International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Decoding the Pulse: Advancements in ECG Data Encryption

Rajasree G[1], R. Mathusoothana S Kumar[*2]

Submitted: 29/01/2024 **Revised**: 07/03/2024 **Accepted**: 15/03/2024

Abstract: The ever-advancing landscape of digital healthcare, it is crucial to securely transmit biomedical data, particularly the vital Electrocardiogram (ECG) signal, over the internet to hospital facilities. This study presents a novel encryption scheme for Electrocardiogram data by leveraging the Chaotic Baker map, Discrete Wavelet Transform and Dual Random Phase Encoding (DRPE). The methodology involves a three-step process designed to enhance security and effectively obscure original ECG information. The first step incorporates a randomized fusion of wavelet coefficients with a random signal, introducing variability. Subsequently, encryption scheme is implemented using 2-D Discrete Wavelet Transform (DWT) to mask the ECG signal and the speech signal, effectively concealing repetitive patterns. The third step employs DRPE, utilizing 2 Random Phase Masks (RPMs) to modify the spectrum of the transformed 2-D ECG signal. This multifaceted approach integrates random projection, salting, chaos-based encryption, and DRPE, providing a layered strategy for securing sensitive ECG data. Decryption involves the reverse application of these steps, ensuring the secure retrieval of the original ECG information. The proposed encryption methodology offers a robust solution for safeguarding ECG data across diverse applications.

Keywords: *Chaotic Baker map, Discrete Wavelet Transform, Dual Random Phase Encoding, Encryption.*

1. Introduction

As a non-invasive and widely accessible diagnostic tool, ECGs are instrumental in diagnosing various cardiac conditions and monitoring overall heart health. The distinctive waveforms captured by an ECG reflect the heart's rhythm, electrical conduction, and the coordination of its chambers [1]. This information is essential for identifying irregularities such as arrhythmias [2], ischemia [3], and myocardial infarctions. The real-time monitoring capabilities of ECGs make them invaluable in critical care situations, guiding healthcare professionals in making informed decisions about patient management and treatment strategies [4]. Routine ECG screenings are employed for early detection of cardiac issues in individuals with risk factors, allowing for proactive interventions and lifestyle modifications to prevent the progression of heart diseases. Figure 1 provides an overview of the typical structure of an Electrocardiogram (ECG). The versatility and reliability of ECG signals make them a cornerstone in the cardiac care continuum, aiding in the comprehensive assessment of cardiovascular health and promoting timely and targeted medical interventions.

Electrodes on particular parts of a person's body create several types of monitoring. Every heartbeat produces a succession of electrical waves, which can be seen on the record. The letters P, Q, R, S, T, and U are used to designate the tops and valleys of the recorded oscillations [5]. The electrical operations are documented on chart sheets or other forms of documentation. The structure, duration, and amplitude of these pulses provide sufficient information regarding the heart's condition.

The encryption of ECG data has become increasingly vital with the digitalization of healthcare systems [6]. As ECG signals contain sensitive information about an individual's cardiac health, ensuring the confidentiality and integrity of this data is paramount. Encryption techniques are employed to safeguard ECG transmissions and storage, preventing unauthorized access and potential misuse. Securing medical data, including ECGs, not only protects patients' privacy but also upholds the integrity of diagnoses and treatment plans, fostering trust in healthcare systems and ultimately contributing to improved patient outcomes [7].

Fig. 1 General format of Electrocardiogram

Various encryption techniques are employed to secure medical data, including ECG signals. Common methods include symmetric key cryptography [8], asymmetric key cryptography [9], and hashing algorithms [10]. A shared key for both encryption and decryption is used in symmetric key cryptography, while asymmetric key cryptography employs a pair of public and private keys. Hashing algorithms generate fixed-size hash codes to verify data integrity. However, these techniques have limitations. Symmetric key cryptography requires secure key distribution, and asymmetric key cryptography is computationally intensive. Hashing alone cannot retrieve

the original data and is susceptible to hash collisions. Balancing the trade-offs between security and computational efficiency is crucial when implementing encryption in healthcare systems to ensure robust protection of sensitive medical information like ECG data.

To enhance the security and robustness of the encryption process, Chaotic Baker map and dual random phase encoding was employed in this method for data encryption [11]. The chaotic Baker map introduces unpredictability and sensitivity to initial conditions, making it a suitable choice for generating cryptographic keys and creating a dynamic, nonlinear transformation in the encryption algorithm. Dual random phase encoding involves encoding information in both the amplitude and phase domains, adding an extra layer of complexity and reducing vulnerability to attacks [12]. By combining these techniques, the encryption system aims to achieve a higher level of security, resisting conventional cryptographic attacks and ensuring the confidentiality and integrity of sensitive data, particularly in applications where the protection of information, such as medical records or financial data, is of utmost importance.

The paper's primary contributions can be summarized as follows:

- Developed a user-friendly ECG encryption framework that seamlessly integrates chaotic dynamics and dual random phase encoding.
- Implemented a nonlinear transformation using Chaotic Baker map to uphold the integrity of ECG signals, preventing tampering and ensuring the accuracy of medical information during encryption processes.
- Employed dual random phase encoding to fortify ECG data encryption, mitigating vulnerabilities and ensuring robust protection against unauthorized access or cyber threats.

2. Literature Review

Algarni et al [13] introduced three cryptosystems for ECG signal encryption, emphasizing the operational efficiency gained by working directly on sample values rather than employing traditional encoding and decoding schemes. The first cryptosystem utilizes random projection on DWT coefficients, salting algorithm, and a three-phase process of fusion, substitution, and chaotic permutation, leveraging a two-dimensional chaotic Baker map for permutation. Fusion of ECG signal and speech signals in the third cryptosystem compensates for extended periods of low activity in ECG signals. Performance evaluation via simulation experiments, considering metrics like histogram, SNR, structural similarity index reveals the superiority of the three-phase cryptosystem [14]. The method exhibits high security levels, it often has limitations along with the comprehensive methodology. The paper is limited by the absence of proper method for ECG feature extraction, hindering potential advancements in diagnosis and authentication applications.

