Taylor & Francis
Taylor & Francis Group

Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/taut20

Secure transmission and monitoring of ECG signals based on chaotic mapping algorithms

G. Rajasree & R. Mathusoothana S. Kumar

To cite this article: G. Rajasree & R. Mathusoothana S. Kumar (2024) Secure transmission and monitoring of ECG signals based on chaotic mapping algorithms, Automatika, 65:3, 957-972, DOI: 10.1080/00051144.2024.2306758

To link to this article: https://doi.org/10.1080/00051144.2024.2306758

Published online: 19 Mar 2024.

AUTOMATIKA
2024, VOL. 65, NO. 3, 957–972
https://doi.org/10.1080/00051144.2024.2306758

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

Secure transmission and monitoring of ECG signals based on chaotic mapping algorithms

G. Rajasree[a] and R. Mathusoothana S. Kumar[b]

[a]Research Scholar, Department of Computer Application, Noorul Islam Centre for Higher Education, Kumarakovil, India; [b]Professor, Department of Information Technology, Noorul Islam Centre for Higher Education, Kumarakovil, India

ABSTRACT

The rapid advancement of digital healthcare and telemedicine has accentuated the need for robust and secure methods of transmitting sensitive medical data, such as electrocardiogram (ECG) signals. This article presents an innovative approach to ECG signal encryption, leveraging the power of chaotic dynamics through the Henon and Baker maps. Chaotic systems have proven to be formidable tools for encryption due to their inherent unpredictability and sensitivity to initial conditions. In this study, we demonstrate the efficacy of Chaotic Henon Map (CHM) and Chaotic Baker Maps (CBM) in encrypting ECG data, ensuring both data privacy and integrity during transmission. Through a detailed exploration of the CHM and CBM, we elucidate their mathematical foundations and unique properties that make them suitable for ECG encryption. The encryption process involves the generation of chaotic keys, which are utilized to scramble the ECG signal in a way that is virtually impossible to decipher without the correct decryption keys. We also discuss the security features of this encryption method, including resistance against common cryptographic attacks. The results of our experiments demonstrate the robustness of this encryption technique in safeguarding sensitive medical information, making it a valuable addition to the toolkit of secure ECG data transmission methods.

ARTICLE HISTORY
Received 26 September 2023
Accepted 2 January 2024

KEYWORDS
ECG encryption; Chaotic Henon map; Chaotic Baker map; medical data security; telemedicine; data privacy

1. Introduction

In an era defined by the exponential growth of digital healthcare and the ubiquitous adoption of telemedicine, the safe and confidential transmission of sensitive medical data is a paramount concern. Among the vast array of medical records and diagnostic information, the Electrocardiogram (ECG) stands as a critical component, providing vital insights into a patient's cardiac health. As this invaluable data becomes increasingly digitized and transmitted across networks, the imperative for robust security measures has never been clearer. This article embarks on a journey into the realm of advanced data encryption, proposing an innovative approach that harnesses the power of chaos in the form of Chaotic Logistic Map (CLM), Chaotic Henon Map (CHM) and Chaotic Baker Map (CBM) to fortify the security of ECG data.

The healthcare industry has witnessed an extraordinary transformation in recent years, driven by technological advancements that are reshaping how medical services are delivered and patient data is managed. This digital revolution has ushered in the era of electronic health records (EHRs), telemedicine, and the widespread integration of medical devices with digital networks. In this context, the Electrocardiogram (ECG), a fundamental diagnostic tool for assessing cardiac health, has assumed a pivotal role. The proliferation of digital healthcare has revolutionized the patient-provider relationship. Telemedicine, in particular, has emerged as a cornerstone of modern healthcare, enabling patients to access medical consultations remotely. This has been especially crucial in improving healthcare accessibility, particularly in remote or underserved areas, and during health crises such as the COVID-19 pandemic. However, with these digital advancements comes an inherent challenge: ensuring the security and privacy of sensitive medical data, including ECG signals, during transmission. ECG is instrumental in diagnosing cardiac conditions, assessing the impact of medications, and monitoring the overall health of patients.

Traditionally, ECG data was captured on paper, but the digital age has witnessed a transition to electronic ECG records, which can be transmitted and accessed remotely. While digital ECG records have made healthcare more efficient and convenient, they have also introduced vulnerabilities. ECG data, like all forms of electronic medical data, is susceptible to unauthorized

CONTACT G. Rajasree ✉ rajasreeg.ca@rediffmail.com Department of Computer Application, Noorul Islam Centre for Higher Education, Kumarakovil, K.K. District, 629180, India

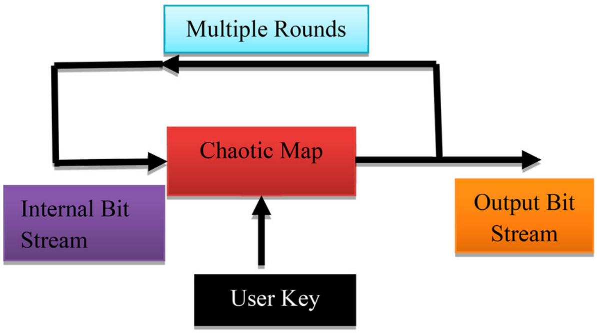


Figure 1. Chaotic map based signal encryption.

access, interception, and tampering during transmission. This poses significant risks, including patient privacy breaches, identity theft, and even the potential for medical fraud and misdiagnoses. Consequently, securing ECG data has become paramount for healthcare providers and institutions.

Encryption has emerged as the cornerstone of data security in the digital age. It involves encoding data in a manner that renders it unintelligible to unauthorized users, ensuring its confidentiality and integrity during transmission. While traditional encryption methods like RSA and AES have been effective, the evolving landscape of cyber threats necessitates innovations that can provide robust security against increasingly sophisticated attacks. As healthcare data, including ECG signals, continues to traverse digital networks, the need for advanced encryption solutions becomes more apparent. It is in this evolving landscape that CHM and CBM, known for their unpredictability and sensitivity to initial conditions, offer a promising avenue to fortify the security of ECG data and safeguard patient privacy. In the following sections, we will delve deeper into the principles of these chaotic systems and their application in ECG data encryption, exploring the potential of chaos in securing our most vital medical information. The general work flow of chaotic map-based encryption system is depicted in Figure 1.

In the realm of data security, where adversaries constantly seek innovative ways to compromise sensitive information, traditional encryption methods have long held their ground. Techniques like RSA and AES have been the bedrock of secure communication for years, relying on complex algorithms and mathematical principles to protect data. However, as the digital landscape evolves, so do the threats. To stay ahead of sophisticated adversaries, security experts have turned to unconventional solutions, including the use of chaotic systems. Chaotic systems, rooted in the field of dynamical systems and nonlinear mathematics, have garnered significant attention in the world of cryptography. What makes these systems particularly fascinating is their intrinsic unpredictability and sensitivity to initial conditions. Unlike traditional cryptographic algorithms, which rely on mathematical rigour and computational complexity, chaotic systems harness the apparent randomness that arises from their dynamics. It is this very unpredictability that adds an extra layer of security to data encryption. Attempting to decipher a message encrypted using chaotic systems becomes akin to trying to predict the exact path of a hurricane – seemingly impossible due to the inherent sensitivity to initial conditions.

The CHM is a nonlinear, discrete-time dynamic system that exhibits chaotic behaviour. Named after its creator Michel Henon, this map is governed by a set of simple mathematical equations. Despite its apparent simplicity, the Henon Map generates intricate, seemingly random patterns when iterated over time. These patterns serve as the foundation for the encryption process. The CHM introduces a level of unpredictability that is challenging to replicate or predict. Similarly, the Chaotic Baker Map is another nonlinear, chaotic dynamic system that has gained prominence in encryption applications. Named after its resemblance to the process of folding dough while baking, this map exhibits complex, chaotic behaviour. The transformations generated by the CBM introduce a high degree of disorder into the data, making it resistant to conventional decryption techniques. By leveraging the chaotic behaviour of the CBM, ECG data can be transformed into a form that appears random and indecipherable. This transformation is reversible only to those who possess the correct decryption keys, making it a formidable tool in securing ECG data during transmission.

One of the significant advantages of chaotic systems in encryption is their resistance to cryptanalysis. Conventional encryption methods can be vulnerable to attacks based on mathematical principles or computational power. In contrast, chaotic systems rely on the inherent complexity of their dynamics, making them less susceptible to brute-force or algorithmic attacks. Decrypting data encrypted with CHM and CBM requires knowledge of the precise initial conditions and parameters used in the encryption process. Even slight deviations in these values can result in entirely different encryption outcomes, further enhancing the security of the encrypted data. This research seeks to explore the utilization of CHM and CBM as formidable tools in the encryption of ECG data. Our objectives encompass the following. Unveil the mathematical foundations and principles underpinning CHM and CBM. Demonstrate the efficacy of these chaotic systems in the encryption of ECG signals. Discuss the potential impact of this innovation on the broader landscape of telemedicine and digital healthcare security.

2. Literature survey

Algarni et al. [1] propose an innovative approach to ECG data encryption within healthcare IoT contexts, leveraging machine learning techniques. Their study focuses on enhancing data privacy and security, particularly in resource-constrained IoT devices. By harnessing machine learning models, they achieve efficient and effective ECG data protection while accommodating the unique challenges of IoT environments. Hameed et al. [2] explore the integration of blockchain technology to enhance ECG data security and sharing in healthcare settings. Their research centres on ensuring data integrity, confidentiality, and access control in a distributed and immutable ledger. Zhai et al. [3] investigate the application of secure multi-party computation (SMPC) techniques to safeguard ECG data privacy within cloud-based health platforms. Their study emphasizes collaborative data analysis while preserving individual privacy. By leveraging SMPC, they enable multiple parties to jointly compute results without revealing sensitive ECG data, making it a promising approach for secure data sharing and analysis in the cloud.

Liu et al. [4] explore the use of homomorphic encryption to protect ECG data privacy in edge computing environments. Their research centres on secure data processing and storage at the edge while maintaining data confidentiality. By applying homomorphic encryption, they enable computations on encrypted ECG data without exposing the raw data, facilitating secure and privacy-preserving edge computing applications in healthcare. Harinee et al. [5] propose a federated learning approach to preserve ECG data privacy during analysis. Their research enables collaborative model training across distributed data sources without centralizing sensitive ECG data. By employing federated learning techniques, they address privacy concerns while deriving insights from ECG data, making it a promising solution for secure and collaborative healthcare analytics. Madhloom et al. [6] investigate the application of differential privacy techniques to securely share ECG data within healthcare networks. Their study prioritizes individual privacy while enabling data sharing for research and analysis. By implementing differential privacy mechanisms, they provide a robust solution for balancing data utility with privacy preservation in healthcare data sharing.

Soni et al. [7] focused on privacy-preserving ECG data aggregation methods within wearable health devices. Their research aims to ensure that aggregated ECG data remains confidential and secure during transmission and processing. By developing effective aggregation techniques, they enable real-time monitoring without compromising individual data privacy in wearable health applications. Abdulbaqi et al. [8] explore secure multiparty computation techniques in fog computing environments to enable collaborative ECG data analysis while maintaining data security. Their research focuses on distributed and privacy-preserving computations in fog networks. By leveraging secure multiparty computation, they facilitate secure and efficient ECG data analysis in fog computing scenarios. Xu et al. [9] investigate privacy-preserving techniques for outsourcing ECG data to the cloud, ensuring data confidentiality even when stored off-site. Their research addresses concerns related to cloud-based healthcare data storage and processing, prioritizing the protection of sensitive ECG data while benefiting from cloud computing resources.

