IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 May 2024, accepted 29 May 2024, date of publication 31 May 2024, date of current version 10 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3408136

RESEARCH ARTICLE

A New Chaotic Memristor-Based Cryptosystem for Secure Bio-Signal Transmission on Low-Cost Hardware

ACHRAF DAOUI[1], MOHAMED YAMNI[2], PAWEŁ PŁAWIAK[3,4], OSAMA ALFARRAJ[5], AND AHMED A. ABD EL-LATIF[6,7], (Senior Member, IEEE)

[1]National School of Applied Sciences, Université Sidi Mohamed Ben Abdellah, Fes 34000, Morocco
[2]Dhar El Mahrez Faculty of Science, Université Sidi Mohamed Ben Abdellah, Fes 34000, Morocco
[3]Department of Computer Science, Faculty of Computer Science and Telecommunications, Cracow University of Technology, 31-155 Kraków, Poland
[4]Institute of Theoretical and Applied Informatics, The Polish Academy of Sciences, 44-100 Gliwice, Poland
[5]Computer Science Department, Community College, King Saud University, Riyadh 11437, Saudi Arabia
[6]Information Countermeasure Technique Institute, School of Cyberspace Science, Faculty of Computing, Harbin Institute of Technology, Harbin 150001, China
[7]Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebeen El-Kom 32511, Egypt

Corresponding author: Ahmed A. Abd El-Latif (ahmedabdellatif@ieee.org)

This work was supported by King Saud University, Riyadh, Saudi Arabia, through the Researchers Supporting Project under Grant RSP2024R102.

ABSTRACT Motivated by the critical need for securing bio-signal transmissions in resource-constrained Internet of Medical Things (IoMT) devices, this paper proposes a novel lightweight cryptosystem based on a newly developed chaotic map called the Logistic-Coupled Memristor (LCM) map. This map is designed by coupling a discrete memristor with the well-known chaotic logistic map. The LCM exhibits a high degree of sensitivity to even slight changes in its ten control parameters, a crucial property for secure communication. We validate the chaotic behavior of the LCM using various established methods (Lyapunov exponents, bifurcation diagrams, parameter sensitivity analysis, and NIST randomness tests). Furthermore, we demonstrate its implementation on a low-cost microcontroller with limited resources. Building upon the LCM's properties, we propose a novel lightweight cryptosystem for securing the wireless transmission of bio-signals. This cryptosystem is also implemented on a low-cost embedded system, showcasing its potential for real-world applications. Extensive simulations and comparisons confirm that the LCM map retains its chaotic behavior even when implemented on resource-constrained microcontrollers. Additionally, the implemented cryptosystem achieves a high level of security with lower cost in comparison to existing solutions.

INDEX TERMS 1D chaotic system, memristor, microcontrollers, embedded systems, bio-signals, cryptosystems.

I. INTRODUCTION

The rapid growth of digital data (sensor data, video, images, text, audio, etc.) is pushing the boundaries of digital storage, processing, and transmission. The ever-growing volume of these data presents a critical security threat, particularly for highly sensitive information (fingerprints, bio-signals, patient details, financial data, and military data) [1]. Steganographic approaches based on symmetry-based modulation [2], Runge-Kutta methods [3], discrete orthogonal transforms [4], [5], can be successfully employed to achieve concealed communication of such sensitive information.

Robust cryptosystems are often seen as powerful tools for protecting sensitive assets from unauthorized access [6]. These tools ensure a secure communication, where only authorized parties can access the communicated data.

There are two fundamental types of cryptosystems: symmetric and asymmetric. They differ in how they use keys for encryption and decryption. Generally, asymmetric

The associate editor coordinating the review of this manuscript and approving it for publication was Walid Al-Hussaibi.

cryptosystems are considered more secure than symmetric ones due to their separate public and private keys [7]. However, this security comes at the cost of increased complexity and slower processing [8]. Conversely, symmetric encryption offers faster and more efficient execution, especially for large datasets, but requires a secure key sharing. Symmetric algorithms generally have low computational complexity, making them an ideal choice for implementing encryption in resource-constrained environments such as microcontrollers and field-programmable gate arrays (FPGAs) [9].

The excellent properties of chaotic and hyperchaotic systems, including their sensitivity to initial conditions, ergodicity, and pseudo-randomness, make them increasingly attractive for cryptographic applications [10].