Qiu et al [15] focused on redefining Secure Electrocardiogram (ECG) schemes in the context of outsourcing ECG data in untrusted Body Sensor Network (BSN) environments. Addressing the inadequacy of classic schemes in scenarios involving machine learning-based disease classification, the authors propose a tailored design to safeguard against unauthorized data classification and protect patient privacy. Extensive tests using a dataset featuring congestive heart failure, cardiac arrhythmia, and normal sinus rhythms validate the efficacy of the proposed SE method. The dataset comprises 162 ECG recordings from PhysioNet databases. The methodology involves redefining classic SE schemes and proposing a machine learning-based ECG classification model. While the paper offers valuable insights, potential limitations and the need for broader datasets or real-world implementations could be explored in future research to enhance the robustness and generalizability of the proposed SE method. The paper is constrained by its current scope, limited to the exploration of a specific set of selective encryption methods. Further research is needed to address diverse encryption approaches and lightweight methods for enhanced data protection tailored to specific application requirements.

Abdulbaqi et al [16] addressed automated process includes secure transmission of ECG reports to doctors. The platform, from data capture to mobile application results, is end-to-end, employing efficient signal processing algorithms and noise elimination filters for accuracy. Although the methodology is executed and demonstrated on various patients, the paper lacks explicit details on the dataset used. The limitation lies in a relatively brief discussion of potential challenges or constraints. Abdulbaqi et al [17] introduced an innovative medical image encryption algorithm leveraging ECG signals. The encryption process integrates chaotic logistic and generalized Arnold maps, with initial conditions derived from the wolf algorithm and the ECG signal. Autoblocking diffusion occurs solely during encryption, enhancing security. Experimental results demonstrate the algorithm's high security and efficiency. The methodology involves ECG signal manipulation and Autoblocking diffusion during encryption, showcasing potential improvements through the incorporation of additional medical data, such as EEG signals for key generation. However, the paper lacks details on specific datasets used for experimentation and fails to address potential limitations, including algorithm robustness under diverse medical image scenarios.

Kh-Madhloom et al [18] introduced an encryption approach, MLAESDNA, merging DNA computing and Advanced Encryption Standard (AES) to enhance the security of IoT health cloud systems [19]. The model generates three keys, facilitating robust protection against plaintext attacks in fog computing clouds. The four DNA rule-derived keys may lead to increased encryption and processing time, posing challenges for real-time applications in public health and emergency scenarios. The proposal is promising for securing ECG signals in insecure healthcare system channels, although future research should focus on optimizing execution time through quantum computing integration and parallel processing. Overall, MLAESDNA demonstrates efficiency, integrity, and robustness, offering a noteworthy advancement in joint encryption techniques.

Hameed et al [20] presented a comprehensive approach for secure and efficient transmission of ECG signals. Leveraging buffer blocks, peak detection, discrete wavelet transforms [21], Huffman coding [22], and AES [23], the system ensures data integrity and privacy protection. Experimental validation using five datasets from the MIT-BIH arrhythmia repository demonstrates superior reconstruction quality compared to unencrypted compression. The study evaluates efficiency metrics such as PRD, CR, PSNR, and MSE, indicating the algorithm's effectiveness. The focus on lightweight model development for ECG signal processing and encryption, along with the proposed block-level processing using 256-bit AES (CBC), suggests applicability in real-time embedded devices.

Kumar et al [24] introduced a cryptography technique for data security based on ECG signal-, employing bilateral random hashing (BRH) and downhill peak follow (DPF) encryption. The encryption system extracts key signatures from ECG signal peaks, creating a random key pattern to encrypt data for secure transmission or storage. The study focuses on enhancing the proposed model's efficiency by combining BRH with DPF, evaluating parameters such as encryption time, reconstruction time.

Patil et al [25] proposed an enhanced strategy for secure data communication through the encoding of masked data in ECG signals. The encryption method scrambles classified information into a complex structure, improving the security of concealed data. Additionally, a chaos crypto framework is introduced to further enhance security. The reversible data hiding technique, utilizing DWT and LSB substitution algorithm, embeds secret messages into high-frequency coefficients. The system ensures data integrity, size preservation, and efficient encoding/decoding processes. Despite its merits, the paper lacks specific details on the dataset used for evaluation and fails to thoroughly address limitations.

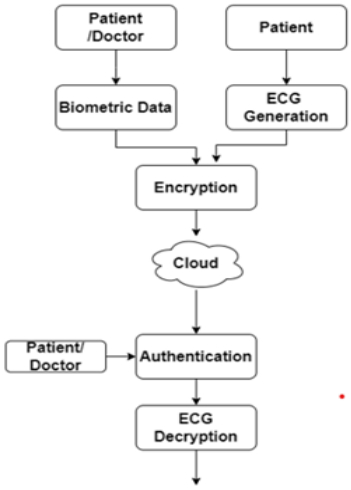
Adithya et al [26] introduced the DMIES cryptosystem, a medical image encryption method employing chaos maps. The system performs chaos intertwining, DNA structure generation, Knight's travel map decomposition, and affine transformation to enhance data security. The pixel DNA-coded matrices and DNA sequencing contribute to the encryption process, ensuring tamper prevention and data integrity. The proposed method's suitability for smart health applications is highlighted, emphasizing its quick processing time of 0.243 seconds.