Qiu et al. [10] propose a secure ECG data transmission method using homomorphic encryption in telemedicine applications. Their research focuses on preserving data confidentiality during remote monitoring and telehealth consultations. By applying homomorphic encryption techniques, they facilitate secure ECG data transmission, ensuring patient privacy in telemedicine scenarios. Huang et al. [11] explore the use of secure multiparty computation (SMPC) for privacy-preserving ECG data sharing in mobile health applications. Their research focuses on enabling collaborative analysis while ensuring the confidentiality of sensitive ECG data. By employing SMPC, they provide a practical solution for secure and efficient data sharing in the mobile health context. Shaikh et al. [12] propose an end-to-end encryption approach for ECG data in remote patient monitoring systems. Their study emphasizes the need for comprehensive data security throughout the data lifecycle. By implementing end-to-end encryption, they ensure that ECG data remains protected from the point of acquisition to analysis and storage.

Tamilarasi et al. [13] investigate the use of federated learning to preserve privacy while analyzing ECG data within distributed healthcare networks. Their research addresses the challenges of collaborative data analysis in a privacy-sensitive environment. By adopting federated learning techniques, they enable multiple healthcare institutions to train machine learning models collectively without sharing raw ECG data. Patel et al. [14] focus on secure ECG data aggregation within IoT-based health monitoring systems. Their research aims to ensure that ECG data remains confidential during the aggregation process. By developing secure aggregation mechanisms, they enable efficient data processing and analysis while maintaining the privacy of individual ECG data sources. Premkumar et al. [15] investigate privacy-preserving techniques for storing ECG data in cloud-based healthcare platforms. Their research addresses concerns related to data security and access control in the cloud. By implementing privacy-preserving storage mechanisms, they enable healthcare providers to securely leverage cloud resources for ECG data management. Bhardwaj et al. [16] explore the application of differential privacy to enable ECG data sharing in medical research collaborations. Their research focuses on preserving individual privacy while facilitating collaborative research efforts. By employing differential privacy techniques, they strike a balance between data utility and privacy preservation in medical research.

Murillo et al. [17] investigate privacy-preserving techniques for ECG data analysis in edge-cloud environments. Their research addresses the challenges of secure and efficient data analysis in decentralized computing environments. By implementing privacy-preserving analytics, they ensure that sensitive ECG data remains confidential while benefiting from edge and cloud resources. Ahmed et al. [18] propose secure methods for ECG data transmission in wearable healthcare devices. Their research emphasizes the need for data security during real-time monitoring. By implementing secure transmission protocols, they enable wearable devices to transmit ECG data while safeguarding it from unauthorized access and interception. (Figure 2)

Hameed et al. [19] present secure methods for ECG data storage and retrieval within personal health records (PHRs). Their research focuses on ensuring data privacy while enabling individuals to access and manage their health data. By implementing secure storage and retrieval mechanisms, they empower patients to control their ECG data securely within PHRs. Bhardwaj et al. [20] propose privacy-enhanced methods for ECG data sharing in e-health systems. Their research addresses the challenge of balancing data sharing for clinical collaboration with patient privacy concerns. By implementing privacy-enhanced sharing protocols, they enable secure and controlled access to ECG data in e-health contexts. The classification of spatial signal encryption schemes is illustrated in Figure 3.

The literature review on ECG encryption reveals a diverse landscape of methods and technologies employed to secure Electrocardiogram (ECG) data. Traditional cryptographic techniques, such as AES and RSA, provide strong security but may encounter performance challenges. Emerging approaches, including Chaotic Map-Based Encryption, Homomorphic Encryption, Federated Learning, Blockchain, Differential Privacy, and Secure Multiparty Computation, address these challenges while preserving data privacy and integrity. The choice of encryption method should align with specific healthcare contexts and system requirements. These methods collectively contribute to protecting ECG data, ensuring its confidentiality and secure transmission in the healthcare ecosystem.

3. Methodology

In this section, we explore the intricate methodology designed to enhance the security of Electrocardiogram (ECG) data through the utilization of Chaotic Henon Map (CHM) and Chaotic Baker Map (CBM). Safeguarding ECG data is of utmost importance in the healthcare sector, where sensitive patient information must be protected while enabling critical diagnostic and research activities. Our methodology centres on the selection of CHM and CBM as encryption mechanisms, leveraging their distinctive chaotic properties and mathematical characteristics. We will elucidate the fundamental principles and algorithms that govern these chaotic maps and how they are adapted to encrypt ECG data effectively. Additionally, the methodology section will provide insights into data preprocessing, key generation, encryption, and decryption procedures, offering a comprehensive grasp of the steps involved in securing ECG data using these chaotic systems. This methodological framework not only assures the confidentiality and integrity of ECG data but also underscores the potential of chaotic systems in fortifying data security within the healthcare sector.

3.1. ECG cryptography using chaotic Henon map

In the Henon map-based mixing process, the common practice involves an arrangement method [22]. The derived keys are primarily positioned in the first column of a 2D array. Sorting in ascending order causes corresponding adjustments in the sorting of next column, which result in a randomized arrangement employed for signal shuffling. However, it's important to note that this approach necessitates the introduction of an additional data dimension that is twice the size of the signl, thereby doubling the required RAM space and significantly increasing computational demands, consequently leading to a reduction in speed of encryption. The state parameters (x, y) maintain continuity in the time domain [23]. The keys are transformed into one-byte representations through a modulo operation (MOD). This, in turn, results in a substantial increase in arithmetic operations. We present an innovative transformation-exchange approach rooted in the CHM for generating a series of confidential keys. This method leverages the chaotic properties of the Henon map, which generates random floating-point values, to facilitate the transformation and exchange procedures applied to the ECG signal. The scheme we propose encompasses three primary phases: key generation, encryption, and decryption. The equation governing the 2-D Henon map is expressed as follows:

$$X_{i+1} = 1 + Y_i - aX_i^2 \tag{1}$$

$$Y_{i+1} = 1 - bX_i, \quad i = 0,\ 1,\ 2,\ \ldots\ldots. \tag{2}$$

In this context, $\mathbf{X}_\mathrm{i}$ and Y_i are state during i-th iteration. The control variables are indicated by "a" and "b". When "a" is set to 1.4 and "b" to 0.3, the chaotic behaviour of the system emerges [24]. Figure 4 presents a visualization of the dynamic characteristics of the CHM for reference. It provides a comprehensive depiction of space (a, b), partitioned into distinct regions corresponding to diverse asymptotic dynamics, including

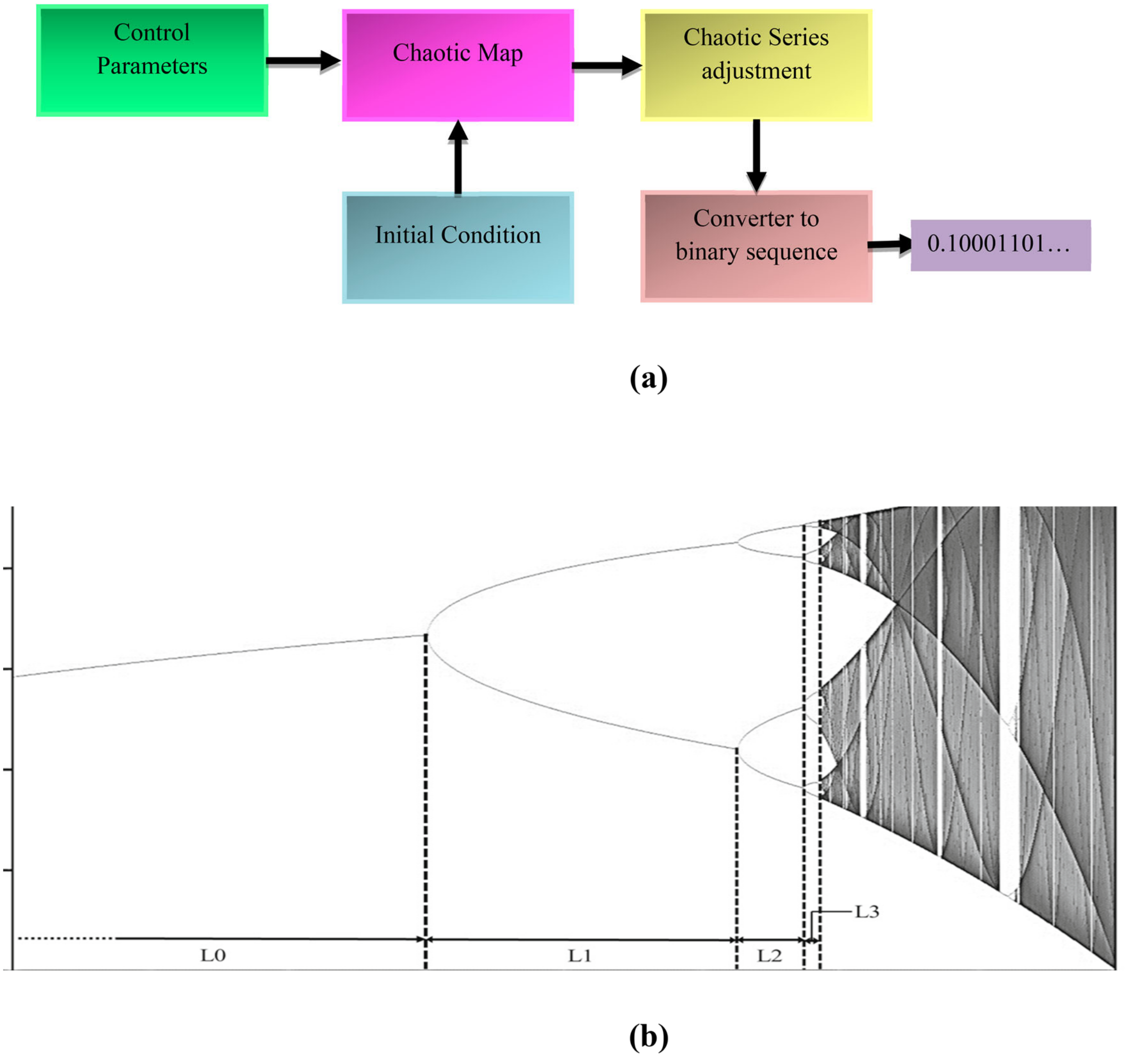


Figure 2. Chaotic encryption (a) Generation of Pseudo random sequence, (b) Sample chaotic map.

