ECG signal was achieved with the QRS complex method, which shows the heart rates (HR) that can be visually seen and traced; thus, it is easy to encrypt the visual part of ECG tracing.

ECG signals are used for identification because it varies between individuals [51]. From a diagnostic perspective, individuals who have a background of heart-related issues and have a long record of ECG require a large amount of storage space [52]. Pan and Tompkin's algorithm helps in the detection of ECG signal [52]. In these regards, selecting the optimal key parameter is significant for an encryption algorithm and this optimization was achieved using the glow-worm swarm optimization method for encryption [5]. Thus, this suggests that a nature-inspired optimization algorithm can play a role in key generation for an encryption algorithm. ECG encryption technique relies on DNA layers and AES to reduce the encryption execution time and improve security for IoT health applications [53]. Methods to extract ECG features include the Lyapunov exponent's spectrum in which the extracted features are used as a secret key to encrypt pictures and text messages [54].

3. Materials and Methods

The method and material section outlines the stages to preprocess ECG signals, extract features, normalize features, generate the feature vector, conduct a statistical analysis on the feature vector including zero crossing, and then save the final feature vector. Developing an encryption algorithm using ECG (Electrocardiogram) signals is an intriguing idea that combines elements of biometric security with cryptography. ECG signals are unique to individuals, which means they can serve as a basis for personalized encryption. The following sub-sections detail how the study approaches this.

3.1. Loading of the ECG Signal Dataset

The ECG signal is loaded from a file or data source. Each recording has a 20-s single-lead ECG signal from LIMB II, with a sampling rate of 500 Hz. The dataset contains 89 ECG recordings, including 25 from healthy individuals in a lab setting, 20 from the MIT-BIH Arrhythmia Database (MITDB), and 44 from cardiac patients in a clinical environment. These data are stored in the "data.mat" file and can be read using Python 3.13 with the Scipy package. The package is organized as a dictionary, with corresponding labels and original signal data, each containing 10,000 data points. The input to the model is the BIH Arrhythmia Database (MITDB).

3.2. Preprocess ECG Signal

The raw ECG signal is cleaned from noise and normalized for further processing. The band-pass filter approach is used to remove noise, which is expressed as a frequency response $H(f)$ (see Equation (1)). The band-pass filter allows only a specific range of frequencies to pass while attenuating frequencies outside this range [0, 1].

$$H(f) = \begin{cases} 1 & \text{for } f_L \leq f \leq f_H \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

where f is frequency, f_L is the lower cutoff frequency, and the upper cutoff frequency is f_H ; therefore, Equation (2) is as follows:

$$h(t) = h_{LP}(t) - h_{HP}(t) \quad (2)$$

where $h_{LP}(t)$ and $h_{HP}(t)$ represent the impulse responses of the low-pass and high-pass filters, respectively. To improve the model's ability to generalize, the recordings were normalized and scaled to a common range (e.g., 0 to 1) using min-max scaling expressed in Equation (3), as follows:

$$F_{norm} = \frac{F - F_{min}}{F_{max} - F_{min}} \quad (3)$$

where F_{min} and F_{max} are the min and max feature normalization in the range [0, 1].

3.3. ECG Extract Features

The adaptive variational model decomposition (adaptive VMD) approach is used to decompose the ECG signal and further remove noise. Thus, given the ECG signal $x(t)$, the decomposition is expressed in Equation (4), as follows:

$$x(t) = \sum_{i=1}^M S_i(t) + n(t) \quad (4)$$

where $x(t)$ is the observed signal, $S_i(t)$ is i th signal, $n(t)$ is residual noise, and M is the total number of signals. Residual noise in the ECG signal and noise after ECG signal reconstruction can impact the feature extraction with the adaptive VMD; thus, functions expressed in Equations (5)–(8) were employed to address these noises.

The variational mode defines the likelihood function F_n , which is expressed in Equation (5), as follows:

$$F_n = p(x|s, n) \quad (5)$$

where the prior distribution probability $p(s, n)$ represents the likelihood of any other noise in the ECG signal. Thus, the objective function of the variational mode is expressed in Equation (6) as follows:

$$Obj(s, n) = R_{error} + R \quad (6)$$

where R_{error} is the reconstruction error and R is the regularization, which is the smoothness of the sparsity of noise. Thus, in Equations (7) and (8),

$$R_{error} = \|x(t) - \sum_{i=1}^M S_i(t) + n(t)\|_2 \quad (7)$$

$$R = \sum_{i=1}^M \lambda_i \|s_i(t)\|_p + \gamma \|n(t)\|_q \quad (8)$$

where λ_i and γ are the regularization parameters and $\|\cdot\|_p$ and $\|\cdot\|_q$ are the norms. The model parameters are adjusted based on the input signal at the decomposition stage at a learning rate based on the observed data; thus, $s_i^{(k)}$ and $n^{(k)}$ parameters are iteratively updated to reduce any possible impact of noise and the parameters were achieved using Equations (9) and (10).

$$s_i^{(k+1)} = s_i^{(k)} - \eta \frac{\delta(Obj)}{\delta.s_i} \quad (9)$$

$$n^{k+1} = n^k - \eta \frac{\delta(Obj)}{\delta.n} \quad (10)$$

where η and k are the learning rate and iteration, respectively.

Though mode decomposition aids in feature extraction, the study went a step further to extract features using the R-peak, which aids in computing the Heart Rate Variability (HRV), RR interval (Time between successive R-wave peaks), and wave characteristics Q, S, and T in terms of amplitude and duration. The approach to compute the HRV is based on the standard deviation of the R-R intervals, which is measured using the Standard Deviation of NN intervals-SDNN). Also, by using the Root Mean Square of Successive Differences (RMSSD), the continual differences in the interval are computed. HRV metrics capture the SDNN and RMSSD of the extracted features, which are expressed using Equations (11) and (12):

$$sdnn = \sqrt{\frac{1}{N-1} \sum_{i=1}^N (RR_i - \text{mean}(RR))^2} \quad (11)$$

$$rmsd = \sqrt{\frac{1}{N-1} \sum_{i=1}^{N-1} (RR_{i+1} - \text{mean}(RR_i))^2} \quad (12)$$

Three types of features are imperative in feature extraction, namely, time-domain, frequency-domain, and time–frequency domain. The time-domain feature $f_{(time)}$ like the mean, standard deviation, root mean square (RMS), skewness, and kurtosis from each segment were computed.

The discrete Fourier transform (DFT) signal is used to compute the spectrum of finite duration signal expressed in Equation (13) by

$$X[k] = \sum_{n=0}^{N-1} x[n] \cdot e^{-j\frac{2\pi kn}{N}} \quad (13)$$

where $X[k]$ and N are the DFT coefficient at index k and total number of samples, respectively. $x[n]$ is the discrete time-domain signal. Then, to recover the original discrete signal, the Inverse Discrete Fourier Transform is expressed in Equation (14) by

$$x[n] = \frac{1}{N} \sum_{k=0}^{N-1} X[k] \cdot e^{j\frac{2\pi kn}{N}} \quad (14)$$

where $x[n]$ and $X[k]$ are the n -th time domain in a sample and the k -th frequency domain components, respectively. N represents the number of points in the sequence and j is the imaginary units.

Furthermore, the time–frequency domain features $f_{(timefreq)}$, which addresses the changes in frequency over time, was computed using a Short-Time Fourier Transform (STFT) that maps subsequent segments of ECG signal into dimensions of time and frequency expressed in Equation (15), as follows:

$$X(t, f) = \int_{-\infty}^{\infty} x(\tau) w(\tau - t) \cdot e^{-j2\pi f\tau} d\tau \quad (15)$$

where $w(\tau - t)$ is the window function positioned at t .

Finally, the fusion of multiple domains f_{fused} is expressed to concatenate all the different domain features into a single vector representation that can be expressed in Equation (16) as:

$$f_{(fused)} = \left[f_{(time)} \mid f_{(freq)} \mid f_{(timefreq)} \right] \quad (16)$$

where $f_{(fused)}$ is the fused vector, $f_{(time)}$ is the vector of the time-domain feature, $f_{(freq)}$ is the frequency-domain feature, and $f_{(timefreq)}$ is the vector of time–frequency domain features.