As described by Ding et al., the chaotic systems can be categorized into two main types: one-dimensional (1D) and multidimensional (nD) [11]. The nD chaotic and hyperchaotic systems encompass the 2D Lorenz system [12], the 3D Rössler system [13], and other recent high-dimensional chaotic and hyperchaotic systems [14], [15], [16], [17]. High-dimensional chaotic systems typically involve many initial values and control parameters, which contribute to a vast key space for cryptosystems, making them more resistant to brute-force attacks. Furthermore, modern cryptosystems are increasingly leveraging multidimensional chaotic maps with adaptive symmetry [18], allowing for the creation of chaos-based encryption schemes with a larger key space [19], [20], which enhances the security level. However, designing effective control mechanisms for the adaptive symmetry changes in chaotic maps can be challenging [21].

Implementing nD chaotic and hyperchaotic systems comes with a significant increase in processing power and memory consumption compared to lower-dimensional systems [22]. This can pose challenges in resource-constrained environments such as embedded systems. Therefore, chaotic systems with a simple mathematical structure and lower complexity are particularly preferred for cryptosystem implementation in resource-constrained environments [23].

Recently, minimal digital chaotic maps [24], a class of chaotic systems, have been designed with a focus on simplicity and low computational complexity. This makes them particularly attractive for resource-constrained environments. However, the efficiency of minimal chaotic maps comes at a cost. Their simpler design often translates to a smaller key space, which weakens their resistance to brute-force attacks. Therefore, achieving a balance between computational efficiency and robust security in encryption schemes is highly desirable when implementing cryptosystems [25].

Due to their simple mathematical models, 1D chaotic maps are particularly attractive for designing lightweight algorithms that strike a balance between efficiency and security in resource-limited settings [26]. However, most of 1D maps present a common weakness, which is the limited number of initial values and control parameters [27]. This factor can contribute to the vulnerability of 1D chaotic system-based schemes to cyberattacks [27], [28]. To address this limitation, recent research has proposed 1D chaotic system models with multiple parameters [29]. This research funding demonstrates great improvements in the security level of security schemes that are based on the multiparametric 1D maps. Indeed, the improved security level is due to the enhanced chaotic behavior arising from the increased complexity of the 1D chaotic maps through the introduction of multiple parameters into the map models. These parameters function as security keys, securely communicated between the sender and the receiver.

Aiming to improve the security level of cryptosystems based on 1D chaotic maps, researchers are exploring the integration of trigonometric functions into the mathematical models of existing 1D chaotic maps. As an example, the work presented in [30], [31], and [32] improves the chaotic behavior of the well-known logistic map by integrating the sine function. Even though this strategy shows promising results in enlarging the key space of 1D chaotic-based cryptosystems, the exploration of other strategies with enhanced security levels remains an open area for further research. In this regard, memristors have recently gained increasing attention in the study of chaotic oscillations due to their unique combination of nonlinearity and plasticity [33], [34]. These properties make memristors excellent candidates for improving the security level of cryptosystems. Indeed, excellent memristor-based cryptosystems have been recently introduced in the literature [35], [36].

Motivated by the potential of memristors to enhance security systems level, the current work proposes a new 1D chaotic map model named the Logistic -Coupled Memristor (LCM) map. This model merges the traditional discrete Hewlett-Packard (HP) memristor [37] with the logistic map, resulting in a system with ten highly sensitive control parameters ideal for use as security keys in cryptosystems. Therefore, the LCM-based cryptosystems are predicted to offer improvements in the security level compared to existing ones.

Recent work [29] demonstrates the feasible implementation of multiparametric 1D chaotic maps on resource-constrained hardware. The successful implementation of multiparametric 1D chaotic maps on resource-constrained hardware is significant. It opens new possibilities for broader applications of these maps, particularly in Cyber-Physical Systems (CPS), and Internet of Things (IoT), which often rely on smaller embedded systems, less complex processors due to size and power limitations [38], [39]. Driven by this interest, the present work presents an implementation of the proposed chaotic map on a low-cost resource-constrained microcontroller.