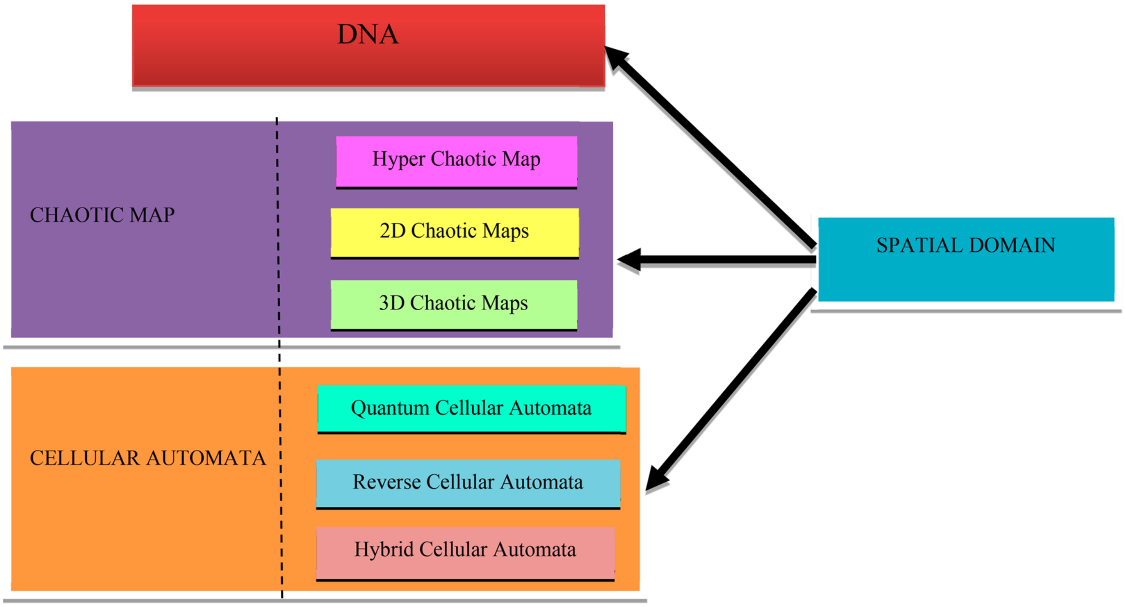


Figure 3. Categories of spatial signal encryption schemes.

Algorithm 1: CHM Based ECG Encryption

```
Input: ECG signal Es from the patient, Primary keys X0, Y0, a, b, based
    on biometric features.
Output: Encrypted ECG signal En.
Step 1: Xkeys and Ykeys are Generated for size ((M x N) + 100) by
    utilizing (X0, Y0, a, b) Henon map.
Step 2: Discard initial 100 values from Xkeys and Ykeys
Step 3: X keys and Ykeys are converted into integers.
Step 4: Xkeys = MOD (Xkeys, N × M)
Step 5: For i = 1 to length (Y), convert Y[i] into Mid [7] array of bytes.
Step 6: Reshape (Es) into one dimension array.
Step 7: Swap Es [i] with Es [X key[i]], if i = 1 to Es
Step 8: En[i] = Es[i] ⊕ K[i], if i = 1 to Es
Step 9: En is reshaped into 2D array.
```

Algorithm 2: CHM Based ECG Decryption

```
Input: Encrypted ECG signal En, Primary keys X0, Y0, a, b, based on
    biometric features.
Output: Decrypted ECG signal Dn.
Step 1: Xkeys and Ykeys are Generated for size ((M x N) + 100) by
    utilizing (X0, Y0, a, b) Henon map.
Step 2: Discard initial 100 values from Xkeys and Ykeys
Step 3: X keys and Ykeys are converted into integers.
Step 4: Xkeys = MOD (Xkeys, N × M)
Step 5: For i = 1 to length (Y), convert Y[i] into Mid [7] array of bytes.
Step 6: Reshape (En) into 1D array.
Step 7: Dn[i] = En[i] ⊕ K[i], if i = 1 to Es
Step 8: Swap Dn[i] with Dn [X key[i]], if i = 1 to Dn.
Step 9: Reshape size of (Dn) into 2D array.
```

fixed-point solutions (represented in black), periodic solutions (in blue), chaotic strange attractors (in red), and unbounded solutions (in white).

In this work, the 2D CHM plays a pivotal role in generating key streams for executing transformation and exchange operations on the ECG signal. The process incorporates initial conditions denoted as (X_0 and Y_0) and control parameters (a, b). Consequently, the number of keys generated aligns with the dimensions of the ECG data, specifically (M x N). To facilitate further operations, the output key stream undergoes conversion from fractional to integer values utilizing the following Equation:

$$S_i = |S_i \times 10^{15}| \tag{3}$$

The generated key stream, denoted as "Si", undergoes a normalization process within the key set (X), ensuring it falls within the range of 0 ... 255 through the application of a modulo operation (MOD). Bytes corresponding to indexes 2, 4, and 5 exhibit maximum entropy values and feature a uniform histogram distribution, rendering them particularly suitable for encryption purposes. The key set (X) is then employed to perform pixel shuffling through an exchange technique. During each iteration, two values are exchanged, resulting in a total of (2 x M x N) exchange operations. This approach enhances the randomness and efficiency of the encryption process within the CHM, as illustrated in Figure 5.

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

Decryption can be done by performing the reverse operation on the encrypted signal with the key. The process flow of proposed CHM based decryption algorithm is depicted in Figure 6.

In order to decrypt an encrypted ECG signal, the CHM should perform a sequence of steps that are explained in Algorithm 2.

3.2. *ECG cryptography using chaotic baker map*

We introduce an innovative cryptographic approach for ECG data, employing CBM in combination with Dual Random Phase Encoding (DRPE). In this scheme, CBM serves as the means to generate a pseudo-random key using a provided fingerprint image, while DRPE is applied to encrypt the given ECG signal [25]. This proposed method establishes a two-tiered security framework, making it exceptionally challenging to breach and enhancing overall data confidentiality. Chaotic systems, known for their cryptographic properties encompassing confusion, diffusion, and disorder, play a pivotal role in this scheme. These systems exhibit high sensitivity to input variations, where even slight alterations in initial conditions and parameter settings result in substantial differences [26].

Here Discrete map is B(n_1, $n_2, \ldots,$ n_k), and [n_1, $n_2, \ldots,$ n_k] is the secret key denoted as S_{key}. N is the data element count within a single row. Additionally, Ni is, introduced, which is equivalent to the sum of $n_1, n_2, \ldots,$ n_{i-1}. This definition is integral to the movement of data located at (q, z). The equation governing Discretized CBM is expressed as follows:

$$B_{(n_1,\ldots\ldots,n_k)}(z,q) = z \bmod \left(\frac{n_i}{N}\right) + \frac{n_i}{N}(N_i - q) \tag{4}$$

The elements within each of these rectangles are subsequently transformed into a row within the rearranged rectangle. These rectangles are selected sequentially, starting with the upper rectangles and then proceeding to the lower ones. Within each rectangle, the scanning process commences at the bottom-left corner and progresses towards the upper elements. Figure 7 provides an illustrative example of this permutation process applied to an 8 × 8 matrix within the context of the CBM. The discrete variant of the CBM is presented in Figure 8.

DRPE operates by altering the orientation of spectrum in the ECG signal. Its core concept revolves around the insertion of two Random Phase Masks (RPMs). One mas is in the input plane and second on is in the Fourier plane. These RPMs are utilized for the encryption of 2-D ECG signal, rendering it indistinguishable from stationary noise within an optical setup. Importantly, decryption operation necessitates the use of the same RPM employed during encryption [27].

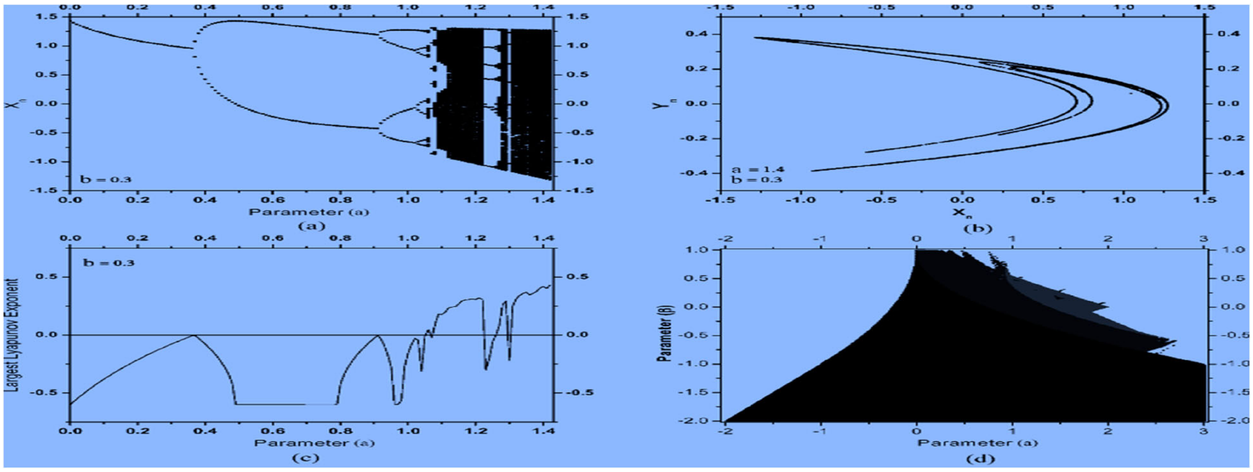


Figure 4. Dynamical behaviour of Henon map.

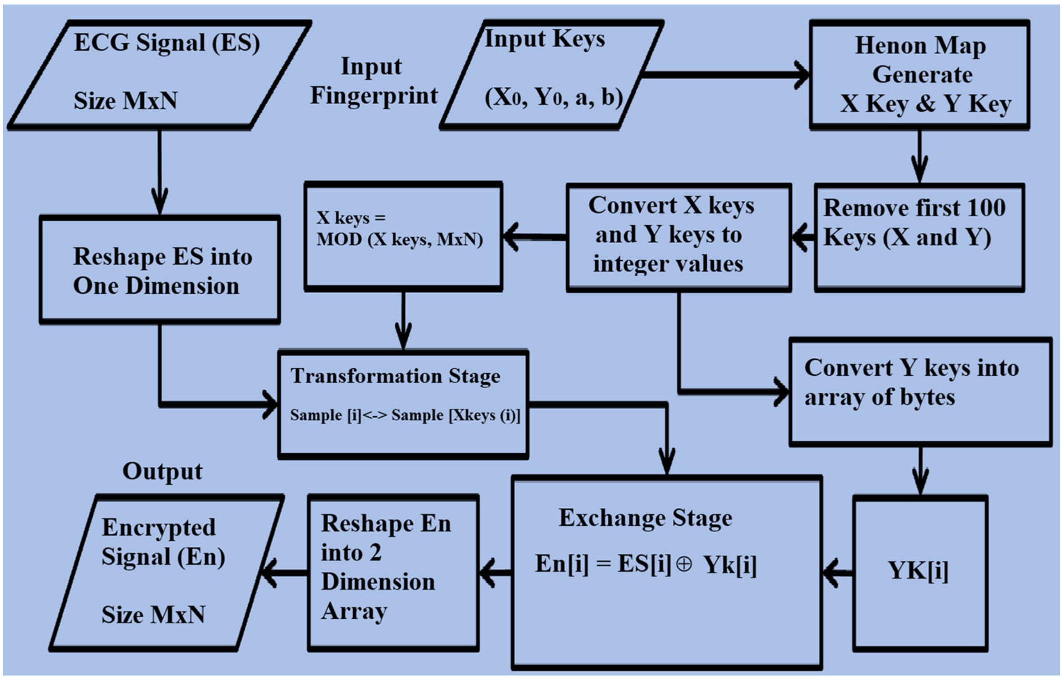

ECG Signal (ES)
Size MxN
Input Fingerprint
Input Keys
(X0, Y0, a, b)
Henon Map Generate X Key & Y Key
Reshape ES into One Dimension
X keys = MOD (X keys, MxN)
Convert X keys and Y keys to integer values
Remove first 100 Keys (X and Y)
Transformation Stage
Sample [i]<-> Sample [Xkeys (i)]
Convert Y keys into array of bytes
Output
Encrypted Signal (En)
Size MxN
Reshape En into 2 Dimension Array
Exchange Stage
En[i] = ES[i]⊕ Yk[i]
YK[i]

Figure 5. Proposed ECG encryption scheme based on chaotic Henon map.