3.4. Statistical Analysis

Zero-crossing rate (ZCR) calculates the number of times the preprocessed signal crosses zero within a time t window. ZCR for the continuous-time signal is expressed in Equation (17) as

$$ZCR = \frac{1}{T} \int_0^T \left| \frac{dS_f(x(t))}{dt} \right| dt \quad (17)$$

where S_f represents the sign function of $x(t)$ between $(+1, 0, -1)$ in Equation (18), as follows:

$$x(t) = \begin{cases} +1, & \text{for } x(t) > 0, \\ -1, & \text{for } x(t) < 0 \\ 0, & \text{if } x(t) = 0 \end{cases} \quad (18)$$

3.5. Bio-Inspired Key Generation

The bio-inspired method was inspired by the concept of the half-life of a radioactive substance, which was considered in the formulation of the kestrel-based search algorithm [55]. The half-life was expressed as having N unstable substances that decay at time t is expressed in Equation (19):

$$\frac{dN}{dt} = -\gamma N, \quad (19)$$

Which can be simplified in Equations (20)–(22), as follows:

$$\gamma_t = \gamma_0 \cdot e^{-\varphi t} \quad (20)$$

$$\varphi = \frac{\ln 0.5}{-t_{\frac{1}{2}}} \quad (21)$$

$$\text{if } \varphi \rightarrow \begin{cases} \varphi > 1, \text{ trail is new} \\ 0, \text{ otherwise} \end{cases} \quad (22)$$

where φ is the decay constant and $t_{\frac{1}{2}}$ is the period of half-life representing the required time for γ_t to become half of γ_0 . γ is the light intensity variation generated at random intervals between [0, 1]. The bio-inspired method has been applied in several problem domains and the selection of the parameters in the method was demonstrated through an experiment with promising performance results [55–57]. Among the parameters include the flight (0.8) and perch (0.2) modes. The initial population in the bio-inspired algorithm is generated using Equation (23), as follows:

$$\gamma_t = [\gamma_1, \gamma_2, \dots, \gamma_n, \text{RandBit}()] \quad (23)$$

Randbit() represents a random bit generator to ensure randomization and reduce the chance of unauthorized breaking of the encryption key. A unique key is generated from the vectorized fused feature and hashed. Afterward, the bio-inspired algorithm final key is generated using the following Equation (24):

$$Fkey = [\text{UniqueFeatureKey}, \gamma_t] \quad (24)$$

$$\text{UniqueFeatureKey} = (F_1, F_2, \dots, F_n) \quad (25)$$

where F_i is the fused multi-domain vectorized ECG feature. The randomness of the generated key with Shannon entropy and Min-entropy for the bio-key generated on the ECG signal of the subject were evaluated to assess randomness through entropy in Equation (26):

$$\text{Shannonentropy} = -\sum_i P_i \log_2 P_i \quad (26)$$

$$\text{Minentropy} = -\log_2 () \quad (27)$$

The final key *Fkey* is used with Chacha20 for encrypting ECG bio-signals. The encryption scheme is mathematically modeled such that it takes the plaintext P_i and applies the XOR on the keystream k to output the cypher text C_i at each position i as expressed by Equation (28):

$$C_i = P_i \otimes K_i \quad (28)$$

Furthermore, the decryption scheme is then expressed by Equation (29), as follows:

$$P_i = C_i \otimes K_i \quad (29)$$

where P_i represents the plaintext and C_i is the cipher text at the i th position. The keystreams k are extracted from the fused vector representation. Figure 1 below illustrates the encryption scheme.

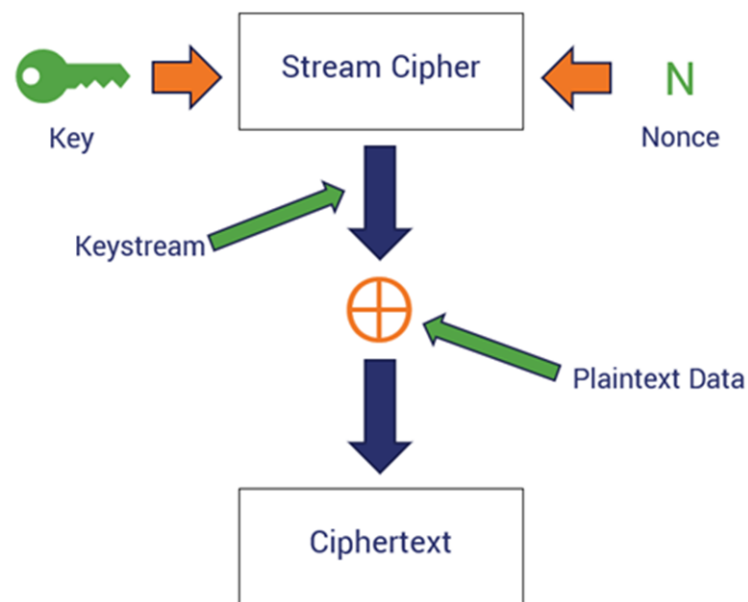


Figure 1. Diagram of the encryption scheme.

3.6. Algorithm to Implement Lightweight Encryption

The algorithm to implement the lightweight encryption steps is expressed with Algorithms 1–3. Algorithm 1 indicates the steps in ECG signal processing. In this algorithm, raw ECG signal is inputted, and then different mathematical computations are performed to output the pre-processed ECG signal.

Algorithm 1: ECG signal Preprocessing

1. **Input:** raw ECG signal, F_{min} , F_{max} ,
 2. **Compute:** $H(f)$ using Equation (1)
 3. **Compute:** $h(t)$ using Equation (2)
 4. **Compute:** F_{norm} using Equation (3)
 5. **Output:** Preprocessed ECG signal
-

Algorithm 2 presents the steps to implement the feature extraction.

Algorithm 2: Feature Extraction

- //data-adaptive variational model decomposition*
1. **Compute:** $x(t)$ using Equation (4)
 2. **Compute:** $Obj(s, n)$ using Equation (6) to compute the objective function and likelihood of error in mode reconstruction
 3. **Compute:** s_{dnn} , r_{mssd}
 4. **Compute:** discrete Fourier transform (DFT) signal using Equation (11)
 5. **Compute:** $X(t, f)$ using Equation (15)
 6. **Compute:** $f_{(fused)}$ using Equation (16)
 7. **Compute:** ZCR using Equation (17)
 8. **Output:** fused feature vector
-

Algorithm 3 presents a fused feature vector and the bio-inspired key generation steps.

Algorithm 3: Fused feature vector and bio-inspired key generation

1. **Initialize population:** F_i
 2. **Generate** Unique key for the feature vector in the string representation
 3. **Generate:** random key using Half-life
 4. **Generate:** Fkey
 5. **Output:** Fkey
 6. **Apply:** Fkey with the Chacha20 encryption scheme as expressed by Equations (28) and (29).
-

4. Results

This section presents the experimental results. Figure 2 shows the frequency of the original ECG data. The highest amplitude is a little above 0.3 and the lowest is below the -0.3 amplitude.

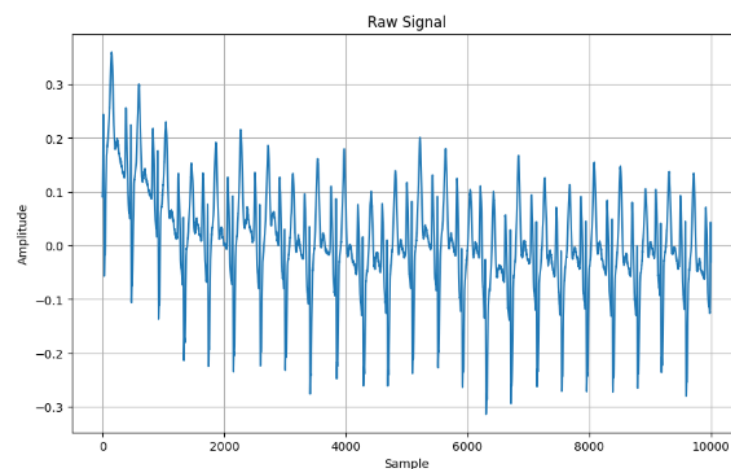


Figure 2. Raw signal.

Figure 3 shows the extracted ECG signal using the adaptive VMD method in which the amplitude signal was 0.90, such as the peak for the 10,000 samples.

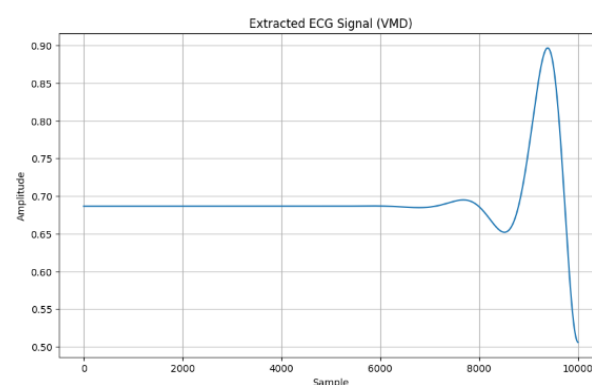


Figure 3. ECG signal extraction using adaptive VMD.