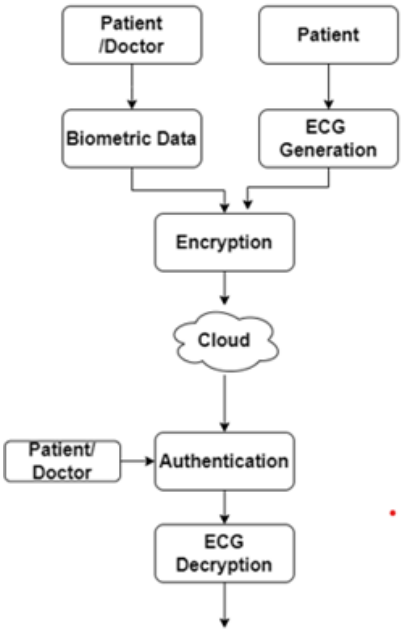
Salem et al [27] addressed the crucial need for secure telemedicine platforms, especially in the context of IoT-enabled medical devices. Focusing on the challenges of safeguarding patient data and ensuring efficient communication between medical staff and patients, the research proposes a lightweight encryption/decryption technique using the Diffie-Hellman (DH) method in IoMT. The DH method, with its four encryption keys, is chosen for its minimal impact on data transmission speed. The experimental results demonstrate the proposed method's efficiency and security, showcasing its ability to meet the required protection levels for securing medical information. The study emphasizes the nascent stage of secure telemedicine solutions and advocates for the adoption of lightweight encryption approaches, particularly those incorporating chaotic IoT networks. The integration of DH into chaotic IoT for telemedicine is discussed, highlighting the potential of this method in ensuring secure communication between doctors and patients in remote healthcare settings.

3. Materials and Methods

Proposed encryption methodology for ECG signals, a three-step process is employed to enhance security and obfuscate the original ECG information effectively. In the first step, the fusion of ECG signal and a random signal is achieved through a randomized process by random projection or salting. This step aims to introduce variability to the ECG signal representation. Subsequently, in the second step, a chaos-based encryption scheme is implemented using a 2-D DWT for further obfuscation. The masking of ECG signal and speech signal lacking silent period, effectively concealing the repetitive pattern inherent in the ECG signal. The fusion process is carried out in the transformed 2-D domain, contributing to the creation of a highly encrypted representation of the ECG signal. In the third step of the encryption process, the Dual Random Phase Encoding (DRPE) technique is employed. This optical encryption approach involves the insertion of two RPMs in different planes. The transformed 2-D ECG signal is multiplied with RPM1, introducing the modification to encrypted signal. The transformed 2-D ECG signal is multiplied with RPM2 in the Fourier plane, constituting the second modification. Inverse Fourier

transform is then applied to obtain the final encrypted 2-D ECG signal in its original 2-D space. For decryption, the process must be reversed using the same RPMs, ensuring the secure retrieval of the original ECG information. Figure 2 illustrates the proposed encryption system. This multifaceted encryption methodology, incorporating random projection, salting, chaos-based encryption, and DRPE, offers a robust and layered approach to safeguarding sensitive ECG data.





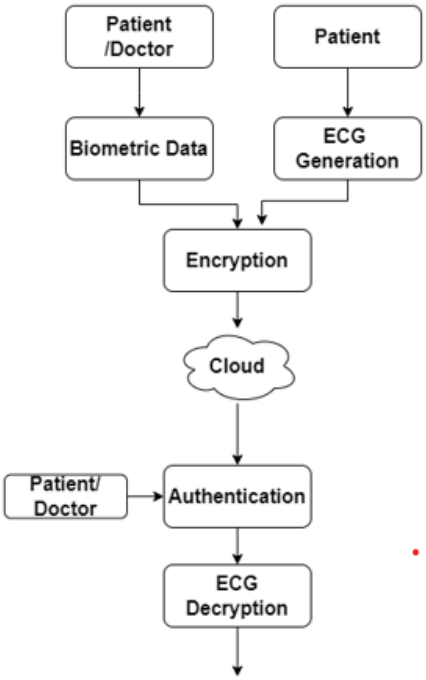


Fig. 2 The architecture of the proposed system

3.1. Dataset description

To conduct experiments, we obtained ECG data from the MITBIH dataset of arrhythmia [28]. Each signal in this database has a duration of approximately 30 minutes and is sampled at a frequency of around 360 Hz. The dataset includes nearly 48 distinct ECG signals. To assess performance, a thorough evaluation was conducted, employing a comprehensive set of metrics and perspectives in the assessment procedure.

3.2. DWT Random projection

The ECG signal is separated into two half-length sub-signals using the DWT. A running average and a running differential make up these sub-signals. Random projection is used to encrypt the wavelet coefficients. We can create a random vector Z by multiplying a vector Y with matrix B in which Y represents ECG signal and B denotes one of its components in the wavelet domain.

$$Z_{K*1} = B_{K*d} * \quad Y_{d*1} \qquad (1)$$

By this multiplication operation the input vector is changed into a random vector. Inverse random projection and inverse DWT are applied to recreate the ECG signal at the receiver for additional analysis. A random sequence is added to the wavelet coefficients or the ECG signal itself to introduce salting. The power of the additional noise affects the efficacy of salting-based cryptosystem. This cryptographic technique combines the DWT coefficients of the original ECG pattern with a random pattern. During

reception the original ECG signal is further examined by a simple subtraction process."