The comprehensive DRPE process is visually illustrated in Figure 9.

The encryption of ECG data involves a series of essential steps. Firstly, the original ECG signal undergoes segmentation and transformation into a 2-D format. Subsequently, the encryption key is concealed through the CBM, and this concealed key is applied to the transformed 2D ECG signal. In the process of clipping, values exceeding 1 are adjusted by subtracting 2, ensuring that all samples fall within the range of −1 and 1. Next, the DRPE technique is applied. Two Fourier Random Phase Masks (RPM) keys, RPM1 and RPM2, are generated. RPM1 is employed to modulate the target ECG signal, while RPM2 is inserted into the ECG signal within the Fourier plane. A second Fourier transformation takes place using a secondary lens, resulting in the encoded ECG signal reverting to its original 2-D spatial format. Subsequently, this 2-D format is reshaped back into a 1-D format, effectively representing the encrypted ECG signal. To complete the encryption process, segments are synthesized. Figure 10 provides a visual representation of the encryption and decryption process flow.

The mask, derived from the confidential key, undergoes a series of transformations to bolster the security of the ECG encryption process. Initially, a predefined number of ones is injected into an initially all-zero block. This modified block then goes through a permutation process using the CBM, resulting in the creation of a mask containing both zeros and ones. Subsequently, the generated output mask is added to every block of the ECG signal. This step is crucial as it conceals specific patterns within the signal, strengthening its resilience against known-plaintext attacks. Given that there are four sub-keys in this context, the following sequence of actions unfolds: initially, four rows of ones are

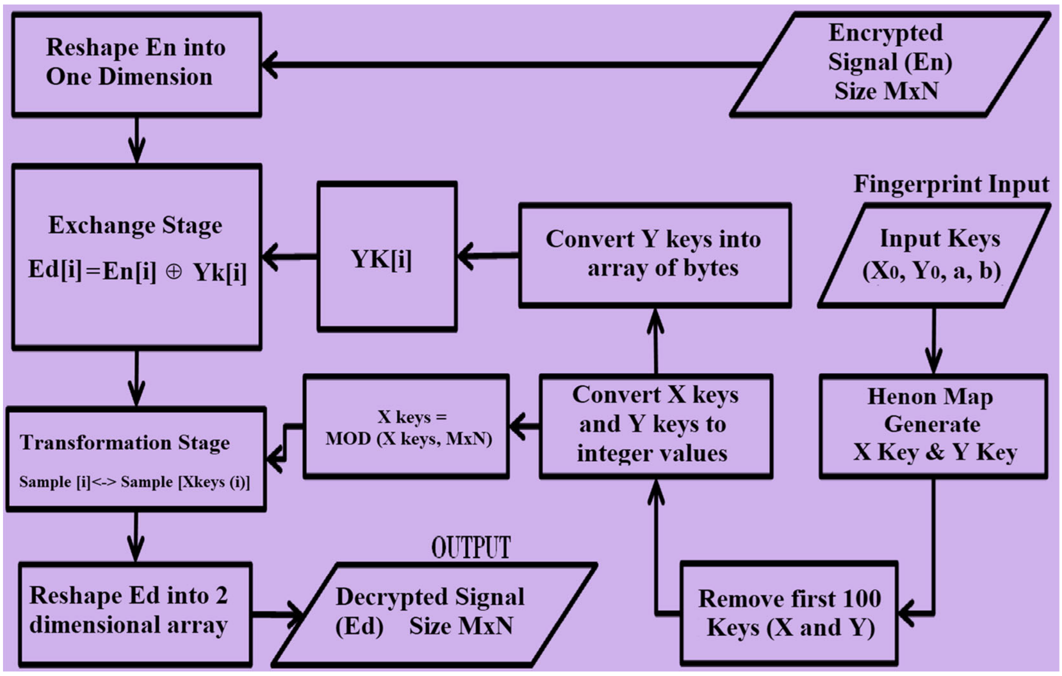

Encrypted Signal (En) Size MxN
Reshape En into One Dimension
Exchange Stage
Ed[i]=En[i] ⊕ Yk[i]
YK[i]
Convert Y keys into array of bytes
Fingerprint Input
Input Keys (X0, Y0, a, b)
Transformation Stage
Sample [i]<-> Sample [Xkeys (i)]
X keys = MOD (X keys, MxN)
Convert X keys and Y keys to integer values
Henon Map Generate X Key & Y Key
OUTPUT
Reshape Ed into 2 dimensional array
Decrypted Signal (Ed) Size MxN
Remove first 100 Keys (X and Y)

Figure 6. Proposed ECG decryption scheme based on chaotic Henon map.

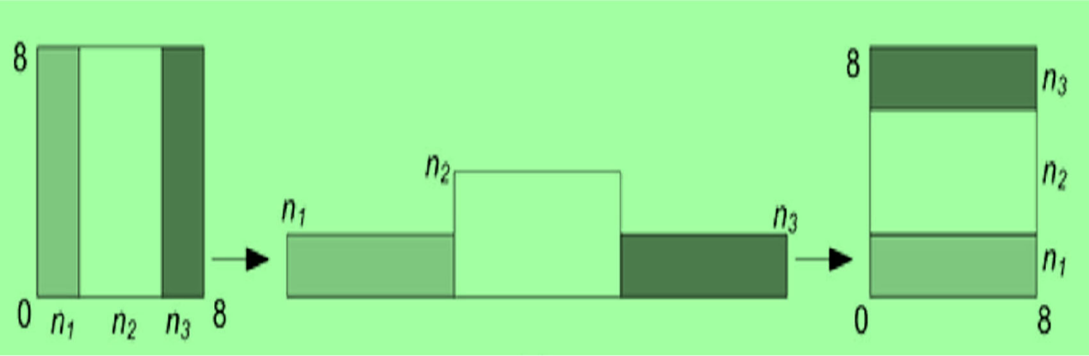
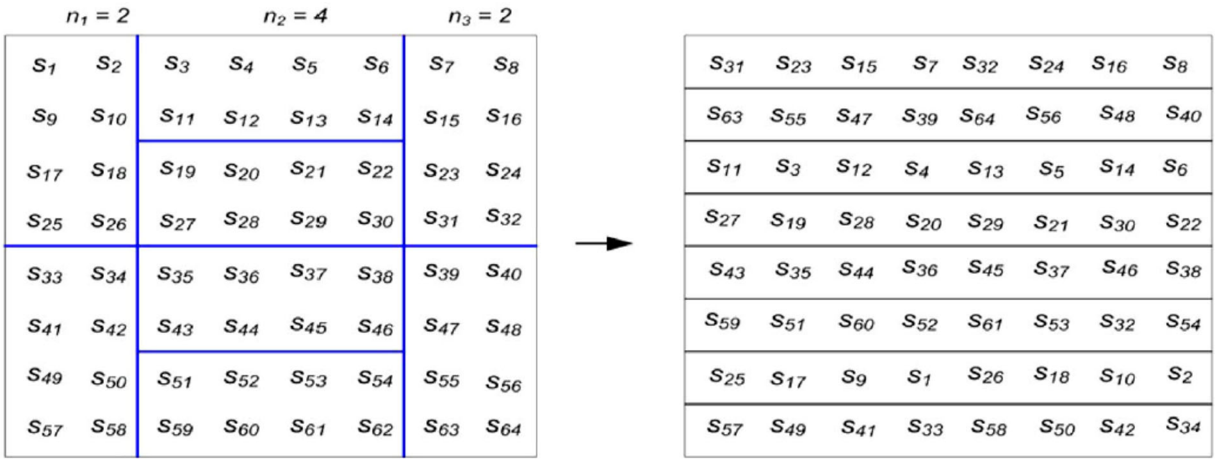


Figure 7. Generalized Chaotic Baker map.

inserted into the 12 × 12 all-zero block, in alignment with the four sub-keys. Subsequently, the block resulting from this step is subjected to permutation using the CBM, ensuring the ones are distributed chaotically throughout the entire block. Finally, the output mask is applied to each block of the ECG signal, followed by a clipping step in the output block. During the clipping process, any values exceeding 1 have 2 subtracted



$n_1 = 2$		$n_2 = 4$				$n_3 = 2$	
S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}
S_{17}	S_{18}	S_{19}	S_{20}	S_{21}	S_{22}	S_{23}	S_{24}
S_{25}	S_{26}	S_{27}	S_{28}	S_{29}	S_{30}	S_{31}	S_{32}
S_{33}	S_{34}	S_{35}	S_{36}	S_{37}	S_{38}	S_{39}	S_{40}
S_{41}	S_{42}	S_{43}	S_{44}	S_{45}	S_{46}	S_{47}	S_{48}
S_{49}	S_{50}	S_{51}	S_{52}	S_{53}	S_{54}	S_{55}	S_{56}
S_{57}	S_{58}	S_{59}	S_{60}	S_{61}	S_{62}	S_{63}	S_{64}

S_{31}	S_{23}	S_{15}	S_7	S_{32}	S_{24}	S_{16}	S_8
S_{63}	S_{55}	S_{47}	S_{39}	S_{64}	S_{56}	S_{48}	S_{40}
S_{11}	S_3	S_{12}	S_4	S_{13}	S_5	S_{14}	S_6
S_{27}	S_{19}	S_{28}	S_{20}	S_{29}	S_{21}	S_{30}	S_{22}
S_{43}	S_{35}	S_{44}	S_{36}	S_{45}	S_{37}	S_{46}	S_{38}
S_{59}	S_{51}	S_{60}	S_{52}	S_{61}	S_{53}	S_{32}	S_{54}
S_{25}	S_{17}	S_9	S_1	S_{26}	S_{18}	S_{10}	S_2
S_{57}	S_{49}	S_{41}	S_{33}	S_{58}	S_{50}	S_{42}	S_{34}

Figure 8. Discretized Chaotic Baker map.

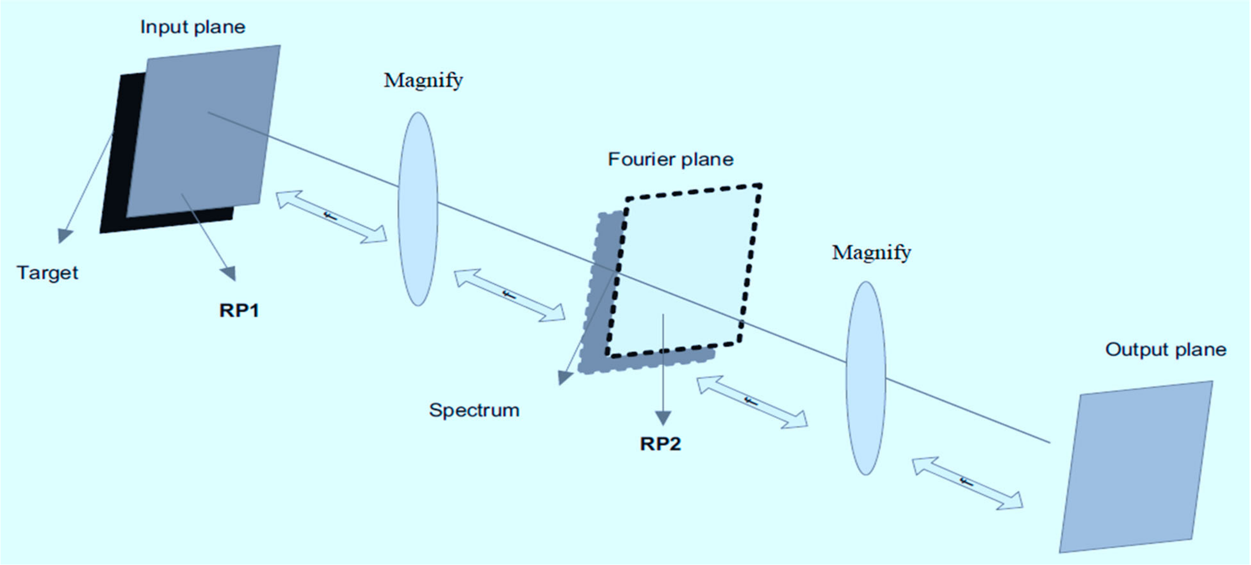


Figure 9. Process of dual random phase encoding.