Figure 4 shows the adaptive VMD consisting of three stages. The first phase of the decomposition initialized the noise tolerance value (0.0), in which the mode five decomposition is created to enable a view of the behavior of the frequencies. The bandwidth constraint of 2000 was set within a tolerant convergence criterion of 1×10^{-7} . The second stage is the visualization of the mode decomposition in terms of the original signal and the five-mode decomposition as shown in Figure 4.

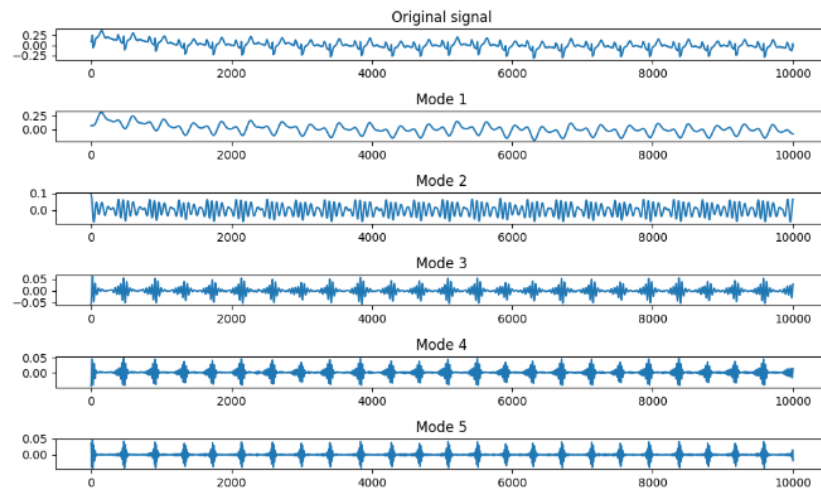


Figure 4. Five adaptive Variational Mode Decomposition (VMD).

Finally, Figure 5 shows the mode reconstruction where all noise has been removed from the signal in preparation for feature extraction. The highest amplitude was a little above the 0.15 amplitude and the lowest amplitude was below -0.10 .

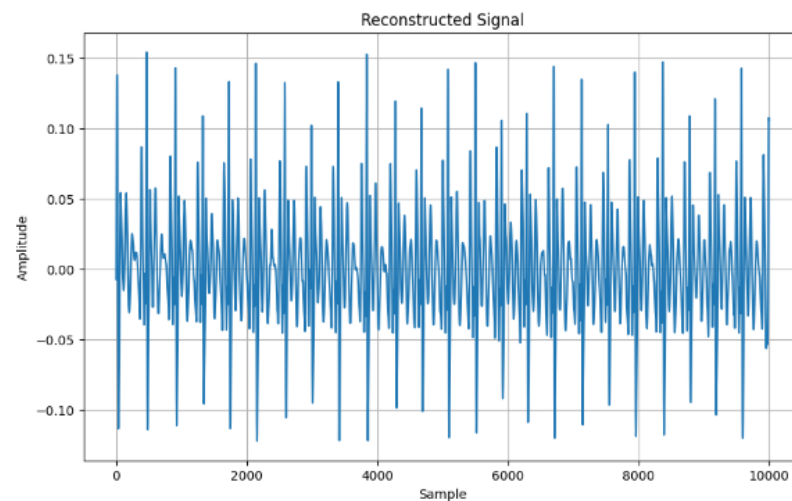


Figure 5. Signal reconstruction with adaptive VMD.

Figure 6 depicts the power spectral density of the adaptive VMD models where mode 1 (in Figure 5) happens to have the highest peak of (0.0006) and mode 2 (0.0001).

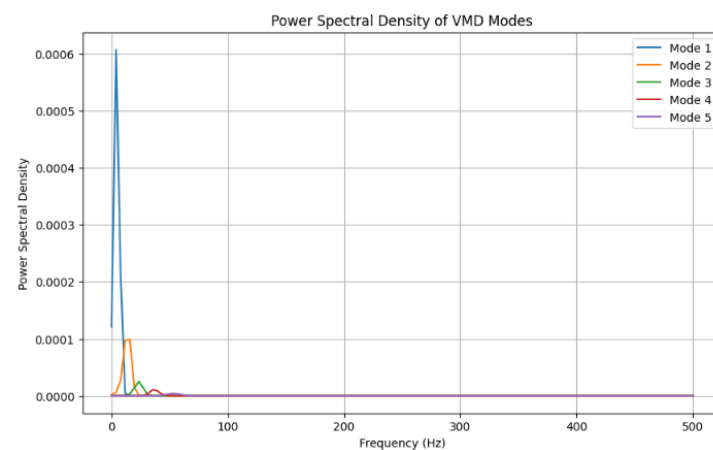
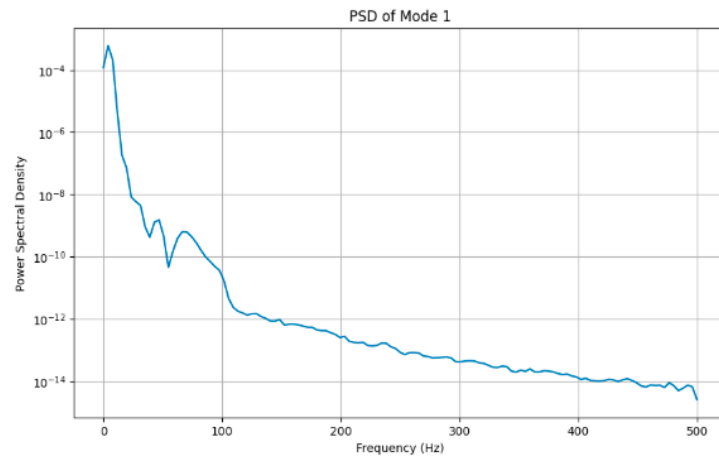
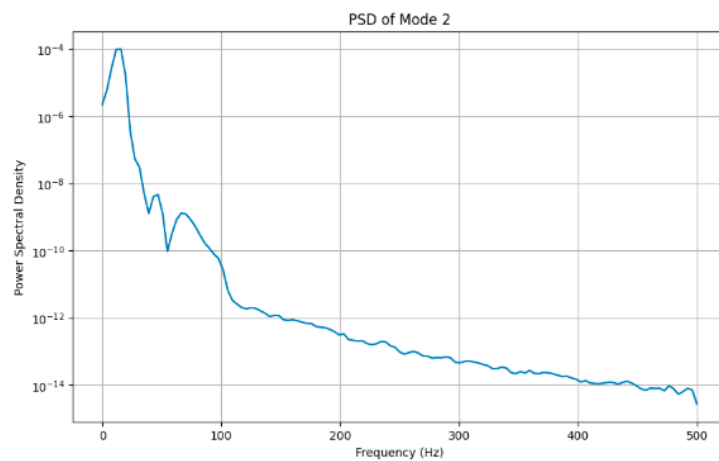


Figure 6. Power spectral density of adaptive Variational Mode Decomposition (VMD).

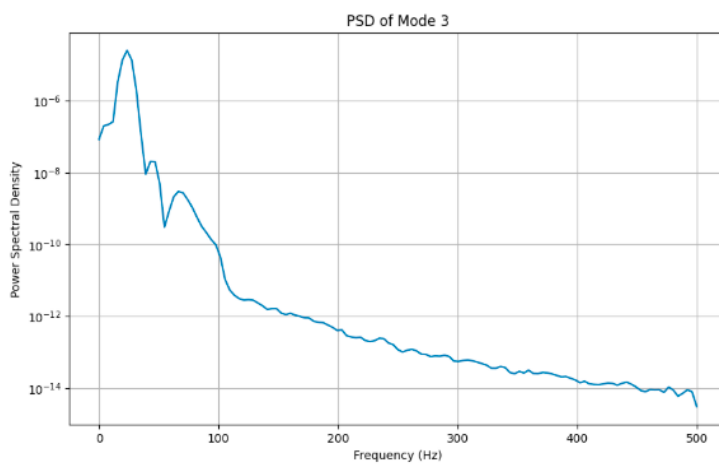
Figure 7 shows each adaptive VMD mode for the reconstructed signal. The mode shows the decomposition of the ECG signal to help understand the frequencies in each segment of the mode.