The Internet of Medical Things (IoMT), a subset of the IoT, typically relies on resource-constrained embedded devices. These devices are often built with smaller chips, low-cost and less complex hardware, resulting in both a compact size and lower power consumption [40]. According

to Yaacoub et al. [41], securing data communication in IoMT is crucial for both preserving patient trust and ensuring the reliable and secure functioning of these modern technologies.

Cryptosystems play a crucial role in securing data communication within the IoMT. Therefore, the design of lightweight and secure cryptosystems holds significant importance for the IoMT [42].

Biomedical signals (Bio-signals), such as electrocardiograms (ECGs), electroencephalograms (EEGs), electromyography (EMG), and photoplethysmography (PPG), are widely communicated between various IoMT users and devices for diagnostic tests purposes [43]. The bit resolution and sampling rate used to represent bio-signal samples can differ between bio-signals [44]. Therefore, the chosen encryption method should be adaptable to these variations in data representation, especially when the encryption is performed during the real-time data acquisition phase.

The significant interest in secure communication for bio-signals motivates the development of novel cryptosystems. This work proposes a new, secure, and lightweight bio-signal cryptosystem based on the proposed LCM. Next, a low-cost embedded system implementation of the suggested cryptosystem is presented, demonstrating its applicability and practical feasibility. This implementation, adopting a wireless communication that is commonly used in IoMT applications [40], [45], [46], aligns well with the intended use case.

The main contributions of this work can be summarized as follows:

∗ Introducing a novel 1D multiparametric LCM chaotic map and analyzes its chaotic behavior on the resource constrained ATMega328P microcontroller.

∗ Proposing a new lightweight confusion-diffusion cryptosystem for secure wireless bio-signal communication.

∗ Providing a low-cost embedded system implementation of the proposed cryptosystem.

∗ Providing simulation and comparison results that demonstrate the high security and real-world feasibility of our cryptosystem.

The paper is further organized as follows: Section II reviews related work and discusses its implications. Section III introduces the fundamental preliminaries used in this work. Section IV details the proposed LCM, its analysis, and its implementation on a microcontroller. Section V details the steps involved in the proposed bio-signal cryptosystem and its low-cost embedded implementation. Section VI presents the simulation and comparison results, demonstrating the high security level of the proposed cryptosystem. Section VII concludes the work and discuss its potential future extensions.

II. RELATED WORK WITH DISCUSSION

Recently, the use of 1D chaotic maps has undergone a significant evolution due to their ease of software and hardware implementation. Indeed, several 1D chaotic maps have been recently introduced and employed in various information security applications.

An analysis of data in Table 1 reveals that 1D chaotic systems are increasingly utilized in various signal security applications including image encryption, speech encryption, text encryption, etc. Also, the implementation of 1D chaotic system-based cryptosystems on microcontrollers is increasingly being developed. However, a major limitation of 1D chaotic systems is their low number of control parameters, which results in limited cryptographic strength when used in cryptosystems [28]. Recent work addresses this limitation by proposing 1D chaotic systems with improved chaotic behavior and multi-control parameters, enhancing the security of 1D-chaotic-system-based cryptosystems [27], [47]. These multiparametric maps have proven their advantages in significantly improving the security level of cryptographic schemes by enlarging the key space of the designed schemes. Therefore, designing 1D multiparametric chaotic systems with robust chaotic behavior is essential for guaranteeing secure data communication over various communication channels.

Recent research [29], [48], [49], has shown that coupling memristor characteristics with 1D chaotic maps significantly enhances the unpredictability of 1D chaotic systems. Building on these promising results, this paper proposes the 1D LCM map by coupling the traditional logistic map with a discrete memristor. The key advantage of this new map is its increased number of control parameters, which can offer a large security key space for cryptographic applications.

The cost-effective hardware implementation of discrete 1D chaotic maps coupled with memristors, as demonstrated in [29], paves the way for wider adoption in security systems. This makes the implementation of cryptosystems on hardware based on these coupled systems highly interesting, showcasing the potential for real-world integration. Driven by this potential, the current work demonstrates the feasibility of implementing the proposed map on a resource-constrained microcontroller, solidifying its practical use.

The key advantages of the suggested LCM-based cryptosystem can be summarized in the following points:

A. ENHANCED SECURITY LEVEL

The LCM map boasts ten control parameters, which can significantly improve the LCM-based cryptosystems resistance to brute-force attacks compared to existing 1D chaotic systems with fewer parameters.