Inverse Discrete Wavelet Transform maintained the perfect reconstruction property of the original input signal. The procedure of wavelet fusion is shown in Figure 3. We assume that wavelet reconstruction is done with Go and G1, while wavelet decomposition is done with Ho and H1.

$$Z(y) = \frac{1}{2}\left(A_0(y) + A_0(-y)\right)H_0(y) + \frac{1}{2}\left(A_1(y) + A_1(-y)\right)H_1(y)$$

$$= \tfrac{1}{2}A(y)\left(G_0(y)^{+}\right.$$
$$H_0(y) + G_1(y)H_1(y)) +$$
$$\tfrac{1}{2}A(-y)G_0(-y)H_0(y) +$$
$$G_1(-y)G_1(y)) \qquad (2)$$

For better reconstruction,

$$\left(G_0(-y)H_0(y) + G_1(-y)H_1(y)\right) = 0 \qquad (3)$$

And can be achieved as

$$G_1(-y) = A^{-k}H_0(y) \qquad (4)$$

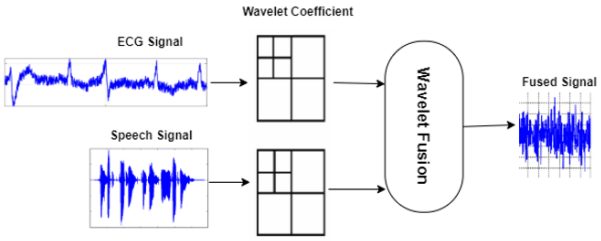


Fig. 3 Wavelet fusion process

3.3. Chaotic Baker map

Sensitivity in initial conditions and parameter settings introduces a high level of unpredictability, making it a robust choice for securing data. The chaotic Baker map exists in two forms: Generalized map and the Discretized map. When it comes to randomizing elements in a square matrix, the Discretized Baker map is often preferred due to its simplicity and effectiveness for this application. Typically, a continuous chaotic map undergoes discretization and subsequent generalization by introducing parameters. This generalized map, with parameters derived from the encryption key, is employed to scramble data.

A chaotic generalized map refers to a mathematical model that exhibits chaotic behaviour in its dynamical system. In the context of mathematical chaos theory, a generalized map typically represents a discrete-time, iterative process where the future state of the system is determined by a mathematical function applied to its current state.

The latter, known for its efficacy in randomizing elements within a square matrix, utilizes a discretized function denoted as $B(n1, \dots, nk)$, where $[n1, \dots, nk]$S key represents the secret key. The secret key is strategically chosen such that each integer ni divides N, with the sum of all ni equalling $N\ (n1 + \ \dots + nk\ =\ N)$.Discretized Baker map is effective for enhancing the randomness and complexity of cryptographic schemes. Discretization refers to the process of converting a continuous system into a discrete one by considering the evolution of the system at distinct, evenly spaced time intervals. It involves a two-dimensional phase space where points undergo a series of stretching and compressing operations, leading to intricate patterns and sensitive dependence on initial conditions.

The secret key is chosen in a manner that each integer n_i divides N,and $n1 + \dots\dots + nk$=N .Let $Ni\ =\ n1\ + \cdots\dots + ni - 1$ and data elements in one row is represented by N. The data item at the indices (q, z), is moved to the indices:

$$B_{(n_{i=m=}n_i)}(q,z) =$$
$$\left(\frac{N}{n_i}(q - N_i) + z \bmod \frac{N}{n_i}\right), \frac{n_i}{N}\left(z -\right.$$
$$\left. z \bmod \left(\frac{N}{n_i}\right)\right) + N_i$$
$$(5)$$

Where $N_i \le q < N_i + n_i, 0 \le z < N, and\ N_1 = 0$

The Baker map key space encompasses all potential permutations of a key. Its design aims to thwart brute-force attacks by ensuring that the key used for encryption remains elusive to adversaries attempting exhaustive searches. Typically, the key space is made sufficiently vast to render such search endeavors impractical, requiring, on average, the exploration of half the key space. "In Baker map creation, the message is organized into a square of side N. Therefore, it is imperative to select a key of ample size to attain a heightened level of security. For a Baker map with N items, where N is 128, the key space is extensive, encompassing (4.4128×1022) possible keys, making it suitable for applications like lightweight encryption. For determining the key possibilities of a Baker map size N, this paper introduces a formalized method through the development of a recursive algorithm. The key's possible alphabet is defined as 2, 4, … 2n, …, N. Constructing a key involves selecting elements from this alphabet such that their sum equals N. The recursive algorithm initiates by calculating the number of key possibilities with a single alphabet in the key, such as [1, 1, 1, 1, 1, 1, 1, 1] ,[1,4,3,1], [2, 2, 2, 2], [2,2,4,4] for instance. The equation for computing the single-key possibilities can be inferred as follows:

$$S(N_i) = \log(N_i) + 1 \qquad (6)$$

The algorithm begins by assessing single alphabet possibilities denoted as S(N_i), where N represents the size of Baker map. To determine the number of key involving

two alphabets it proceeds drawing on the count of single-key alphabets".

During the implementation of the chaotic permutation through the Discretized Baker map, a square matrix of dimensions N x N undergoes partitioning into N rectangles. Each rectangle, possessing N elements, is characterized by a width of n_i.The subsequent step involves reconfiguring these rectangles, where their elements are reorganized into rows within the permuted rectangle. The rearrangement process unfolds by traversing the rectangles in a left-right manner, commencing with upper rectangle and subsequently advancing to lower one. Within each rectangle, the scanning process commences from the left corner, progressing upwards through the elements. This systematic yet chaotic permutation of data elements ensures a secure and unpredictable transformation, bolstering the robustness of cryptographic systems.

3.4. Masking the ciphertext with a secret pseudo-random signal

Masking in the context described the creation of a cryptographic mask derived from a secret key, which is subsequently applied to hide specific periods within an electrocardiogram (ECG) signal. The secret key, in this instance, is utilized to generate a mask by introducing a specific number of one into an initially all-zero block. Using the chaotic Baker map this block is then subjected to permutation resulting in a mask comprising both zeros and ones. The purpose of this masking operation is to enhance the security of the ECG signal by obscuring certain segments, making it more resistant to known-plaintext attacks. The steps outlined in the masking process are crucial for introducing variability and complexity to the masked signal, preventing potential attackers from exploiting known patterns.