(a)

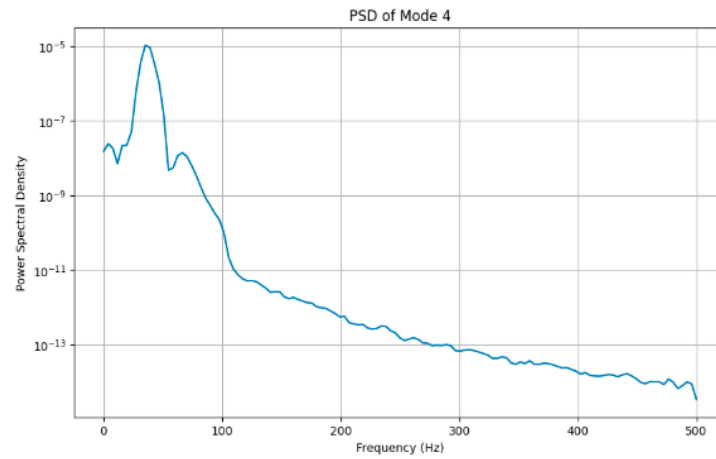


(b)

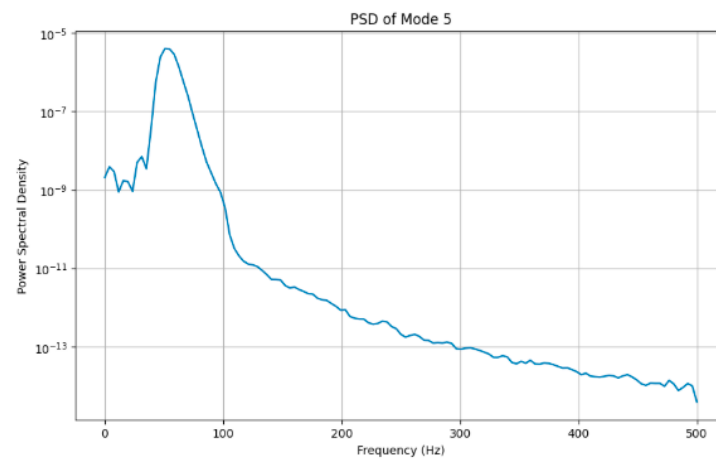


(c)

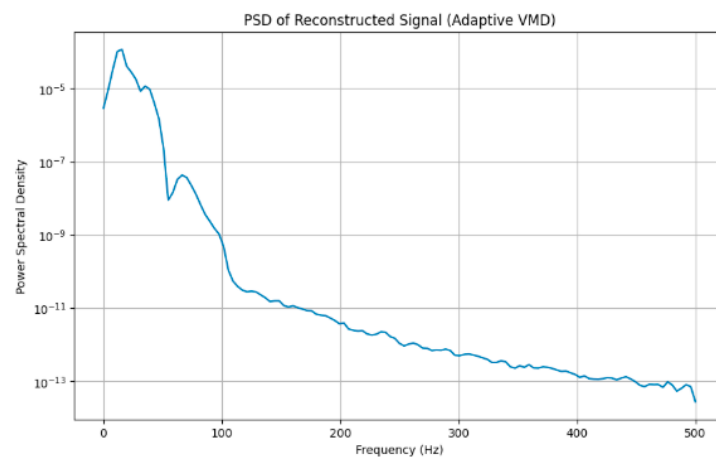
Figure 7. Cont.



(d)



(e)



(f)

Figure 7. Power spectral density of the adaptive VMD with five modes.

Figure 8 shows the Empirical Mode Decomposition method (EMD) as another approach to recovering the ECG signal in which the first Intrinsic Mode Function (IMF) of the ECG signal is identified as it recognizes the highest frequency. IMF varies in amplitude and frequency, where the high amplitude is approximating to 0.04.

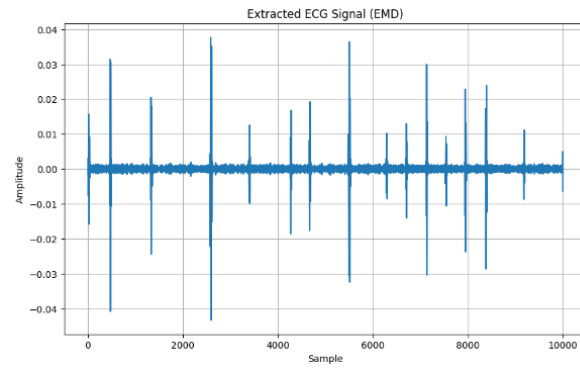


Figure 8. Extracted ECG signal with EMD.

Using the EMD approach, the first IMF becomes the recovered signal, which is depicted in Figure 9.

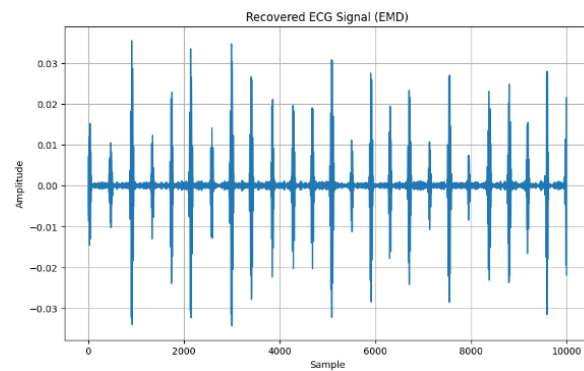


Figure 9. Recovered ECG signal (EMD).

Figure 10 shows the reconstructed signal with the time-domain features extracted showing the mean (0.0004), standard deviation (0.0395), skewness (0.2989), and kurtosis (1.4022).

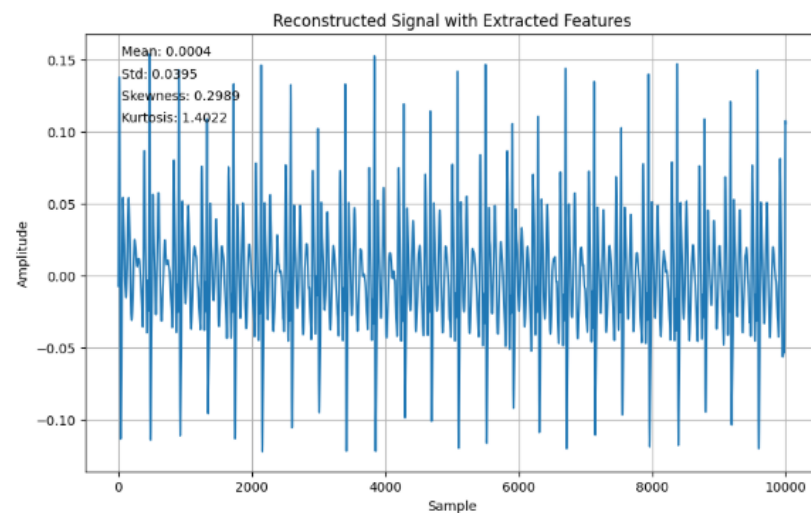


Figure 10. Reconstructed signal with extracted features.

Figure 11 shows the frequency domain feature extractions using the continuous Fourier transform. The magnitude spectrum was computed and the features captured are the dominant frequency (14.3000 Hz), spectral centroid (−0.0030), spectral spread (80.3951), spectral entropy (10.1530), and spectral Rolloff (−14.0000). In Figure 12, the Inverse Discrete

Fourier Transform (IDFT) is presented as it converts the frequency-domain features back to the corresponding time domain; such conversion confirms Figures 10 and 11.

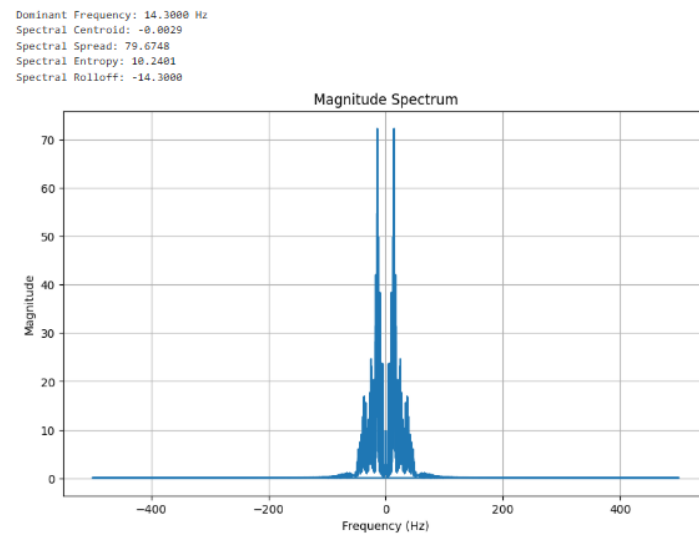


Figure 11. Frequency domain features extracted from the reconstructed signal using a continuous Fourier transform.