B. LIGHTWEIGHT AND EFFICIENT DESIGN

The current work successfully implements the LCM map on a low-cost microcontroller. This demonstrates its potential for use in resource-constrained environments, such as Internet of Medical Things (IoMT) devices.

C. FOCUS ON REAL-WORLD APPLICATION

The current work goes beyond simply proposing the LCM map. It presents a lightweight LCM-based cryptosystem

specifically designed for securing bio-signal wireless communication in IoMT. This focus on a practical application with its own unique requirements strengthens the value proposition of the LCM map.

III. PRELIMINARIES

This section outlines the preliminary concepts used in our work, including the discrete memristor model and the 1D chaotic logistic map.

A. DISCRETE MEMRISTOR

Decades of electrical component design were dominated by the three main elements: resistors, capacitors, and inductors. However, in 1971, Leon Chua thought of a hitherto absent element: the Memristor (M), a component consisting of a memory and a resistor [64]. The theoretical existence of M remained in the minds of engineers until 2008, when a pioneering team at Hewlett-Packard Laboratories [37] demonstrated its existence through ingenious partial doping. Since then, the memristor has been increasingly integrated into various fields of engineering applications.

The memristor is considered as a memory device due to the movement of dopants within its structure. This characteristic is modeled by the length of the doped region (w), which varies between zero and the total device length (D). The instantaneous resistance of the memristor is given as follows [37]:

$$R(t) = \frac{dq}{d\phi} = \frac{v(t)}{i(t)} = \chi R_{ON} + (1-\chi)R_{OFF} \text{ with } \chi = w/D \quad (1)$$

where q is the charge, ϕ represents the flux, $R(t)$ is the instantaneous resistance, w is the Memristor state variable, $v(t)$ is the input voltage and $i(t)$ is the current. R_{ON} denotes the fully doped resistance, and R_{OFF} the resistance of the completely undoped M with $R_{ON} \ll R_{OFF}$.

The instantaneous resistance of M can be generalized for linear dopant drift as follows [37] and [65]:

$$R(t) = \sqrt{R_0^2 - 2kR_d d\phi(t)}$$
$$\text{with } R \in (R_{ON}, R_{OFF}) \text{ and } k = \frac{\mu_v R_{ON}}{D^2} \quad (2)$$

where R_0 is the initial resistance at $t = 0, R_d = R_{OFF} - R_{ON}$ is the boundary resistance difference, k is dopant drift mobility and μ_v represents the dopant drift mobility of the device material and $\phi(t)$ is the flux at instant t that is computed by [65]:

$$\phi(t) = \int_{t_0}^{t_n} v(\tau)d\tau \approx \sum_{k=1}^{n} \frac{1}{2}(v(t_k) + v(t_{k-1}))\Delta t_k \quad (3)$$

where $v(t_k)$ represents the voltage at time t_k, and Δt_k is the time step between t_k and t_{k-1}.

The memristor in Eq. (1) is controllable via the parameters $R_0, \mu_v, D, R_{ON}, R_{OFF}$ and f. These parameters can therefore be used as security keys for a chaotic map, which allows for a significant increase in the key space of cryptosystems. In addition, the integration of the memristor into cryptosystems can improve the complexity of these systems, which provides a higher level of security.

The following subsection introduces a brief yet informative description of the traditional logistic map.

B. LOGISTIC MAP

The logistic map (LM) is widely used in cryptosystems due to its inherent characteristics of sensitivity to initial condition and control parameter, as well as its pseudo-random behavior. Additionally, its implementation is straightforward due to its simple mathematical model, which is given by [66]:

$$X_i = \rho X_{i-1}(1 - X_{i-1}) \text{with } X_i \in (0, 1) \quad (4)$$

The behavior of the LM becomes chaotic when $\rho \in [3.54, 4]$ and $0 < X_0 < 1$.