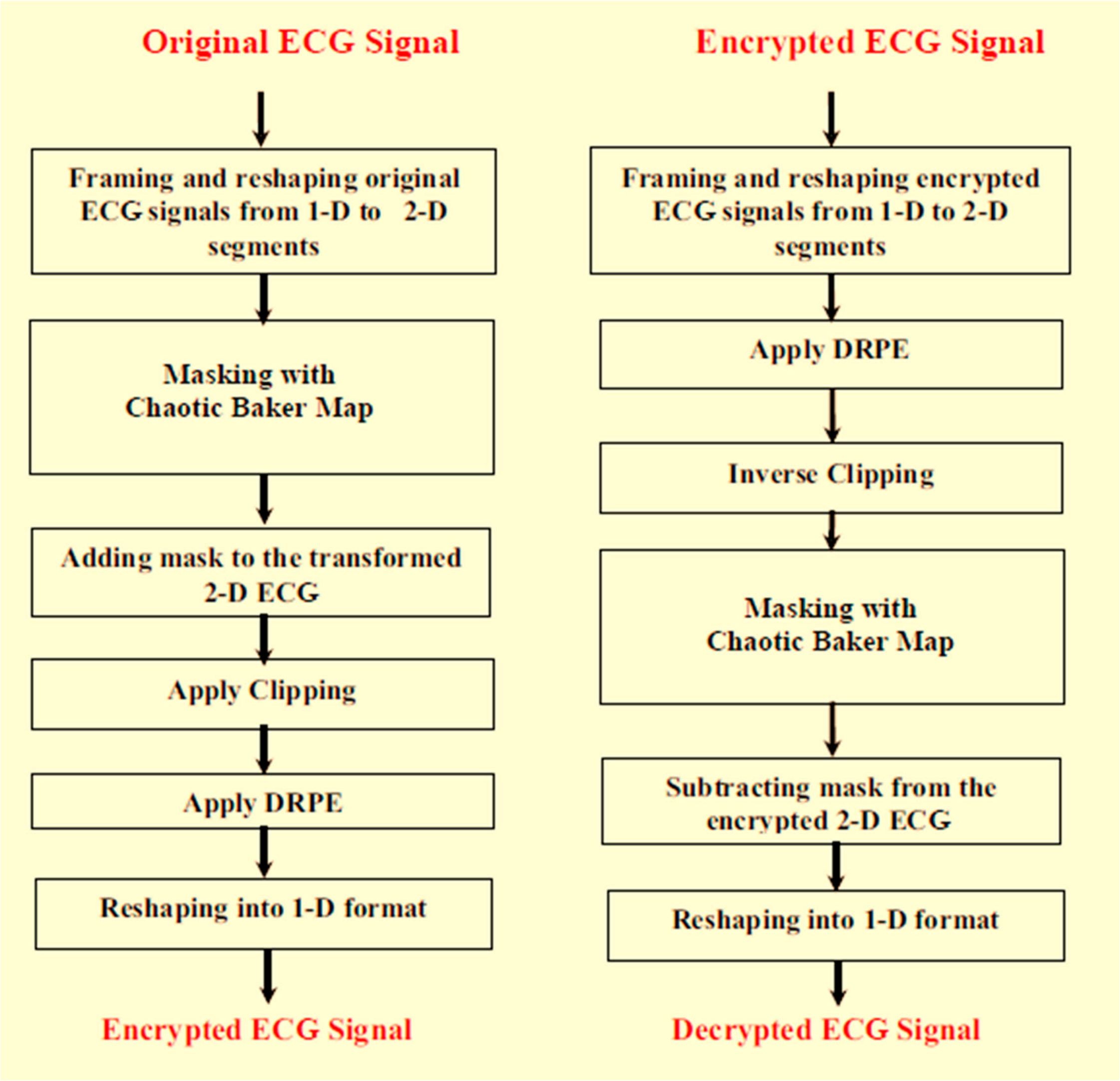

Original ECG Signal
Framing and reshaping original ECG signals from 1-D to 2-D segments
Masking with Chaotic Baker Map
Adding mask to the transformed 2-D ECG
Apply Clipping
Apply DRPE
Reshaping into 1-D format
Encrypted ECG Signal
Encrypted ECG Signal
Framing and reshaping encrypted ECG signals from 1-D to 2-D segments
Apply DRPE
Inverse Clipping
Masking with Chaotic Baker Map
Subtracting mask from the encrypted 2-D ECG
Reshaping into 1-D format
Decrypted ECG Signal

Figure 10. Proposed ECG cryptography scheme based on Chaotic Baker map.

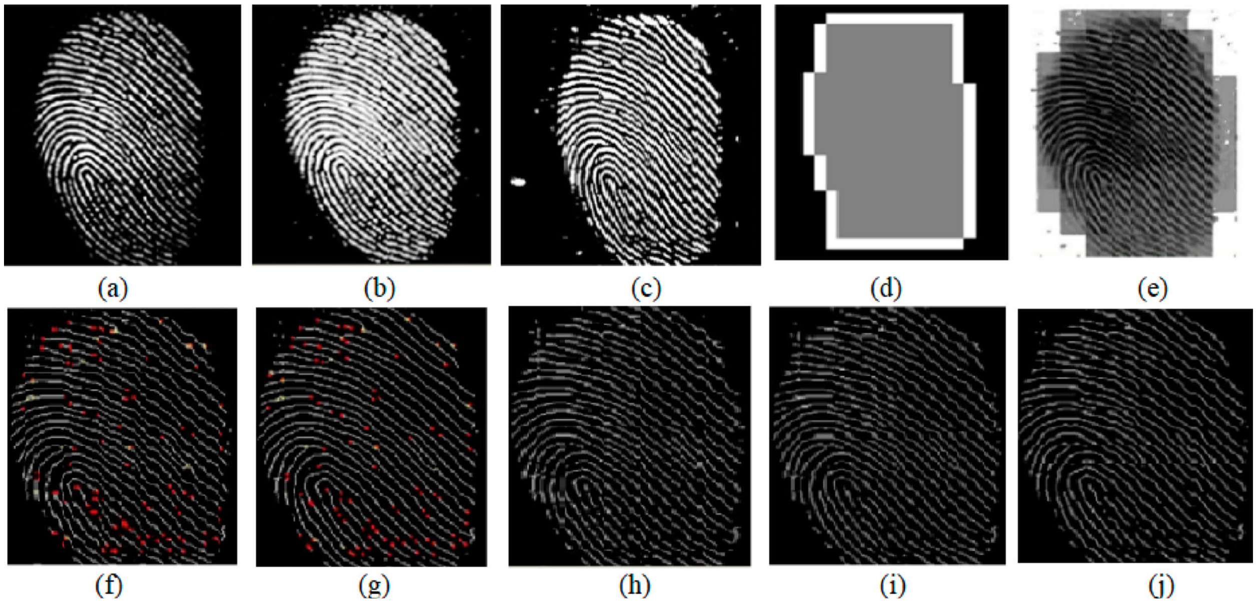


Figure 11. Fingerprint feature extraction results (a) input fingerprint image (b) Enhanced fingerprint (c) Binarized (d) ROI mask (e) ROI (f) Minutiae marked (g) Minutiae removed (h) Ridge bifurcation (i) Ridge ending (j) triples counting branch.

Algorithm 3: Encryption Based on CBM

```
Input: ECG signal Es from the patient, Primary keys based on biometric
    features.
Output: Encrypted ECG signal En.
Step 1: Segment the original ECG Signal Es.
Step 2: Reshape Segments into 2-D Format.
Step 3: Generate Mask Using CBM.
Step 4: Apply Mask to Reshaped 2D ECG Signal.
Step 5: Clip Values to Ensure They Are Between $-1$ and 1.
Step 6: Apply DRPE on the resultant signal.
Step 7: Fourier RPM Key (RPM1) is generated and Multiply with ECG
    Signal.
Step 8: Fourier RPM Key (RPM2) is generated and Insert into ECG Signal
Step 9: Perform Second Fourier Transform by utilizing a second lens
Step 10: Reshape Encoded 2-D ECG Signal into 1-D Format
Step 11: Synthesize Segments to Obtain Encrypted ECG Signal En.
```

Algorithm 4: Decryption Based on CBM

```
Input: Encrypted ECG signal En, Primary keys based on biometric
    features.
Output: Decrypted ECG signal Dn.
Step 1: Segment the encrypted ECG signal.
Step 2: Reshape Segments into 2-D Format.
Step 3: Inverse Clipping: Add 2 to Negative Values Less Than $-1$
Step 4: Masking with CBM (Subtraction).
Step 5: Reshape Encrypted 2-D ECG Signal into 1-D Format
Step 6: Synthesize Segments to Reconstruct ECG Signal
Step 7: Perform Inverse Fourier Transform Using a Second Magnifier.
Step 8: Remove the values introduced by RPM2
Step 9: Perform Inverse Fourier Transform Using the First RPM Key
    (RPM1)
Step 10: Apply DRPE
Step 11: Remove the Mask Applied Earlier
Step 12: Return the decrypted ECG signal Dn.
```

from them, thereby ensuring that all samples within the encrypted ECG data fall within the range of -1 to 1. This not only enhances data integrity but also strengthens security. To encrypt an ECG signal, the CBM should execute a series of steps detailed in Algorithm 3.

The decryption procedure for the ECG signal commences with the segmentation of the encrypted data into distinct segments, which are subsequently transformed into a 2-D format. The encryption key is then concealed using the CBM, and DRPE is applied. Two Fourier RPM keys, RPM1 and RPM2, are generated to facilitate decryption. RPM1 is utilized by multiplying it with the target ECG signal designated for decryption, whereas RPM2 is inserted into the ECG signal within the Fourier plane, thereby introducing the second amendment into the targeted ECG signal. A second Fourier transformation is performed with the assistance of a secondary magnifier, resulting in the encoded ECG signal reverting to its original 2-D spatial format. Subsequently, an inverse clipping operation is carried out by adding a value of 2 to any negative values less than -1 present in the resultant encrypted 2-D ECG signal. The CBM is once again employed for masking, followed by the subtraction of the mask from the encrypted 2-D ECG signal. This process leads to the reshaping of the 2-D ECG data into a 1-D format, effectively representing the original ECG signal. Finally, segments are synthesized, culminating in the reconstruction of the ECG signal and thus completing the decryption process. To decrypt an encrypted ECG signal, the CBM must follow a sequence of steps as detailed in Algorithm 4.