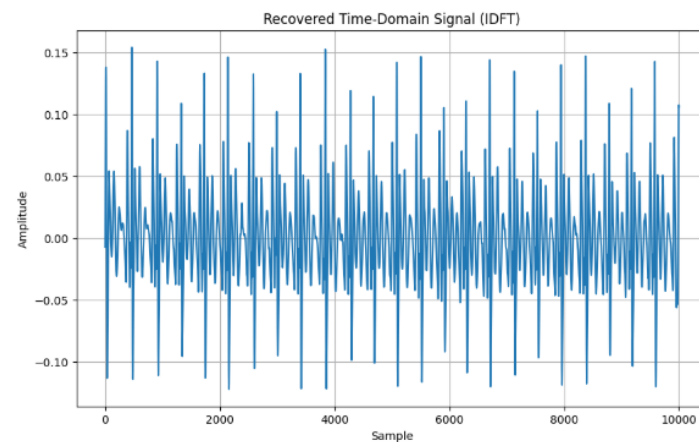


Figure 12. Time domain signal.

Figure 13 shows the STFT magnitude spectrogram showing the actual signals. It highlights the time–frequency property for an accurate representation of the signal. Colors represent the amplitude frequency at each point in time. Dark portions are regions with one signal. Through the distribution, the patterns can be visualized and timed in seconds (s) displayed.

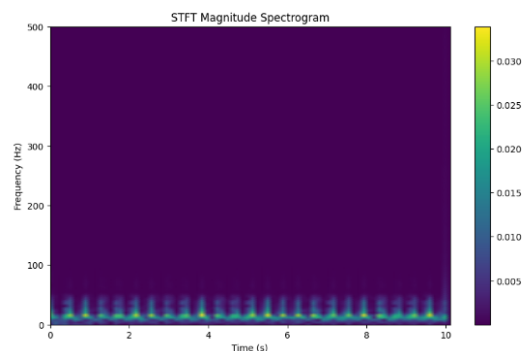


Figure 13. STFT Magnitude spectrogram visualization.

Figure 14 shows the frequency domain in terms of the mean and spectral entropy over time. The mean frequency describes the central frequency of the power spectrum concentration.

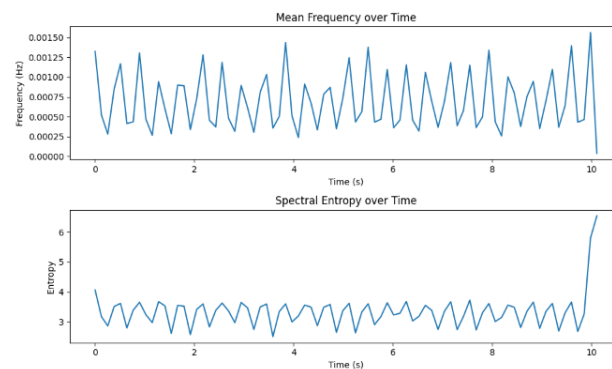


Figure 14. Frequency domain.

Figure 15 shows the difference between reconstructed and recovered signals. The MSE and RMSE are the statistical methods used to find the differences, which demonstrates that the means were both 0.00, suggesting that there is no variation between the reconstructed and the recovered signals. Figure 16 shows further analysis of the reconstructed and recovered signal, which further demonstrates no variation.

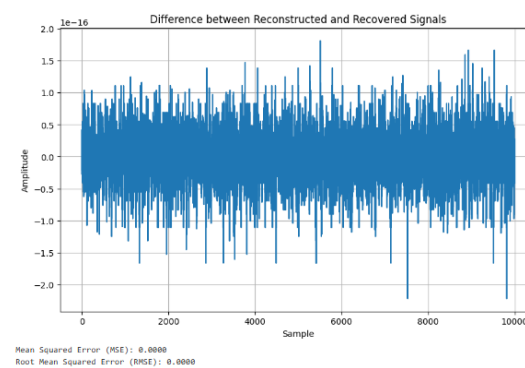


Figure 15. Differences between reconstructed and recovered signal.

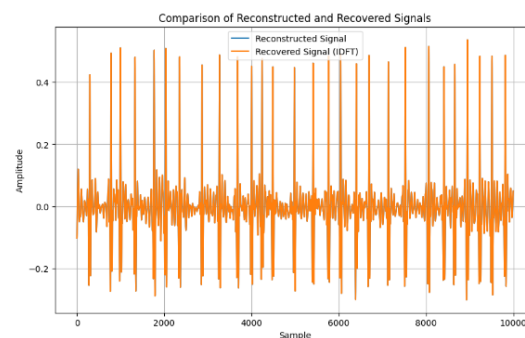


Figure 16. Comparison of reconstructed and recovered signal.

Figure 17 displays both the IBI and its histogram. The fluctuation in the heartbeat varies with time indicates a functioning nervous system of the individual. Again, the histogram demonstrates the time interval of successive heartbeats over some time. These features of the heartbeat are imperative in creating an effective encryption scheme from the human features.

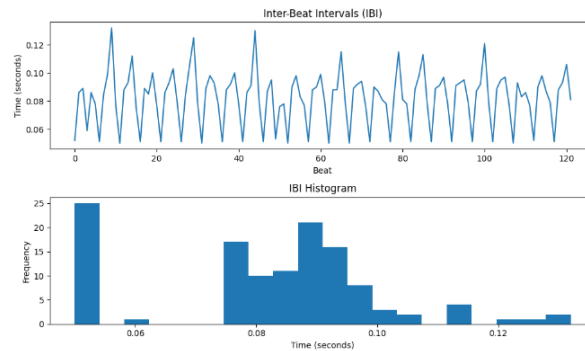


Figure 17. Inter-beat interval (IBI) and IBI histogram.

The HRV computation utilized standard deviation among others to calculate, in beats per minute (BPM), the heart rate, which was recorded as 738.00 (BPM), RMSSD (0.0840 s), SDNN (0.0191 s), NN50 (0), and pNN50 (0.00%). Also, the zero-crossing rate was 0.0245. Table 1 shows the aggregated domain features in terms of the time domain and frequency domains.

Table 1. Domain features.

Aggregated Features	Value	Type of Feature Domain
Dominant Frequency:	14.3000	Frequency domain
Spectral Centroid:	−0.0029	Frequency domain
Spectral Spread:	79.6748	Frequency domain
Spectral Entropy:	10.2401	Frequency domain
Spectral Rolloff:	−14.3000	Frequency domain
Mean Frequency:	0.0007	Time–frequency
Mean Spectral Entropy:	3.3442	Time–frequency
Mean	0.0004	Time domain
standard deviation	0.0395	Time domain
Skewness	0.2989	Time domain
Kurtosis	1.4022	Time domain

The fusing approach is an aggregation of time–frequency domain features, frequency domain features, time-domain features, EMD, and adaptive VMD features, which were vectorized. Having extracted these features as shown in a vector representation, the bio-inspired algorithm was utilized to generate a random key. Before this, the extracted feature vector is converted to string representation and the bio-key was applied to finally generate the encryption key. The encryption scheme was evaluated by loading different ECG signals to extract the features in vector format and applied for ECG signal encryption. The resultant feature extracted is shown in Figure 18 as

```

Aggregated Features:
Dominant Frequency: 14.3000
Spectral Centroid: -0.0029
Spectral Spread: 79.6748
Spectral Entropy: 3.3442
Spectral Rolloff: -14.3000
Mean Frequency: 0.0007
Mean Spectral Entropy: 3.3442
Feature Vector: [14.3, -0.002915515185382191, 79.67477338394227, array([4.06575802, 3.17452134, 2.86174545, 3.51166797, 3.61642615,
2.79194799, 3.38879297, 3.65292222, 3.23736493, 2.97473138,
3.67446494, 3.53199381, 2.60919275, 3.55166933, 3.52244106,
2.57375795, 3.41762178, 3.59603665, 2.83045495, 3.38095283,
3.62749833, 3.36772089, 2.97215678, 3.6460379 , 3.46862016,
2.74559641, 3.49773824, 3.59401521, 2.50512399, 3.34447296,
3.59904615, 2.99649459, 3.19264629, 3.56171814, 3.49147876,
2.87147118, 3.48741202, 3.57764066, 2.64807141, 3.36884634,
3.61996902, 2.6311235 , 3.32957951, 3.60209139, 2.90419884,
3.17415784, 3.63668131, 3.22945751, 3.2855181 , 3.68128278,
3.03034219, 3.18411653, 3.55191029, 3.38377912, 2.74385371,
3.35147697, 3.67178181, 2.73773781, 3.18135503, 3.72518946,
2.72745831, 3.30468865, 3.61139266, 3.01164798, 3.14546461,
3.5608408 , 3.48529257, 2.81024951, 3.35332882, 3.65730325,
2.78319609, 3.35426688, 3.61419813, 2.69398781, 3.30126569,
3.66014471, 2.67755731, 3.25788281, 5.80114608, 6.53831279]), -14.3, 0.0006928341710578382, 3.344168737990118]
Bio Key: 14.3000-0.002979.67483.3442-14.30000.00073.3442

```

Figure 18. Fused feature vector with adaptive VMD.