IV. PROPOSED LOGISTIC-COUPLED MEMRISTOR MAP AND ITS MICROCONTROLLER IMPLEMENTATION

A. MATHEMATICAL MODEL

Starting from the premise that coupling classical 1D chaotic systems with HP memristor, which offer a wide range of control parameters, can significantly enhance the security level of cryptographic systems by introducing unpredictable dynamics and greater control flexibility, the present work introduces the next model of the proposed LCM:

$$L_t = \text{mod}(4 \times (1 - G_1 \times |i(t)|)L_{t-1} \times (1 - X_{t-1} + G_2 \times i(t)), 1) \quad (5)$$

where $mod()$ and $|.|$ are the modular and the absolute value operators, G_1 and G_2 are real gains, $i(t)$ represents the current at time t passing across the memristor, which is given by:

$$i(t) = \frac{v(t)}{R(t)} \quad (6)$$

Eq. (5) reveals that the LCM's nine tunable control parameters $(R_0, \mu_v, D, R_{ON}, R_{OFF}, fAmp, G_1$ and $G_2)$ in addition to the initial value $L_0(0 < L_0 < 1)$. L_0 is selected in this interval because the proposed LCM is based on the classical LM, whose initial value falls within the range [0-1].

The LCM flexibility, along with the wider range of parameters, suggests richer and more unpredictable chaotic behavior, offering cryptosystem users greater control over fine-tuning security levels or adjusting the system's dynamics.

It's important to note that the LCM in Eq. (5) is based on a nonlinear mathematical model of the HP discrete memristor. However, the hardware realization of this model may exhibit different behavior.

The following section delves into the chaotic dynamics of LCM to demonstrate its rich and unpredictable behavior, desirable characteristics for robust cryptographic systems.

TABLE 1. Review of recent 1D Chaotic Maps with their Properties, applications, and hardware implementation.

1D chaotic map reference	Number of control parameters	Application	Implementation on a Hardware?	Used Hardware	Embedded system implementation?
Talhaoui & Wang [50]	2	Image encryption	No	-	No
Talhaoui et al. [51]	2				
Wang et al. [52]	2				
Belazi et al. [53]	1				
Zhu et al. [54]	1				
Rong et al. [55]	1				
Zhu et al. [56]	3				
Liu & Wang [57]	3				
Daoui et al. [27]	6				
Yamni et al. [4]	4	Image steganography	No	-	No
Daoui et al. [47]	8	Lossless image compression-encryption	No	-	No
Charalampidis et al. [58]	3	Speech encryption	Yes	STM32 microcontroller	Yes
Janakiraman et al. [59]	1	Image encryption	Yes	LPC2148 microcontroller	Yes
Murillo-Escobar [60]	2	Text encryption	Yes	Atmel AVR Microcontroller	Yes
Yihyis et al. [48]	3	-	No	-	No
Li et al. [49]	4	-	No	-	No
Bao et al. [29]	5	-	Yes	STM32F407 microcontroller	No
Fan et al. [61]	4	Medical data encryption	No	-	-
Murillo-Escobar [62]	1	Bio-signal Encryption	No	-	-
Pandey et al. [63]	3	ECG bio-signal Encryption	No	-	-
This work	**10**	**Bio-signal Encryption**	**Yes**	**ATmega328P microcontroller**	**Yes**

B. CHAOTIC BEHAVIOR ANALYSIS

The bifurcation diagram is considered a valuable visualization tool for showing the dynamic behavior of chaotic maps across a range of control parameters.

Figure 1 shows the bifurcation diagrams of LCM with respect to its control parameters. To obtain these diagrams, the LCM parameters are initially set to:

$$\mu_v = 10^{-14},\ D = 10 \times 10^{-9},\ R_{ON} = 200,$$
$$R_{OFF} = 40 \times 10^3, R_0 = 2 \times 10^3, G_1 = 8,$$
$$G_2 = 9 \text{ and } L_0 = 0.3.$$

From Figure 1, it's evident that the LCM exhibits rich chaotic behavior when its control parameters are varied. This observation provides strong evidence for the chaotic nature of the LCM. Investigating this behavior further, the Lyapunov Exponent (LE) is calculated when varying LCM control parameters within the ranges given in Figure 1.

Figure 2(a) reveals that the LCM retains its chaotic character across parameter variations, with consistently positive LE values. This empowers users to dynamically adjust these parameters as safety keys, enhancing the security level of cryptosystems through controlled unpredictability. Furthermore, Figure 2(b) displays the LCM's clear advantage over its original version. Indeed, LE values achieved via LM are higher than the original LM's. These results make the LCM a strong candidate for applications requiring unpredictable dynamics and secure communication.