0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.2	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.2	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.2	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.2	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.2	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.2	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.2	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.2	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.2	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.2	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.2	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.2	0	0	0

Original signal

1	1	1	1	1	1	1	1	1	1	1	1
0	0	1	0	0	1	0	0	1	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1
0	0	1	0	0	1	0	0	1	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1
0	0	1	0	0	1	0	0	1	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0

Mask

Fig. 4. Original signal and corresponding mask

The use of a chaotic Baker map ensures a non-linear and unpredictable transformation, contributing to the effectiveness of the masking technique. Additionally, the clipping step at the end of the process is employed to limit the values within a specified range (-1 to 1), ensuring that the masked signal remains within a manageable and interpretable range. Figure 5 illustrates the signals subsequent to the masking process. Overall, the masking approach described provides a layer of security by transforming the ECG signal in a controlled yet intricate manner, safeguarding sensitive information from unauthorized access or analysis.

1.1	1	1	1.5	1.4	1.4	1.4	1.4	0.8	1	1	1
0.1	0	2	0.5	0.4	1.4	0.4	0.4	0.7	0	0	1
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.3	0	0	0
1.1	1	1	1.5	1.4	1.4	1.4	1.4	0.8	1	1	1
0.1	0	2	0.5	0.4	1.4	0.4	0.4	0.7	0	0	1
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.3	0	0	0
1.1	1	1	1.5	1.4	1.4	1.4	1.4	0.8	1	1	1
0.1	0	2	0.5	0.4	1.4	0.4	0.4	0.7	0	0	1
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.3	0	0	0

Signals after masking

-0.9	1	1	-0.5	-0.6	-0.6	-0.6	-0.6	0.8	1	1	1
0.1	0	0	0.5	0.4	-0.6	0.4	0.4	0.7	0	0	1
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.3	0	0	0
-0.9	1	1	-0.5	-0.6	-0.6	-0.6	-0.6	0.8	1	1	1
0.1	0	0	0.5	0.4	-0.6	0.4	0.4	0.7	0	0	1
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.3	0	0	0
-0.9	1	1	-0.5	-0.6	-0.6	-0.6	-0.6	0.8	1	1	1
0.1	0	0	0.5	0.4	-0.6	0.4	0.4	0.7	0	0	1
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.4	0.4	0.4	-0.3	0	0	0

Resultant Block

Fig. 5. Signals after masking

3.5. Dual random-phase encoding

The resulting encoded image exhibits heightened security and robustness when it follows the encoding of the input image through the utilization of two independent random phases attributable to its characteristic white noise. Moreover, the DRPE technique seamlessly integrates with various classic optical information processing technologies. This integration extends to optical image encryption scheme and authentication algorithm, achieved through the expansion from Fourier transform domain to Fresnel transform domain, wavelet transform domain, Gyrator transform domain, and other transform domains. To optimize storage efficiency and reduce data storage costs, the phase information generated by DRPE for image authentication is designed to occupy minimal storage space. Consequently, only a selective portion of the phase information is retained, while all amplitude information is deliberately discarded, enhancing image compression and facilitating efficient data transmission.

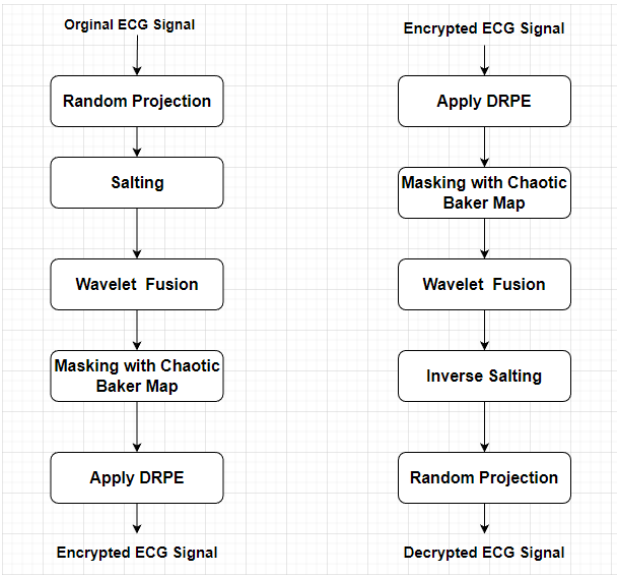


Fig. 6. Encryption, Decryption Process

Illustrated in Figure 6 is the intricate process of encryption and decryption, providing a visual representation of the steps involved in securing and retrieving ECG data. The proposed cryptosystem integrating CS with DRPE can achieve encryption and authentication synchronously. The flowchart of our proposed encryption scheme is depicted in Fig. 1, which clearly shows that the encryption process from plaintext image to ciphertext image goes through four stages: DRPE phase, CS phase, permutation phase and diffusion phase, respectively. First, the plaintext image is encoded and quantified to obtain the authentication information through DRPE transformation, and then, the same plaintext image is compressed and quantified to obtain the corresponding measurements through CS. Next, the authentication information and the measurements are permutated together to obtain the permutation image. Finally, the permutation image is diffused into the ciphertext image by the XOR operation.