Figure 19 depicts the bio-key, random bio key, and encryption key obtained from the feature vector.

```
Bio Key: 14.3000-0.002979.67483.3442-14.30000.00073.3442
Randomized Bio Key: 0.78-0.70-.04910132360230.343.004.4409070324.04
Encryption Key: a31f6dd3116596e2fe93f33fcbda22a9febb70d14ccdc12fc29e76c805697e3e
```

Figure 19. Key generation.

Figure 20 shows the cipher and decrypted text. It also indicated the status of decryption.

```
Ciphertext: 5d5201d19de058c7fad9a7b466d04c889d940e39d525167049af1c7ca6e1491
Decrypted Hashed Key: 87ed52ab2539cacc68fb551e0acc958abd5a915b33284c9ff827e66cdbfedc4b
Decryption Successful: True
```

Figure 20. Cipher and decrypted text.

A large population of kestrels can cover a broader search area, which increases the chances of finding a global optimum key but requires more computational resources. In this study, the population size was 200, to limit the computational cost of devices. However, a small population might fail to explore enough of the solution space, leading to a less secure key. Table 2 provides a comparison of the execution time of the encryption algorithms.

Table 2. Comparison of execution time.

Encryption Scheme	Encryption Time	Decryption Time	Key Generation Time	Total Time
ChaCha20	9.40 μ s	9.75 μ s	7.85 μ s	27 μ s
ChaCha	10.80 μ s	10.98 μ s	7.85 μ s	29.63 μ s
Salsa20	11.45 μ s	11.60 μ s	7.85 μ s	30.90 μ s

The computing time (execution time) was considered in terms of time of encryption, time of decryption, and time for key generation. In this instance, the same population size in the bio-inspired search method was maintained and the efficiency was recorded in terms of execution time. The speed of encryption and decryption were measured (in microseconds (μ s)) by executing the algorithm and recording the time taken. From Table 2, it can be observed that Chacha20 has a total execution time of 27 μ s, Chacha (29.63 μ s), and Salsa20 (30.90 μ s). Thus, Chacha20 was efficient and suitable for resource-constrained devices.

The potential vulnerability of the proposed encryption scheme was the noise removal from the raw signal, which may impact the encryption key generation. Thus, the signal reconstruction approach was introduced to further remove noise, thus providing the surety and robustness of the encryption scheme.

5. Discussion

This study focused on extracting features from ECG signals to create an encryption scheme. The results demonstrated the capability to extract features into vector forms using time domain, frequency domain, and time–frequency domains. The advantage of time-domain approaches is their simplicity, which is based on statistical measures such as mean and variance. Again, this suggests less computation in signal analysis. Furthermore, it is effective for stationary signal analysis due to the statistical properties that do not change over time [58]. The advantage of the frequency domain is that it is more applicable for non-stationary signals due to the changing frequency over time. Again, it is more useful for processing more compact signals. Furthermore, it helps to identify noise signals and filter the signal to identify the most relevant signals [59]. Whereas, the advantage of time–frequency domain is that it provides a more comprehensive analysis of the signal, in both time and frequency domain features, over time. Again, it shows more patterns and insight into the signal. Bao, Yan [12] provided fusing mechanisms that leverage Variational Mode Decomposition (VMD) and Convolutional Neural Networks (CNNs) for feature extraction toward user identification system development. The VMD model can decompose features

and remove noise that may affect the ECG signal quality. Modes from these decomposed features were derived (Figure 5) after all residual noise had been removed to enable feature extraction. In furtherance to this, the Empirical Mode Decomposition method (EMD) is an approach to enable the ECG signal to be recovered using the IMF to find the highest frequency. The EMD technique is used to assist in understanding the frequency oscillations of heartbeats.

In terms of the time domain, by using the reconstructed signal features, the mean (0.0004), standard deviation (0.0391), skewness (0.1562), and kurtosis (1.2205) were all extracted (Figure 10) from the ECG data. The use of IDFT and DFT further validated the consistency of the conversion as captured in Figures 10 and 11, such that the frequency-domain features are correlated with the back with the time-domain representation features.

With respect to the frequency domain, the mean and spectral entropy were also displayed in Figure 14. The spectral entropy helps quantify the uncertainty that might occur in the power distribution of the signal from different frequency points of view. While high spectral entropy signifies the complexity of frequency distribution, the contrary suggests a more predictable distribution. Moreover, the power distribution is indicative of how power can be dispersed over frequencies [28].

Using metrics of MSE and RMSE to measure variation, Figure 15 shows that there was no deviation between the reconstructed and the recovered signals. Hence, the viability of our methods is demonstrated.

The features of the heartbeat are critical in the process of developing unique bio-keys for encryption; these features are indicated in the inter-beat interval and histogram as illustrated in Figure 17. Metrics about the time and frequency domain were extracted through HRV computation as outlined in Table 1 from these HRV-related features.

In the final analysis, the study utilized the feature extraction methods in this paper to aggregate these metrics into feature vectors to enable the encryption scheme development. Notably, HRV was employed as a simple key-generation approach [8]. Moreover, our approach provides a more robust key generation approach because it leverages the capabilities of more feature extraction approaches to create a more complex feature vector.

Bio-inspired algorithms, which by their nature provide randomness, increase the robustness of the encryption key. The bio-inspired algorithm Kestrel's initial population is randomly generated as potential solutions to be found. This randomized searching enables bits of the fused feature vector to be chosen at random. The concept of half-life, introduced in the Kestrel algorithm, provides an additional layer of randomization, via the light intensity variation in the half-life component, in the formulation of the encryption key.

The selection of parameters in bio-inspired algorithms is crucial for the efficiency and security of the encryption key generation. Tuning the population size of the bio-inspired algorithm optimizes the generation of robust unpredictable keys that enhance the security of encryption systems. Moreover, an improper parameter selection may result in weak keys or longer computation times, which could undermine the effectiveness of an encryption system. Setting an optimal population size can provide an efficient key generation for an encryption algorithm and also ensure security. The trade-off between security and efficiency depends on the computing limitations and the strength of the encryption key [40]. Thus, while a smaller population size may guarantee faster results, it may compromise the security of the generated key. On the other hand, a larger population size provides a more secure encryption key at a high computational cost. Thus, while Table 2 provides the trade-offs on executing time as the measure of efficiency, Chacha20 was efficient.

This simplified encryption key is provided as a parameter for use in the ChaCha20 encryption algorithm while The ChaCha20 algorithm is a symmetric-key algorithm as it ensures that the same key is both used for encryption and decryption in applications that require high speed and security [41]. Our study has provided an encryption scheme that is suitable for high-speed environments and for IoMT devices that can process data quickly but also ensure the security transmission of data using extracted human features. Our study extracts human features from the bio-signals of these IoMT devices to ensure that

these bio-signals can be securely encrypted and transmitted. From a theoretical perspective, this study contributes to the introduction of the unique bio-inspired Kestrel algorithm with its randomized searching and its half-life component, both of which add layers of randomization for a more secure key for ECG signals. In this research, the impact of noise on generated encryption keys and the impact of bio-inspired search parameters on key generation were, respectively, addressed with signal reconstruction and the use of population tuning of the bio-inspired search method.

6. Conclusions

The paper sought to extract features from ECG signals to create an encryption scheme that does not only rely on the time domain, frequency domain, or time–frequency domains. Instead, through the use of the mode decomposition approach, features of an intra-relationship were extracted and statistically validated to help create a fusion feature vector. Through leveraging this vector with the unique features of the bio-inspired Kestrel algorithm, a more robust encryption scheme is provided. Thus, by leveraging the chacha20 encryption algorithm with our feature extraction and key generation approach, we provide an encryption scheme that might be suitable for lightweight devices like IoMT. Future work includes further evaluation of this proposed encryption scheme within the context of IoMT devices in the real-world environment.