4. Result and discussions

The implementation of the proposed cryptosystems is carried out using MATLAB (R2018a). In this evaluation, both CHM and CBM algorithms are employed for encrypting the initial ECG signals, allowing for the assessment of their effectiveness. For experimentation, the ECG data utilized is sourced from the MIT-BIH

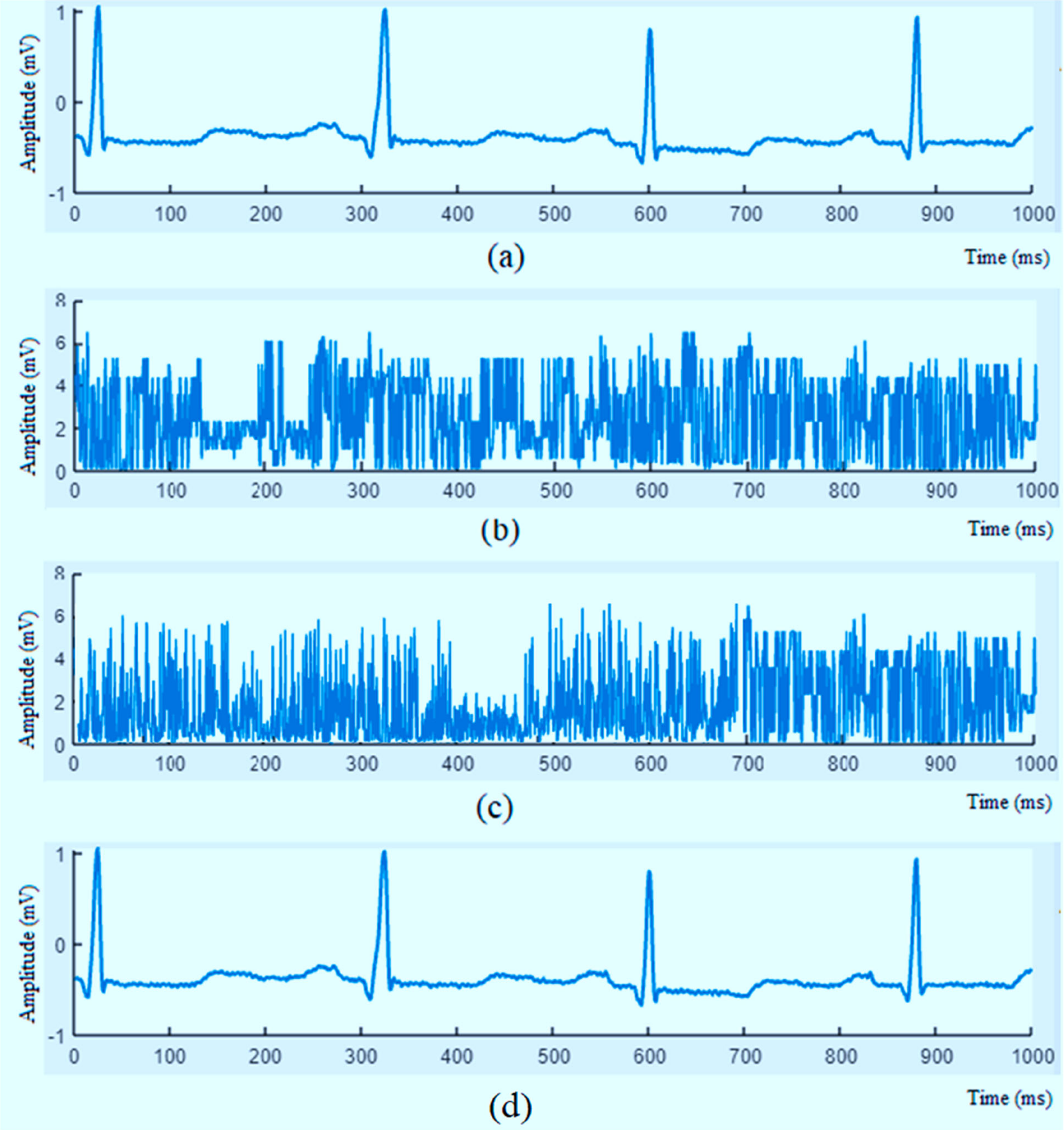


Figure 12. ECG encryption (a) Input ECG (b) Chaotic Henon map encrypted ECG (c) Chaotic Baker map encrypted ECG (c) Decrypted ECG.

dataset of arrhythmia [21]. Each signal within this database spans approximately 30 min and features a sampling frequency rate of around 360 Hz. The dataset encompasses nearly 48 distinct ECG signals. The performance assessment procedure encompasses a comprehensive array of metrics and perspectives to provide a thorough evaluation.

The fingerprint obtained through a fingerprint scanner undergoes a series of steps outlined in the process flow to extract the necessary features required for person identification. This meticulous extraction of fine details from the fingerprint serves to assess its structural attributes, enhancing the efficiency of the matching algorithm. The results derived from the feature extraction process are visually presented in Figure 11. These extracted features are subsequently employed in the generation of keys used for encrypting ECG signals. Figure 12 showcases the original ECG signal alongside the ECG signals encrypted using CHM and CBM algorithms, as well as the decrypted ECG signal. This comparison allows for the observation of differences in amplitude and frequency within the ECG signal as a result of the encryption process.

The evaluation of the proposed encryption system's performance, aimed at enhancing security in the transmission of biomedical signals, is conducted through both qualitative and quantitative assessments. Notably, the execution time of the proposed encryption algorithm demonstrates a decrease, attributed to the reduction in the number of rounds during key

Table 1. Execution time comparison.

	Execution Time for Encryption (ms)					
File Size of ECG (kB)	DES	TDES	AES	CLM	CHM (Proposed)	CBM (Proposed)
16	2.24	2.31	2.21	1.81	1.49	1.13
43	6.31	7.28	6.17	4.31	4.15	3.64
91	8.63	9.42	9.32	7.32	7.02	6.83
156	11.56	12.88	11.45	10.03	9.74	7.42
302	14.69	15.36	16.12	12.15	11.36	10.58
415	17.31	17.94	18.71	14.82	12.93	10.89

generation. However, it's important to note that the execution time is contingent on the size of the ECG file utilized for testing. As the file size increases, the execution time also experiences an increment. To provide a comprehensive understanding, the execution time is meticulously calculated and juxtaposed with the execution time of standard encryption algorithms. The variations in execution time concerning various input file sizes are elaborated upon in Table 1.

The analysis of execution times for different encryption algorithms applied to various file sizes of ECG data provides valuable insights. Notably, the proposed CBM encryption algorithm consistently outperforms its counterparts, demonstrating the shortest execution times across all file sizes. This indicates that CBM is highly efficient in securing ECG data, making it an appealing choice for both real-time transmission and secure storage of ECG information. In contrast, traditional encryption methods such as AES and TDES exhibit moderate execution times that increase as the file sizes grow. While these methods offer reliability, their efficiency diminishes as computational demands increase. CLM falls slightly behind AES and TDES in terms of execution times, while DES, although the fastest among the traditional methods, lags significantly behind CBM in terms of efficiency. CHM falls in between, presenting intermediate execution times. As expected, execution times tend to rise across all algorithms as file size increases. In practical applications, the selection of an encryption algorithm should carefully balance security requirements and computational resources. CBM emerges as a promising solution for efficient ECG data encryption without compromising security, as it offers the shortest execution times across a range of file sizes. Figure 13 provides a visual representation of the variation in execution time with respect to various input file sizes.

The evaluation of a system's resilience against statistical attacks is assessed through histograms, which provide crucial insights into the effectiveness of the encryption process. In this context, it is imperative that the encrypted ECG signals exhibit a uniform distribution, a characteristic that is graphically represented in their histograms. Figure 14 (a and b) showcases an ECG encrypted using the CHM and its corresponding histogram. Similarly, Figure 14 (c and d) displays an ECG encrypted using the CBM alongside its associated histogram. Notably, the histograms of CBM cryptography exhibit uniformity, signifying that the system is robust against statistical attacks. Upon a closer examination of these two histograms, it becomes evident that the amplitudes are evenly distributed across the entire range. The increased amplitude and broader range of the encrypted ECG signals are indicative of the new distribution pattern, reinforcing the notion that the encrypted signals are resistant to potential attacks.

The SSIM is used to assess the original ECG signal and the encrypted ECG for resemblance. Equation 5 is used to compute SSIM. Here μ_x is the mean of x (original) and μ_y is the mean of y (encrypted). δ_x^2 is the variance of x and δ_y^2 is the variance of y. δ_{xy} is the cross-covariance between x and y. c_1 and c_2 are small constants. SSIM indicates the resemblance of signals and it varies between 0 and 1. 0 indicate entirely different and 1 indicates exactly same.

$$SSIM = \frac{(2\mu_x\mu_y + c_1)(2\delta_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\delta_x^2 + \delta_y^2 + c_2)} \tag{5}$$

It is evident that the proposed security system exhibits a higher encryption complexity when compared to existing algorithms. Notably, the CBM encryption system records the lowest SSIM value, standing at 0.032. In contrast, the CHM cryptosystem yields a slightly higher SSIM value of 0.043. This disparity reveals that the CBM encryption introduces a greater degree of dissimilarity in the structure of the encrypted signal when compared to the original ECG signal. The comparison of SSIM values is visually represented in Figure 15, further highlighting the differences in structural resemblance between the encrypted and original ECG signals.

To achieve enhanced encryption quality, it is crucial to attain higher values of both Spectral Distortion (SD) and Log-Likelihood Ratio (LLR). The LLR serves as a metric based on the spatial distance between Linear Prediction Coefficients (LPC) vectors computed from the original and encrypted signals, as delineated in Equation 6. This measure plays a pivotal role in assessing the efficiency of the cryptosystem in conserving the spectral characteristics of the original signal. Higher LLR values signifying superior encryption quality. Here l_x and l_y are the LPCs for original ECG and encrypted ECG respectively. R_x represents autocorrelation matrix of input ECG and R_y represents autocorrelation matrix of encrypted ECG.

$$LLR = \left| \log \left[\frac{l_x R_x l_x^T}{l_y R_y l_y^T} \right] \right| \tag{6}$$

While considering LLR, CBM has an increase of 0.09 as compared to CHM. This indicates that the spatial distance between CBM encrypted ECG and the original ECG is very high. The comparison of SSIM is illustrated in Figure 16.

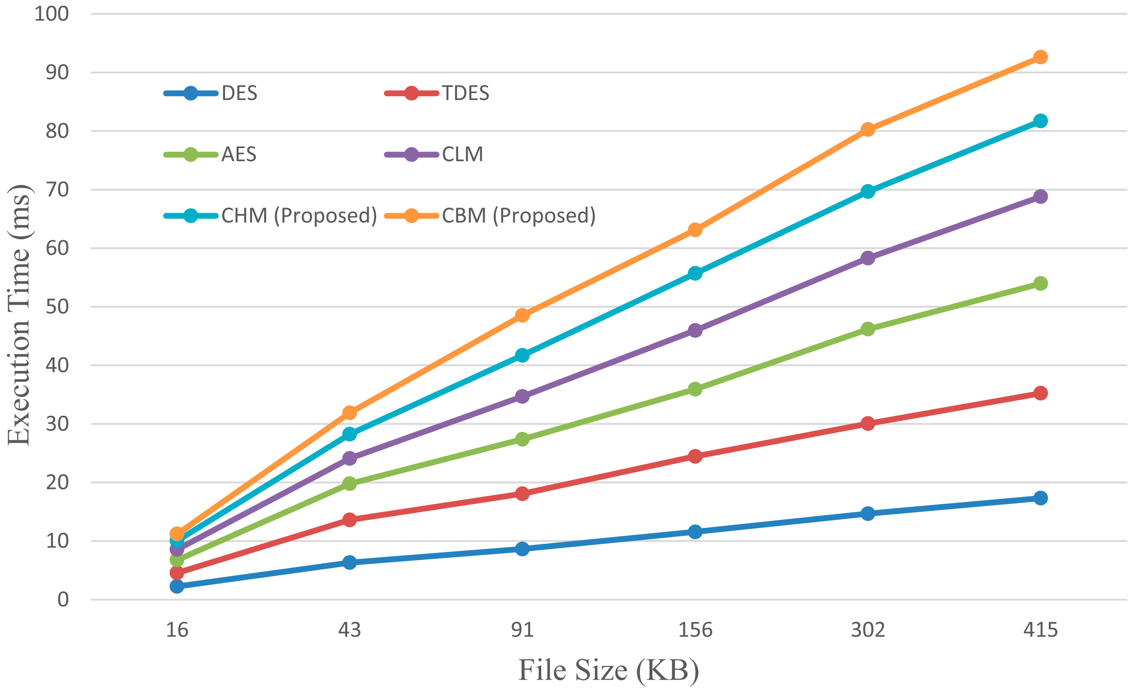


Figure 13. Variation in execution time for various file sizes.