Algorithm 1: Encryption Process

1. Segment original ECG signal into segments, and then reshape them into 2-D format.
2. Mask the Key using Chaotic Baker map.
3. Add this mask to the transformed 2D ECG Signal.
4. While performing **Clipping**, A value of 2 is subtracted from all values exceeding 1 resulting in negative values to make all samples between -1 and 1.
5. Apply DRPE.
   - Generate first Fourier RPM key RPM1 and multiply it by the target ECG signal to be encrypted.
   - Generate second Fourier RPM key RPM2, and insert it into the ECG signal in the Fourier plane.
   - Perform the second Fourier transform using a second lens to obtain the encoded ECG signal in the original 2-D space of ECG signal.
6. Reshape the 2-D format to 1-D format which represents the encrypted ECG signal.
7. Synthesize segments.
8. END

DRPE involves the insertion of two RPM one in the input plane and the other in the Fourier plane. The primary objective of DRPE is to transform the original 2-D ECG signal into stationary noise, enhancing its security through encryption. The encryption process is initiated by multiplying the first RPM (RPM1) with the transformed 2-D ECG signal. This multiplication induces the initial modification in encrypted 2-D ECG signal. Second RPM is directly multiplied into the spectrum of the transformed 2-D ECG signal in the Fourier plane. Introducing the second modification to the spectrum of the transformed 2-D ECG signal, the spectrum obtained in the initial stage undergoes multiplication with RPM2. The final step of the encryption process involves a second inverse Fourier transform through a magnifier, resulting in the generation of an encrypted 2-D ECG in the original ECG 2-D space. To decrypt the encrypted signal, the same RPMs used in the encryption process are required, along with the complex conjugate Fourier phase key, ensuring the reversibility of the transformation and the recovery of the original 2-D ECG signal. The DRPE technique provides a secure and effective means of protecting sensitive biomedical data through optical encryption methodologies".

Algorithm 2: Decryption Process

1. Segment encrypted ECG signal into segments and then reshape them into 2-D format Mask the Key using Chaotic Baker map.
2. Apply DRPE.
   - Generate first Fourier RPM key RPM1 and multiply it by the target ECG signal to be encrypted
   - Generate second Fourier RPM key RPM2, and insert it into the ECG signal in the Fourier plane.
   - The insertion of the RPM2 in the ECG obtained in the first phase introduces the second amendment into the target ECG signal.
   - Perform the second Fourier transform using a second magnifier to obtain the encoded ECG in the original 2-D space of ECG signal.
3. Perform Inverse clipping by adding a value of 2 to negative values less than -1 in the resulting encrypted 2-D ECG signal.
4. Masking with Chaotic Baker map.
5. Subtract mask from the encrypted 2-D ECG signal.
6. Reshape the 2-D ECG to 1-D format which represents the original ECG signal.
7. Synthesize segments and reconstruct ECG signal.
8. End

4. Experimental Setup

To evaluate the effectiveness of the proposed cryptosystems, simulation testing is conducted using MATLAB (R2018a). The implementation encompasses all recommended cryptographic techniques. The encryption of initial ECG signals is achieved using the CLM algorithm, serving as a benchmark for efficiency assessment. The experimental dataset comprises ECG data obtained from the MIT-BIH arrhythmia dataset [21], where each signal spans approximately 30 minutes, with a sampling frequency rate of around 360 Hz. This dataset encompasses nearly 48 ECG signals. The assessment of performance employs a comprehensive array of measures and

perspectives to thoroughly evaluate the proposed cryptosystems.

The evaluation of correlation in the analysis determines the extent of similarity between corresponding elements in the original and encrypted matrices [7]. The sensitivity of the algorithm to the secret key can be quantified using the correlation coefficient, as expressed in the following equation

$$C = \frac{N\sum_{i=1}^{M}(x_i * y_i) - \sum_{i=1}^{M} x_i * \sum_{i=1}^{M} y_i}{\sqrt{(N\sum_{i=1}^{M} x_i^2 - (N\sum_{i=1}^{M} y_i^2 - \sum_{i=1}^{M} y_i^2))}} \quad (7)$$

In Baker map matrix where $, y_i$ are the values of two adjacent items and N is the total number of items. Figure 7 displays the original ECG signal, the ECG signal after, and the decrypted ECG signal. The visualization highlights discernible variations in both amplitude and frequency of the ECG signal, underscoring the impact of the encryption process.

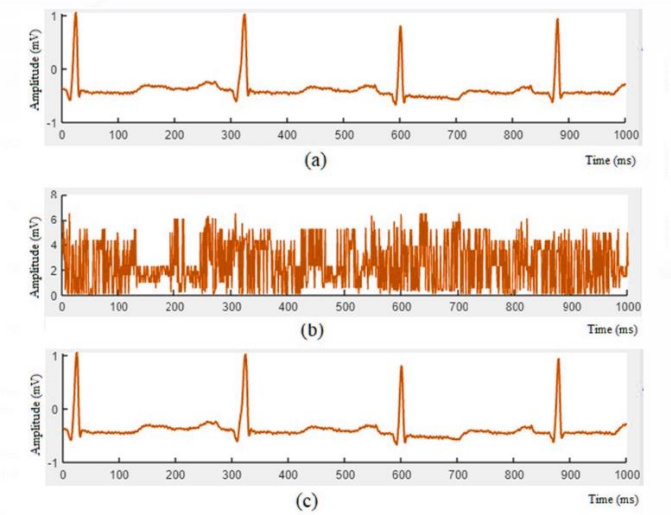


Fig. 7. Original signal, encrypted signal, decrypted signal

The table 1 presents a comprehensive performance comparison of three approaches – logistic map, Henon map, and Baker map – with respect to key image quality metrics such as PSNR (Peak Signal-to-Noise Ratio), MSE (Mean Squared Error), and SSIM (Structural Similarity Index Metric). The evaluation aims to assess the efficacy of these chaotic maps in encryption and decryption process. The results reveal insights into how each map influences the quality of the processed images, with higher PSNR values indicating better signal fidelity, lower MSE values signifying reduced distortion, and SSIM metrics providing a measure of structural similarity between the original and processed images. This comparative analysis offers valuable information for selecting an appropriate chaotic map based on specific image processing requirements and desired quality outcomes.