Author Contributions: Conceptualization, methodology, writing—original draft preparation, writing—review and editing, I.E.A.; writing—review and editing, supervision, analysis, R.C.M.; writing—review and editing, E.F.; writing—review and editing, W.W.; writing—review and editing, X.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded in part by the National Key R&D Program of China (Grant number: 2023YFE0110200), in part by the National Research Foundation of South Africa (Grant number 151178).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are available upon request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Karimian, N.; Guo, Z.; Tehranipoor, M.; Forte, D. Highly reliable key generation from electrocardiogram (ECG). *IEEE Trans. Biomed. Eng.* **2016**, *64*, 1400–1411. [[CrossRef](#)] [[PubMed](#)]
2. Aziz, S.; Hayat, M.M.; Naqvi, S.Z.H.; Furqan, M.; Khan, M.U.; Zahid, M.Z. Electrocardiography based Biometric Verification System. In Proceedings of the 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 12–13 June 2020.
3. Neri, L.; Oberdier, M.; van Abeelen, K.; Menghini, L.; Tumarkin, E.; Tripathi, H.; Jaipalli, S.; Orro, A.; Paolucci, N.; Gallelli, I.; et al. Electrocardiogram Monitoring Wearable Devices and Artificial-Intelligence-Enabled Diagnostic Capabilities: A Review. *Sensors* **2023**, *23*, 4805. [[CrossRef](#)] [[PubMed](#)]
4. Asim, M.; Akhtar, M.; Faraz, M.; Khan, M.U.; Aziz, S.; Montes, G.A. Pattern Analysis for Biometric Authentication using Electrocardiogram Signal. In Proceedings of the 2023 2nd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (EETECTE), Lahore, Pakistan, 27–29 November 2023.
5. Shuma, M.; Madhumathy, P. Brakerski-Gentry-Vaikuntanathan fully homomorphic encryption cryptography for privacy preserved data access in cloud assisted internet of things services using glow-worm swarm. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4641. [[CrossRef](#)]
6. Lin, Y.; Xie, Z.; Chen, T.; Chen, X.; Wen, H. Image privacy protection scheme based on high-quality reconstruction DCT compression and nonlinear dynamics. *Expert Syst. Appl.* **2024**, *257*, 124891. [[CrossRef](#)]
7. Karpagachelvi, S.; Arthanari, M.; Sivakumar, M. ECG Feature Extraction Techniques—A Survey Approach. (*IJCSIS*) *Int. J. Comput. Sci. Inf. Secur.* **2010**, *8*, 1–5.
8. Pirbhulal, S.; Zhang, H.; Mukhopadhyay, S.C.; Li, C.; Wang, Y.; Li, G.; Wu, W.; Zhang, Y.-T. An Efficient Biometric-Based Algorithm Using Heart Rate Variability for Securing Body Sensor Networks. *Sensors* **2015**, *15*, 15067–15089. [[CrossRef](#)]

9. Kumar, S.; Vaishali, K.; Maiya, G.; Shivashankar, K.N.; Shashikiran, U. Analysis of time-domain indices, frequency domain measures of heart rate variability derived from ECG waveform and pulse-wave-related HRV among overweight individuals: An observational study. *F1000Research* **2023**, *12*, 1229. [[CrossRef](#)]
10. Escribano, P.; Ródenas, J.; García, M.; Arias, M.A.; Hidalgo, V.M.; Calero, S.; Rieta, J.J.; Alcaraz, R. Combination of frequency-and time-domain characteristics of the fibrillatory waves for enhanced prediction of persistent atrial fibrillation recurrence after catheter ablation. *Heliyon* **2024**, *10*, e25295. [[CrossRef](#)]
11. Zhao, L.; Li, J.; Ren, H. Multi domain fusion feature extraction and classification of ECG based on PCA-ICA. In Proceedings of the 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 12–14 June 2020.
12. Bao, Z.; Yan, L.; Wang, M. Multi-feature Fusion ECG Signal Recognition Algorithm Based on VMD. In Proceedings of the 2022 4th International Conference on Natural Language Processing (ICNLP), Xi'an, China, 25–27 March 2022.
13. Bazhutina, A.; Khamzin, S.; Sinitca, A.; Chmelevsky, M.; Zubarev, S.; Budanova, M.; Rainer, W. An Ensemble of Machine Learning Models for Multilabel Classification of Cardiovascular Diseases by ECGs. In Proceedings of the 2023 Computing in Cardiology (CinC), Atlanta, GA, USA, 1–4 October 2023.
14. Buyya, A.; Ogeti, T.; Suhas, G.; Kashapogula, P.; Panigrahy, A.K. Arrhythmias Classification by using STFT-based Spectrograms, Transfer Learning and Concatenation of features. In Proceedings of the 2023 4th International Conference for Emerging Technology (INCET), Belgaum, India, 26–28 May 2023.
15. Choudhary, S.K.; Sandee, B. Real Time Biometric Authentication System Using ECG. In Proceedings of the 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 6–8 July 2023.
16. Choudhary, T.; Das, M.; Sharma, L.N.; Bhuyan, M.K. A Non-Fiducial Noise Robust VMD-based Framework for ECG-based Biometric Recognition. In Proceedings of the 2021 IEEE 18th India Council International Conference (INDICON), Guwahati, India, 19–21 December 2021.
17. Pradhan, B.K.; Neelappu, B.C.; Sivaraman, J.; Kim, D.; Pal, K. A Review on the Applications of Time-Frequency Methods in ECG Analysis. *J. Healthc. Eng.* **2023**, *34*, 3145483. [[CrossRef](#)]
18. Anjitha, P.; Dhanya, K.R.; Sindhu, N.; Jerritta, S. The Untapped Potential of Feature Selection for Emotion Recognition: Literature Review. In Proceedings of the 2020 International Conference on Power, Instrumentation, Control and Computing (PICC), Thrissur, India, 17–19 December 2020.
19. He, W.; Ye, Y.; Pan, T.; Meng, Q.; Li, Y. Emotion Recognition from ECG Signals Contaminated by Motion Artifacts. In Proceedings of the 2021 International Conference on Intelligent Technology and Embedded Systems (ICITES), Chengdu, China, 31 October 2021–2 November 2021.
20. Ihsan, M.F.; Mandala, S.; Pramudyo, M. Study of Feature Extraction Algorithms on Photoplethysmography (PPG) Signals to Detect Coronary Heart Disease. In Proceedings of the 2022 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, 6–7 July 2022.
21. Khan, M.U.; Aziz, S.; Naqvi, S.Z.H.; Zaib, A.; Maqsood, A. Pattern Analysis Towards Human Verification using Photoplethysmograph Signals. In Proceedings of the 2020 International Conference on Emerging Trends in Smart Technologies (ICETST), Karachi, Pakistan, 26–27 March 2020.
22. Omar, N.; Dey, M.; Ullah, M.A. Detection of Myocardial Infarction from ECG Signal Through Combining CNN and Bi-LSTM. In Proceedings of the 2020 11th International Conference on Electrical and Computer Engineering (ICECE), Dhaka, Bangladesh, 17–19 December 2020.
23. Khan, M.U.; Saad, M.; Aziz, S.; Ch, J.M.; Naqvi, S.Z.H.; Qasim, M.A. Electrocardiogram based Gender Classification. In Proceedings of the 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 12–13 June 2020.
24. Mahmud, M.S.; Nayan, M.M.R.; Hasan, S.; Taj, M.N.A. A Deep Ensemble Model with an Efficient Feature for Multi-class Arrhythmia Classification Utilizing 12-Lead ECG Signal. In Proceedings of the 2022 12th International Conference on Electrical and Computer Engineering (ICECE), Dhaka, Bangladesh, 21–23 December 2022.
25. Nijaguna, G.S.; Lal, N.D.; Divakarachari, P.B.; Prado, R.P.d.; Woźniak, M.; Patra, R.K. Feature Selection Using Selective Opposition Based Artificial Rabbits Optimization for Arrhythmia Classification on Internet of Medical Things Environment. *IEEE Access* **2023**, *11*, 100052–100069. [[CrossRef](#)]
26. Chen, L.; Zhang, C.; Gao, X. Speech Signal Analysis of Autistic Children Based on Time-Frequency Domain Distinguishing Feature Extraction. In Proceedings of the 2022 IEEE 34th International Conference on Tools with Artificial Intelligence (ICTAI), Macao, China, 31 October 2022–2 November 2022.
27. Kuznetsov, I.V. Movements Classification Based on Surface Electromyography Using Time-frequency Domain Features. In Proceedings of the 2024 XXVII International Conference on Soft Computing and Measurements (SCM), Saint Petersburg, Russian, 22–24 May 2024.
28. Singh, A.K.; Krishnan, S. ECG signal feature extraction trends in methods and applications. *BioMed. Eng. OnLine* **2023**, *22*, 22. [[CrossRef](#)] [[PubMed](#)]
29. Alyasseri, Z.A.A.; Al-Betar, M.A.; Awadallah, M.A.; Makhadmeh, S.N.; Alomari, O.A.; Abasi, A.K.; Doush, I.A. EEG Feature Fusion for Person Identification Using Efficient Machine Learning Approach. In Proceedings of the 2021 Palestinian International Conference on Information and Communication Technology (PICICT), Gaza, Palestine, 28–29 September 2021.