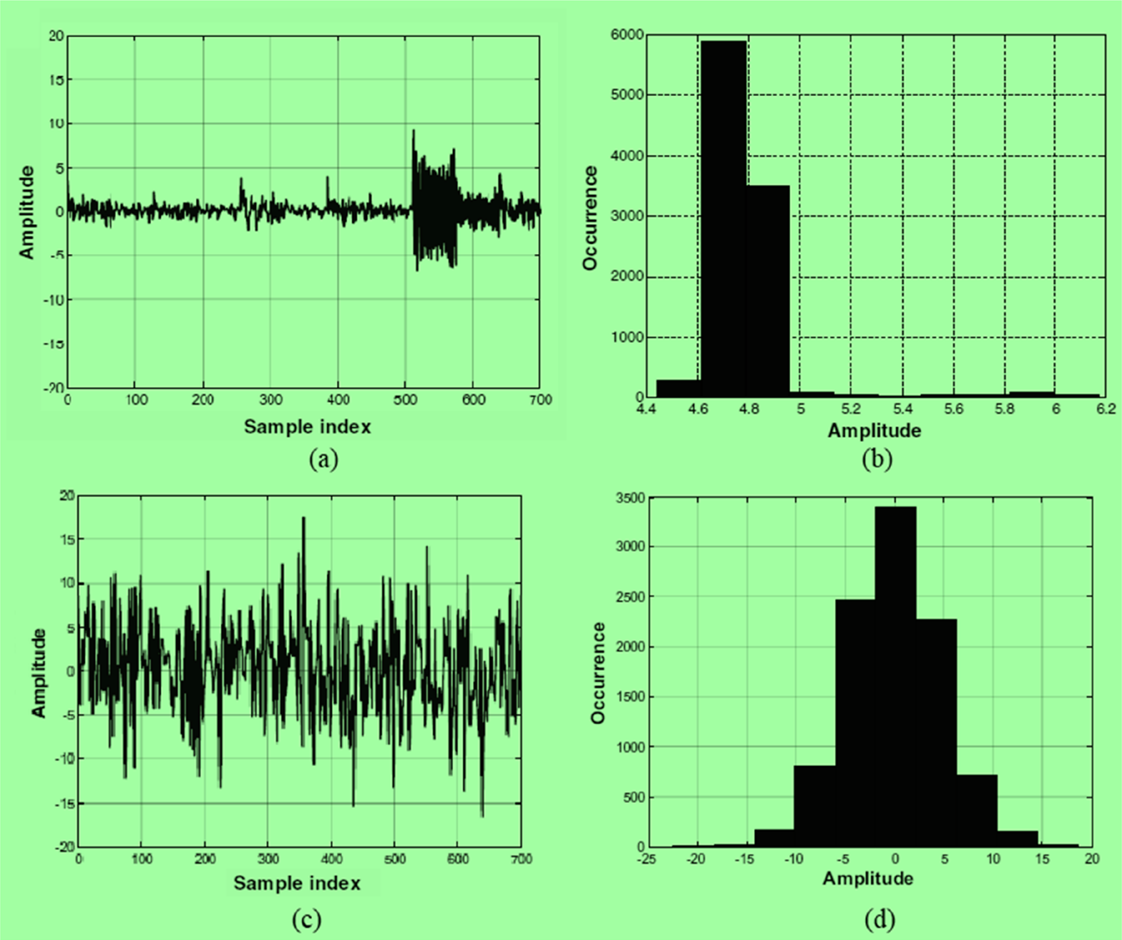


Figure 14. Histogram analysis (a) CHM Encrypted ECG (b) Histogram of CHM encrypted ECG (c) CBM encrypted ECG (d) Histogram of CBM encrypted ECG.

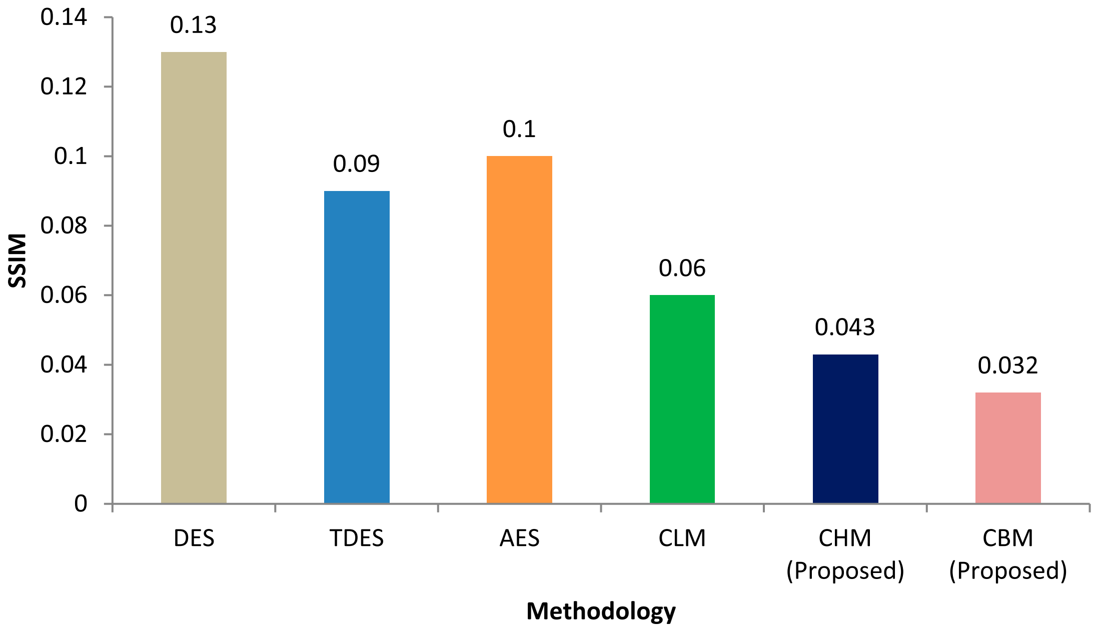


Figure 15. Comparison of SSIM.

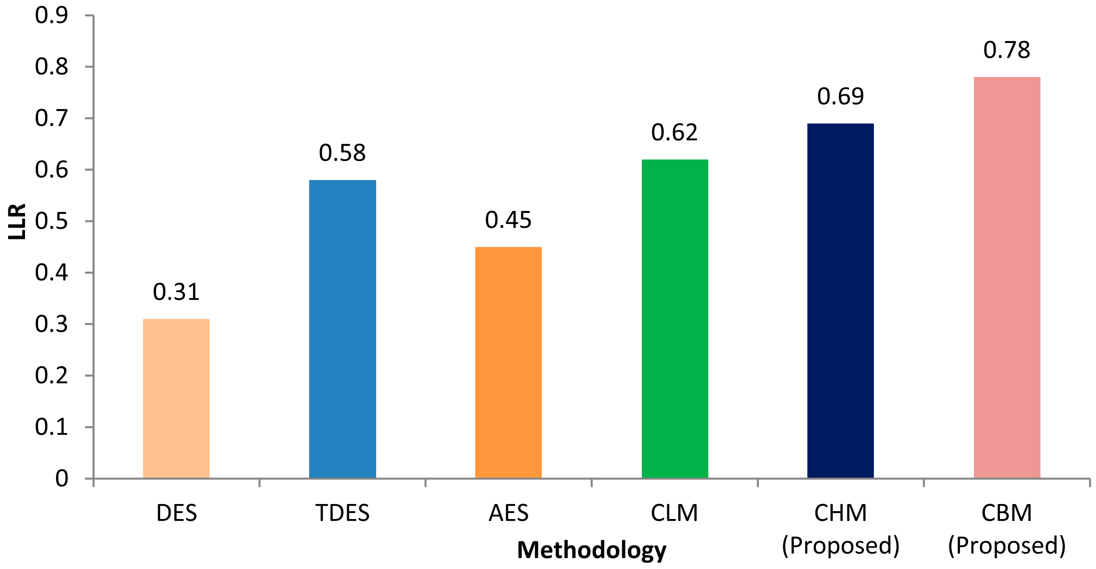


Figure 16. Comparison of LLR.

SD displays the distance between the spectrums of encrypted ECG and original ECG. This value is evaluated in frequency domain as given in Equation 7. $Q_x(i)$ represents the spectral distribution of ECG signal, while $Q_y(i)$ corresponds to the spectral distribution of the encrypted ECG signal. The comparison of the suggested cryptosystems with respect to Spectral Distortion (SD) is depicted in Figure 17. SD of CBM represents the largest spectral distortion, emerges as the most favourable in terms of encryption quality.

$$SD = \frac{1}{M}\sum_{m=0}^{M-1}\sum_{i=Nm}^{Nm+N-1}|Q_x(i) - Q_y(i)| \tag{7}$$

CBM exhibits an increase of 9 in the SD value as compared to CHM. This indicates large distance between the spectrums of original ECG and encrypted ECG. The comparison of SD is illustrated in Figure 17.

To further evaluate the performance of the cryptosystems, the correlation between the input and resulting ECG signals is calculated using Equation 8, where cov(x, y) represents covariance, and $\sigma_x{}^2$ and $\sigma_y{}^2$ signify variances.