TABLE 1 : PERFORMANCE COMPARISON

ECG Sample	PSNR (dB)			MSE			SSIM		
	Logistic Map	Henon Map	Baker Map	Logistic Map	Henon Map	Baker Map	Logistic Map	Henon Map	Baker Map
Patient 1	25.403	23.654	21.857	188.203	281.747	426.485	0.0013	0.00072	0.00087
Patient 2	25.401	23.222	21.275	188.372	310.514	487.454	0.0016	-0.00306	0.00217
Patient 3	25.511	24.038	22.395	184.105	258.319	377.483	0.0019	0.00345	0.00351
Patient 4	25.558	24.026	22.338	182.201	258.259	380.675	0.0001	0.00022	0.00110
Patient 5	25.484	23.680	21.867	185.245	281.512	428.176	0.0018	0.00162	0.00074

The PSNR comparison involves evaluating the performance of three distinct chaotic maps—logistic map, Henon map, and Baker map—applied to ECG signals from five different patients is shown in figure8. The Peak Signal-to-Noise Ratio (PSNR) values are computed to quantify the quality of the reconstructed signals in comparison to the original ECG signals. This analysis aims to provide insights into how each chaotic map contributes to the preservation of signal fidelity across various patient datasets. Higher PSNR values indicate improved reconstruction accuracy, suggesting a more effective preservation of signal details. This comparison serves as a valuable assessment of the performance of chaotic maps in the context of ECG signal processing and encryption for diverse patient data

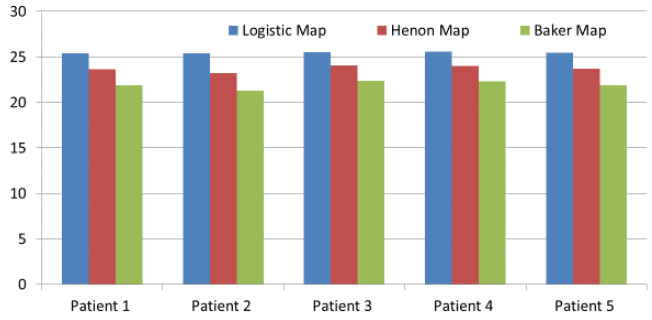


Fig. 8. PSNR Comparison

The MSE comparison involves assessing the performance of three distinct chaotic maps—logistic map, Henon map, and Baker map is shown in figure 9. The evaluation measures the Mean Squared Error (MSE) between the original ECG signals and their corresponding encrypted counterparts for each chaotic map. A lower MSE value indicates a closer resemblance between the encrypted and original signals, reflecting a reduced level of distortion or information loss. This comparative analysis provides insights into how each chaotic map impacts the fidelity of the encrypted ECG signals across a diverse set of patient data, aiding in the understanding of their effectiveness in preserving signal integrity during the encryption process.

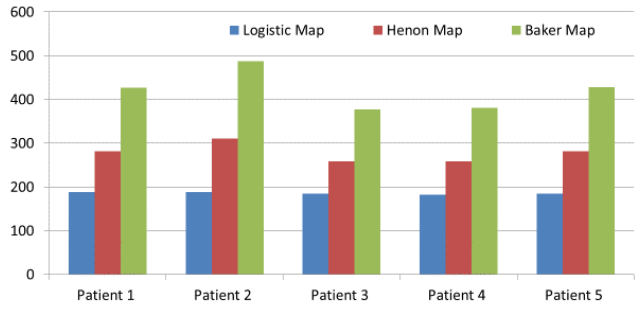


Fig. 9. MSE Comparison

The SSIM values obtained from the comparison of logistic map, Henon map, and Baker map against ECG signals is shown in figure10. The comparison involves evaluating the structural similarity between the original ECG signals and those processed by each chaotic map. The resulting SSIM values provide a quantitative measure of the degree of similarity in structural features, indicating how well each chaotic map preserves the information content of the ECG signals. This analysis aids in understanding the effectiveness of the logistic map, Henon map, and Baker map in maintaining the fidelity of diverse ECG patterns across multiple patients

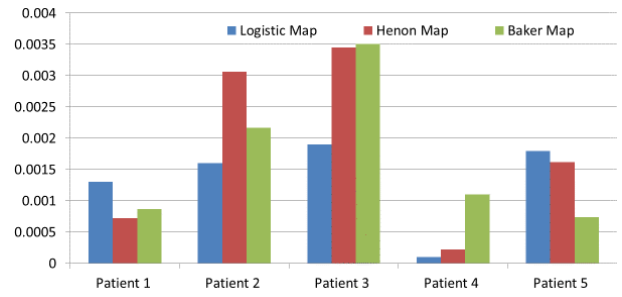


Fig. 10. SSIM Comparison

5. Conclusion

ECG signal encryption is highly relevant in healthcare to ensure the confidentiality and privacy of patients' cardiac health data. Encrypting ECG signals helps prevent unauthorized access, protecting sensitive information from potential breaches and misuse. As healthcare systems increasingly rely on digital platforms for data storage and transmission, robust ECG signal encryption plays a crucial role in maintaining the integrity of medical records and fostering trust in the security of cardiovascular information. The proposed method introduced an advanced three-step encryption scheme for Electrocardiogram (ECG) data, integrating the Chaotic Baker map and Dual Random Phase Encoding (DRPE). The methodology strategically introduces variability and complexity through a randomized fusion of wavelet coefficients, employs a chaos-based encryption scheme with 2-D DWT, and enhances security further with DRPE using two Random Phase Masks. The proposed method, encompassing random projection, salting, and holistic encryption, provides a robust solution for securing sensitive ECG data, addressing the critical need for heightened data protection in medical applications.

References

[1] Badr, M., Al-Otaibi, S., Alturki, N., & Abir, T. (2022). Detection of heart arrhythmia on electrocardiogram using artificial neural networks. Computational Intelligence and Neuroscience, 2022.

[2] Schwartz, P. J., Ackerman, M. J., Antzelevitch, C., Bezzina, C. R., Borggrefe, M., Cuneo, B. F., & Wilde, A. A. (2020). Inherited cardiac arrhythmias. Nature Reviews Disease Primers, 6(1), 58.