30. Khushaba, R.N.; Al-Timemy, A.H.; Samuel, O.W.; Scheme, E.J. Myoelectric Control with Fixed Convolution-Based Time-Domain Feature Extraction: Exploring the Spatio-Temporal Interaction. *IEEE Trans. Hum. Mach. Syst.* **2022**, *52*, 1247–1257. [[CrossRef](#)]
31. Khushaba, R.N.; Phinyomark, A.; Al-Timemy, A.H.; Scheme, E. Recursive Multi-Signal Temporal Fusions With Attention Mechanism Improves EMG Feature Extraction. *IEEE Trans. Artif. Intell.* **2020**, *1*, 139–150. [[CrossRef](#)]
32. Jiang, K.; Wang, Z.; Shen, R.; Wang, S.; Liu, Y.; Feng, Y.; Lisun, X.; Li, Z. A Neurological Recovery Prediction Algorithm Based on Multi-Feature Extraction and Bagging Aggregation. In Proceedings of the 2023 Computing in Cardiology (CinC), Atlanta, GA, USA, 1–4 October 2023.
33. Kherdekar, V.A.; Naik, S.A. Feature Fusion Extraction Method for Improvement of Recognition of Continuous Speech: A Feature Fusion Method for Recognition of Continuous Speech. In Proceedings of the 2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 11–12 January 2024.
34. Jain, R.; Garg, V.K. An Efficient Feature Extraction Technique and Novel Normalization Method to Improve EMG Signal Classification. In Proceedings of the 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, UK, 27–29 April 2022.
35. Premkumar, S.; Mohana, J. An efficient method for Secure ECG Feature Based Cryptographic Key Generation. In *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*; Blue Eyes Intelligence Engineering & Sciences Publication: Bhopal, India, 2019.
36. Mathivanan, P.; Ganesh, A.B.; Venkatesan, R. QR code-based ECG signal encryption/decryption algorithm. *Cryptologia* **2019**, *43*, 233–253. [[CrossRef](#)]
37. Karthikeyan, M.J.; Martin Leo Manickam, A. 128-Bit secret key generation using unique ECG Bio-signal for medical data cryptography in lightweight wireless body area networks. *J. Biotechnol.* **2017**, *14*, 257–264.
38. Rahman, M.S.; Khalil, I.; Yi, X. Reversible Biosignal Steganography Approach for Authenticating Biosignals using Extended Binary Golay code. *IEEE J. Biomed. Health Inform.* **2020**, *25*, 35–46. [[CrossRef](#)]
39. Garcia-Baleon, H.A.; Alarcon-Aquino, V.; Starostenko, O. A Wavelet-Based 128-bit Key Generator Using Electrocardiogram Signals. In *2009 52nd IEEE International Midwest Symposium on Circuits and Systems*; IEEE: Piscataway, NJ, USA; pp. 644–647.
40. Radhakrishnan, L.; Jadon, S.; Honnavalli, P.B. Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. *Sensors* **2024**, *24*, 4008. [[CrossRef](#)]
41. KEBANDE, V.R. Extended-Chacha20 Stream Cipher with Enhanced Quarter Round Function. *IEEE Access* **2023**, *18*, 114220–114237. [[CrossRef](#)]
42. Pirbhulal, S.; Zhang, H.; Wu, W.; Mukhopadhyay, S.C.; Zhang, Y.-T. Heart-Beats Based Biometric Random Binary Sequences Generation to Secure Wireless Body Sensor Networks. *IEEE Trans. Biomed. Eng.* **2018**, *65*, 2751–2759. [[CrossRef](#)]
43. Khokher, R.; Singh, R.C. Generation of Security Key using ECG Signal. In Proceedings of the International Conference on Computing, Communication and Automation (ICCCA2015), Greater Noida, India, 15–16 May 2015; pp. 1–6.
44. Viand, A.; Jattke, P.; Hithnawi, A. SoK: Fully Homomorphic Encryption Compilers. In Proceedings of the 2021 IEEE Symposium Conf. on Security and Privacy (SP), IEEE Computer Society, San Francisco, CA, USA, 24–27 May 2021; pp. 1092–1108.
45. Moosavi, S.R.; Nigussie, E.; Virtanen, S.; Isoaho, J. Cryptographic Key Generation Using ECG Signal. In Proceedings of the 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017; pp. 1–8.
46. Hwang, H.B.; Lee, J.; Kwon, H.; Chung, B.; Lee, J.; Kim, Y. Preliminary Study of Novel Bio-Crypto Key Generation Using Clustering-Based Binarization of ECG Features. *Sensors* **2024**, *24*, 1556. [[CrossRef](#)]
47. Karthikeyan, M.; Manickam, J.M.L. ECG-signal based secret key generation (ESKG) scheme for WBAN and hardware implementation. *Wirel. Pers. Commun.* **2019**, *106*, 2037–2052. [[CrossRef](#)]
48. Gonzalez-Manizano, L.; Fuentes, J.M.D.; Peris-Lopez, P.; Camara, C. Encryption by Heart (EbH)-using ECG for time-invariant symmetric key generation. *Future Gener. Comput. Syst.* **2017**, *77*, 136–148. [[CrossRef](#)]
49. Hernández-Álvarez, L.; Barbierato, E.; Caputo, S.; Fuentes, J.M.d.; González-Manzano, L.; Encinas, L.H.; Mucchi, L. KeyEncoder: A secure and usable EEG-based cryptographic key generation mechanism. *Pattern Recognit. Lett.* **2023**, *173*, 1–9. [[CrossRef](#)]
50. Shaikh, M.U.; Adnan, W.A.W.; Ahmad, S.A. Secured electrocardiograph (ECG) signal using partially homomorphic encryption technique-RSA algorithm. *Pertanika J. Sci. Technol.* **2020**, *28*, 231–242. [[CrossRef](#)]
51. Ahmed, A.A.A.; Madboly, M.M.; Guirguis, S.K. Securing data transmission and privacy perserving using fully homomorphic encryption. *Int. J. Intell. Eng. Syst.* **2023**, *16*, 2023.
52. Shaikh, M.U.; Adnan, W.A.W.; Ahmad, S.A. Sensitivity and positive prediction of secured electrocardiograph (ECG) transmission using fully homomorphic encryption technique (FHE). In Proceedings of the 2020 IEEE-EMBS Conference of Biomedical Engineering and Sciences (IECBES), Langkawi Island, Malaysia, 1–3 March 2021; pp. 292–297.
53. Madhloom, J.K.; Ghani, M.K.A.; Baharon, M.R. ECG encryption enhancement technique with multiple layers of AES and DNA computing. *Intell. Autom. Soft Comput.* **2021**, *28*, 493–512. [[CrossRef](#)]
54. Premkumar, S.; Mohana, J. A novel ECG based encryption algorithm for securing patient confidential information. *Int. J. Electr. Eng. Technol. (IJEET)* **2020**, *11*, 35–43.

55. Agbehadji, I.E.; Abayomi, A.; Bui, K.-H.N.; Millham, R.C.; Freeman, E. Kestrel-based Search Algorithm (KSA) for parameter tuning unto Long Short Term Memory (LSTM) Network for feature selection in classification of high-dimensional bioinformatics datasets. In Proceedings of the Federated Conference on Computer Science and Information Systems, Poznan, Poland, 9–12 September 2018; pp. 15–20.
56. Agbehadji, I.E.; Millham, R.; Fong, S.J.; Hong, H.-J. Nature-Inspired Search Method and Custom Waste Object Detection and Classification Model for Smart Waste Bin. *Sensors* **2022**, *22*, 6176. [[CrossRef](#)]
57. Agbehadji, I.E.; Millham, R.; Fong, S.J.; Hong, H.-J. Integration of Kestrel-based search algorithm with artificial neural network for feature subset selection. *Int. J. Bio-Inspired Comput.* **2019**, *13*, 222–233. [[CrossRef](#)]
58. Wang, W.-K.; Wan, M.; Zhang, W.-H.; Yang, Y. Chatter detection methods in the machining processes: A review. *J. Manuf. Process.* **2022**, *77*, 240–259. [[CrossRef](#)]
59. Jardine, A.K.S.; Lin, D.; Banjevic, D. A review on machinery diagnostics and prognostics implementing condition-based maintenance. *Mech. Syst. Signal Process.* **2006**, *20*, 1483–1510. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.