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sigma_x \sigma_y} \tag{8}$$

The calculated correlation value (r_{xy}) for CBM is slightly lower by 0.003 compared to that of CHM. This decrease in correlation indicates a weaker relationship between the encrypted signal and the original ECG signal, imparting greater robustness to the encrypted signal against potential attacks. The comparison of correlation values is visually depicted in Figure 18. This underscores the effectiveness of adding extra chaotic

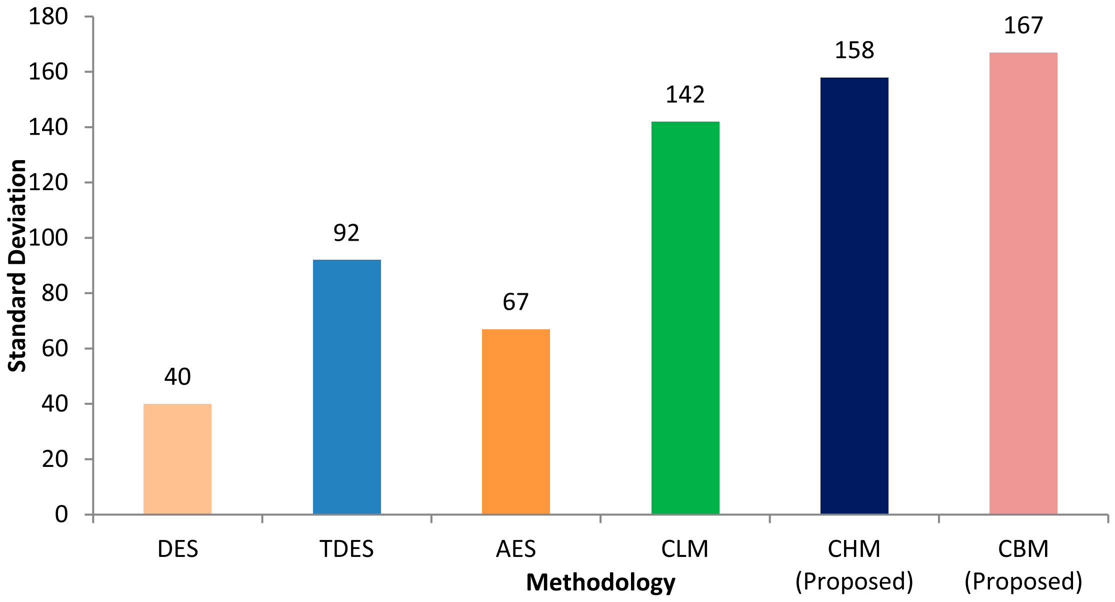


Figure 17. Comparison of SD.

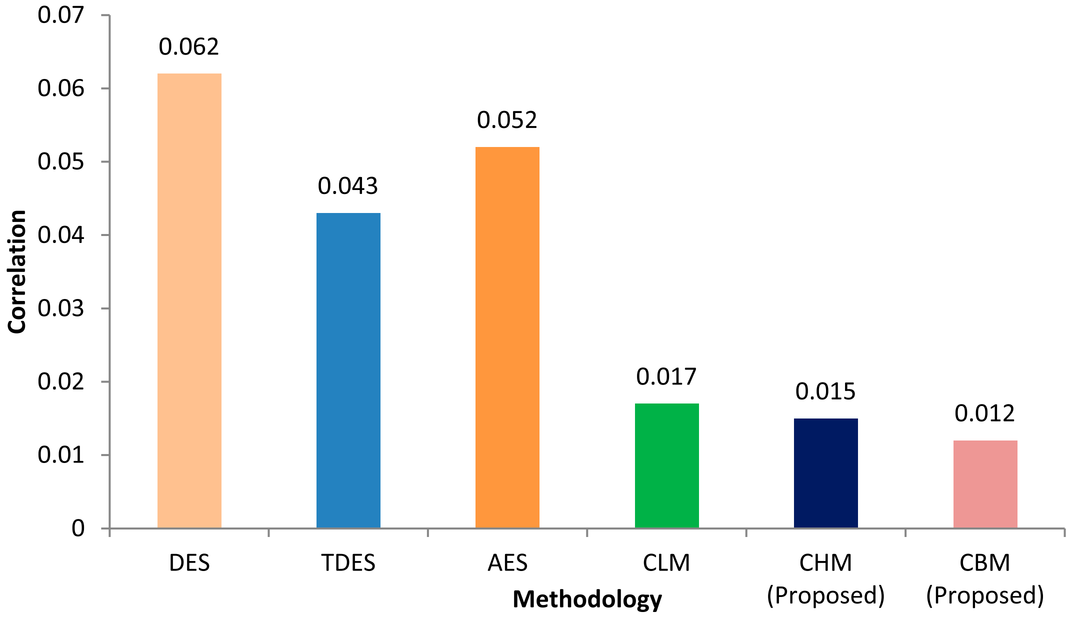


Figure 18. Comparison of correlation.

layers in the algorithm, a key factor contributing to the improved performance of ECG encryption.

In this work, the efficiency of various encryption algorithms in safeguarding ECG data was examined across different file sizes. Notably, the proposed CBM encryption algorithm consistently demonstrated the shortest execution times, making it an appealing choice for securing ECG data in real-time applications and storage. Traditional encryption methods like AES, TDES, and DES showed competitive performance but required more processing time, particularly with larger datasets. The CLM and CHM fell within the mid-range of efficiency. As a general trend, execution times increased with larger file sizes, highlighting the algorithm's sensitivity to computational demands. Ultimately, the analysis suggests that CBM strikes an excellent balance between security and efficiency, positioning it as a strong candidate for ECG signal encryption needs.

5. Conclusion

This work described a cryptosystem for generating safe ECG signals for use in telemedicine applications. Initially, the fingerprint features were extracted and key was generated for performing CHM and CBM on ECG. The choice of CHM and CBM encryption improved the security of ECG signal while transferring from patient unit to monitoring unit. Computation of performance parameters such as SSIM, Histogram, SD, Correlation and LLR indicated the efficiency of proposed algorithms over existing algorithms. According to the findings, using greater levels of encryption improves security. CBM encryption algorithm emerges as a standout performer, consistently delivering the shortest execution times. This finding positions CBM as an efficient and practical choice for safeguarding ECG data, particularly in real-time applications where computational efficiency is crucial. Traditional encryption methods such as AES, TDES, and DES remain viable options but exhibit increasing execution times with larger datasets. The CLM and CHM present competitive, albeit intermediate, performance. It's essential to consider the trade-off between security and computational resources when selecting an encryption algorithm. Overall, the study underscores CBM's potential as an effective and efficient solution for ensuring the confidentiality and integrity of ECG data in healthcare and related domains.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

[1] Algarni AD, Soliman NF, Abdallah HA, et al. Encryption of ECG signals for telemedicine applications. Multimed Tools Appl. 2021;80:10679–10703. doi:10.1007/s11042-020-09369-5

[2] Hameed ME, Ibrahim MM, Manap NA. Compression and encryption for ECG biomedical signal in healthcare system. Telecommun Comput Electron Control. 2019;17(6):2826–2833.

[3] Zhai X, Ali A, Amira A, et al. ECG encryption and identification based security solution on the Zynq SoC for connected health systems. J Parallel Distrib Comput. 2017;106:143–152. doi:10.1016/j.jpdc.2016.12.016

[4] Liu TY, Lin KJ, Wu HC. ECG data encryption then compression using singular value decomposition. IEEE J Biomed Health Inform. 2017;22(3):707–713. doi:10.1109/JBHI.2017.2698498

[5] Harinee S, Mahendran A. Secure ECG signal transmission for smart healthcare. Int J Performability Eng. 2021;17(8):711. doi:10.23940/ijpe.21.08.p7.711721

[6] Madhloom J, Ghani MKA, Baharon MR. ECG Encryption enhancement technique with multiple layers of AES and DNA computing. Intell Autom Soft Comput. 2021;28(2):493–512.

[7] Soni N, Saini I, Singh B. AFD and chaotic map-based integrated approach for ECG compression, steganography and encryption in E-healthcare paradigm. IET Signal Proc. 2021;15(5):337–351. doi:10.1049/sil2.12031

[8] Abdulbaqi AS, Al Naffakh HAH, Joseph PS. Exploring the potential of offline cryptography techniques for securing ECG signals in healthcare. Period Eng Nat Sci. 2023;11(3):148–154. doi:10.21533/pen.v11i3.3604

[9] Xu G. IoT-assisted ECG monitoring framework with secure data transmission for health care applications. IEEE Access. 2020;8:74586–74594. doi:10.1109/ACCESS.2020.2988059

[10] Qiu H, Qiu M, Lu Z. Selective encryption on ECG data in body sensor network based on supervised machine learning. Inf Fusion. 2020;55:59–67. doi:10.1016/j.inffus.2019.07.012

[11] Huang P, Guo L, Li M, et al. Practical privacy-preserving ECG-based authentication for IoT-based healthcare. IEEE Internet Things J. 2019;6(5):9200–9210. doi:10.1109/JIOT.2019.2929087

[12] Shaikh MU, Wan Adnan WA, Ahmad SA. Secured electrocardiograph (ECG) signal using partially homomorphic encryption technique–RSA algorithm. Pertanika J Sci Technol. 2020;28(S2):231–242. doi:10.47836/pjst.28.s2.18

[13] Tamilarasi K, Jawahar A. Medical data security for healthcare applications using hybrid lightweight encryption and swarm optimization algorithm. Wirel Pers Commun. 2020;114:1865–1886. doi:10.1007/s11277-020-07229-x

[14] Patel SK. Improving intrusion detection in cloud-based healthcare using neural network. Biomed Signal Process Control. 2023;83:104680. doi:10.1016/j.bspc.2023.104680

[15] Premkumar S, Mohana J. A novel ECG based encryption algorithm for securing patient confidential information. Int J Electr Eng Technol. 2020;2(11):35–43.

[16] Bhardwaj R. An improved reversible data hiding method in encrypted domain for E-healthcare. Multimed Tools Appl. 2023;82(11):16151–16171. doi:10.1007/s11042-022-13905-w

[17] Escobar M, Angel M, Cardoza-Avendaño L, et al. A double chaotic layer encryption algorithm for clinical signals in telemedicine. J Med Syst. 2017;41:1–17. doi:10.1007/s10916-016-0650-y

[18] Ahmed AA, Madboly MM, Guirguis SK. Securing data transmission and privacy preserving using fully homomorphic encryption. Int J Intell Eng Sys. 2023;16(1).

[19] Hameed ME, Ibrahim MM, Manap NA, et al. A lossless compression and encryption mechanism for remote monitoring of ECG data using Huffman coding and CBC-AES. Future Gener Comput Syst. 2020;111:829–840. doi:10.1016/j.future.2019.10.010

[20] Bhardwaj R. Effective electrocardiogram steganography for secured patient information transmission based on most significant bit planes prediction. Multimed Tools Appl. 2023;82(10):15779–15796. doi:10.1007/s11042-022-13955-0

[21] Yan W, Zhang Z. Online automatic diagnosis system of cardiac arrhythmias based on MIT-BIH ECG database. J Healthc Eng. 2021;2021:1–9.

[22] Roy A, Misra AP. Audio signal encryption using chaotic Hénon map and lifting wavelet transforms. Eur Phys J Plus. 2017;132:1–10. doi:10.1140/epjp/i2017-11280-8

[23] Meranza-Castillón MO, Murillo-Escobar MA, López-Gutiérrez RM, et al. Pseudorandom number generator based on enhanced Hénon map and its implementation. AEU-Int J Electron Commun. 2019;107:239–251.

[24] Sheela SJ, Suresh KV, Tandur D. Image encryption based on modified Henon map using hybrid chaotic shift transform. Multimed Tools Appl. 2018;77:25223–25251. doi:10.1007/s11042-018-5782-2

[25] Faragallah OS, Naeem EA, El-Shafai W, et al. Efficient chaotic-Baker-map-based cancelable face recognition. J Ambient Intell Humaniz Comput. 2021;2021:1–39.

[26] Elashry IF, El-Shafai W, Hasan ES, et al. Efficient chaotic-based image cryptosystem with different modes of operation. Multimed Tools Appl. 2020;79:20665–20687. doi:10.1007/s11042-019-08322-5

[27] Musanna F, Kumar S. Image encryption using quantum 3-D Baker map and generalized gray code coupled with fractional Chen's chaotic system. Quantum Inf Process. 2020;19:1–31. doi:10.1007/s11128-019-2494-0.