[3] Lee, R. H., Lee, M. H., Wu, C. Y., e Silva, A. C., Possoit, H. E., Hsieh, T. H., ... & Lin, H. W. (2018). Cerebral ischemia and neuroregeneration. Neural regeneration research, 13(3), 373.

[4] Borujeni, A. M., Fathy, M., & Mozayani, N. (2019). A hierarchical, scalable architecture for a real-time monitoring system for an electrocardiography, using context-aware computing. Journal of biomedical informatics, 96, 103251.

[5] Estévez-Báez, M., Machado, C., Montes-Brown, J., Jas-García, J., Leisman, G., Schiavi, A., ... & Carmeli, E. (2018). Very high frequency oscillations of heart rate variability in healthy humans and in patients with cardiovascular autonomic neuropathy. Progress in Medical Research, 49-70.

[6] Harinee, S., & Mahendran, A. (2021). Secure ECG signal transmission for smart healthcare. International Journal of Performability Engineering, 17(8), 711.

[7] Pirbhulal, S., Samuel, O. W., Wu, W., Sangaiah, A. K., & Li, G. (2019). A joint resource-aware and medical data security framework for wearable healthcare systems. Future Generation Computer Systems, 95, 382-391.

[8] Vyakaranal, S., & Kengond, S. (2018, April). Performance analysis of symmetric key cryptographic algorithms. In 2018 international conference on communication and signal processing (ICCSP) (pp. 0411-0415). IEEE.

[9] Uppu, R., Wolterink, T. A., Goorden, S. A., Chen, B., Škorić, B., Mosk, A. P., & Pinkse, P. W. (2019). Asymmetric cryptography with physical unclonable keys. Quantum Science and Technology, 4(4), 045011.

[10] Stevens, H. (2018). Hans Peter Luhn and the birth of the hashing algorithm. IEEE spectrum, 55(2), 44-49.

[11] Luo, Y., Yu, J., Lai, W., & Liu, L. (2019). A novel chaotic image encryption algorithm based on improved baker map and logistic map. Multimedia Tools and Applications, 78, 22023-22043.

[12] Faragallah, O. S., Alzain, M. A., El-Sayed, H. S., Al-Amri, J. F., El-Shafai, W., Afifi, A., ... & Soh, B. (2018). Block-based optical color image encryption based on double random phase encoding. IEEE Access, 7, 4184-4194.

[13] Algarni, A. D., Soliman, N. F., Abdallah, H. A., & Abd El-Samie, F. E. (2021). Encryption of ECG signals for telemedicine applications. Multimedia Tools and Applications, 80, 10679-10703.

[14] Alqawasmi, K. E. (2022, May). Estimation of ARMA Model Order Utilizing Structural Similarity Index Algorithm. In 2022 8th International Conference on Control, Decision and Information Technologies (CoDIT) (Vol. 1, pp. 1087-1090). IEEE.

[15] Qiu, H., Qiu, M., & Lu, Z. (2020). Selective encryption on ECG data in body sensor network based on supervised machine learning. Information Fusion, 55, 59-67.

[16] Abdulbaqi, A. S., Obaid, A. J., & Abdulameer, M. H. (2021). Smartphone-based ECG signals encryption for transmission and analyzing via IoMTs. Journal of Discrete Mathematical Sciences and Cryptography, 24(7), 1979-1988.

[17] Abdulbaqi, A. S., Obaid, A. J., & Mohammed, A. H. (2021). ECG signals recruitment to implement a new technique for medical image encryption. Journal of Discrete Mathematical Sciences and Cryptography, 24(6), 1663-1673.

[18] Kh-Madhloom, J., Ghani, M. K. A., & Baharon, M. R. (2021). ECG Encryption Enhancement Technique with Multiple Layers of AES and DNA Computing. Intelligent Automation & Soft Computing, 28(2).

[19] Sharma, S., Chen, K., & Sheth, A. (2018). Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. IEEE Internet Computing, 22(2), 42-51.

[20] Hameed, M. E., Ibrahim, M. M., Abd Manap, N., & Mohammed, A. A. (2020). A lossless compression and encryption mechanism for remote monitoring of ECG data using Huffman coding and CBC-AES. Future generation computer systems, 111, 829-840.

[21] Van Fleet, P. J. (2019). Discrete wavelet transformations: An elementary approach with applications. John Wiley & Sons.

[22] Moffat, A. (2019). Huffman coding. ACM Computing Surveys (CSUR), 52(4), 1-35.

[23] Smid, M. E. (2021). Development of the advanced encryption standard. Journal of Research of the National Institute of Standards and Technology, 126.

[24] Kumar, A. S., & Naik, B. R. (2023). Bilateral hashing model of ECG signal encryption system using downhill peak follow (DPF)-based encryption technique. Soft Computing, 1-9.

[25] Patil, P., & More, S. A. (2022). Analysis of Encrypted ECG Signal in Steganography Using Wavelet Transforms. In Information and Communication Technology for Competitive Strategies (ICTCS 2020) ICT: Applications and Social Interfaces (pp. 411-419). Springer Singapore.

[26] Adithya, B., & Santhi, G. (2022). A DNA Sequencing Medical Image Encryption System (DMIES) Using Chaos Map and Knight's Travel Map. International Journal of Reliable and Quality E-Healthcare (IJRQEH), 11(4), 1-22.

[27] Salem, I. E., Abdulshaheed, H. R., & Gheni, H. M. (2022). A secure telemedicine electronic platform based on lightweight cryptographic approach. TELKOMNIKA (Telecommunication Computing Electronics and Control), 20(5), 988-995.

[28] Apandi, Z. F. M., Ikeura, R., & Hayakawa, S. (2018). Arrhythmia detection using MIT-BIH dataset: A review. Proceedings of International Conference on Computational Approach in Smart Systems Design and Applications, 1-5, IEEE.