Encouraged by the sustained positive LE values and enhanced unpredictability of the LCM demonstrated in the current analysis, the next step is to implement it on a low-cost microcontroller. This will explore the parameter sensitivity and real-time performance of its chaotic behavior, thereby demonstrating its practical feasibility for real-world applications. With this understanding, the LCM's chaotic dynamics can be harnessed for a potential application in digital signal security using low-cost embedded systems.

C. MICROCONTROLLER-BASED IMPLEMENTATION OF LCM

Implementation of chaotic maps on microcontrollers is an important technology for developing and deploying high-performance, energy-efficient, and reliable chaotic systems in real-world applications. Microcontrollers are particularly well-suited for real-time operations and interaction with the physical world. In this work, the ATmega328P microcontroller is used to implement the LCM. This microcontroller is a popular choice for embedded systems because it is relatively inexpensive, easy to use, and widely available. It is also used in many Arduino boards (Arduino Uno and Arduino Nano), which makes it a good choice for rapid prototyping and development. In the present work, the embedded Arduino Nano board is used to implement the LCM.

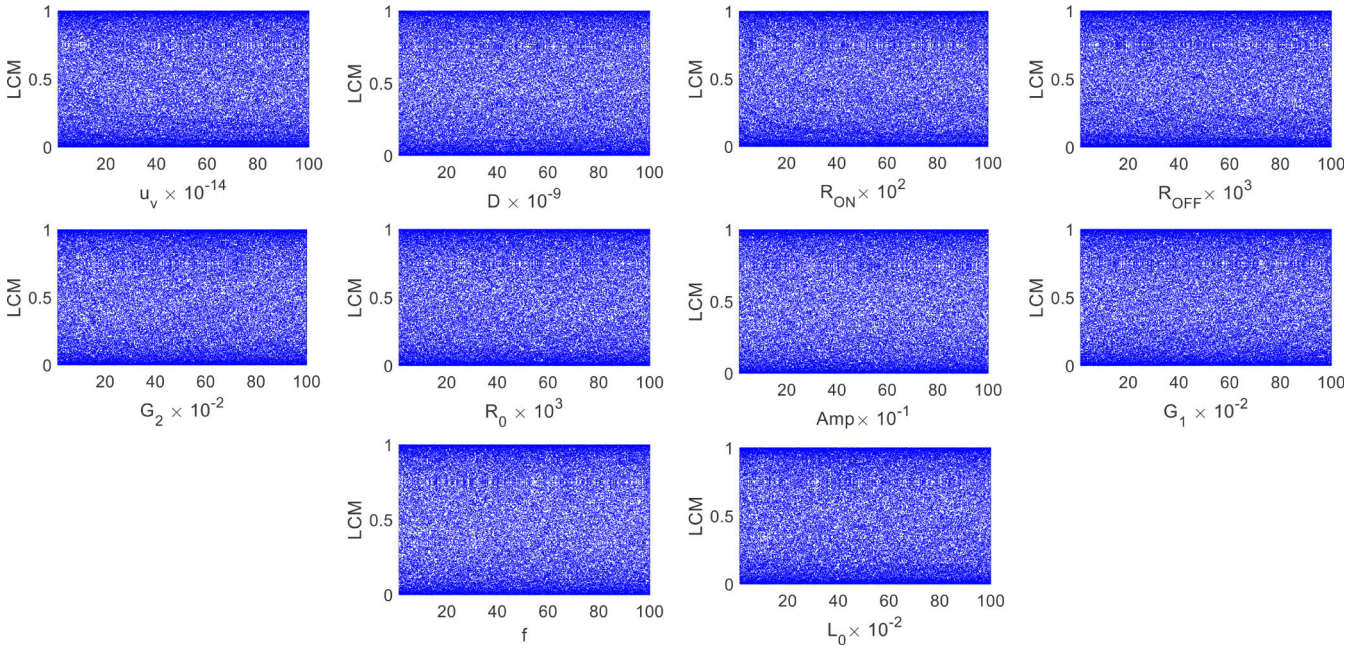


FIGURE 1. Bifurcation diagrams of the LCM for its control: R_0, μ_v, D, R_{ON}, R_{OFF}, f, Amp, G_1, G_2 and L_0.

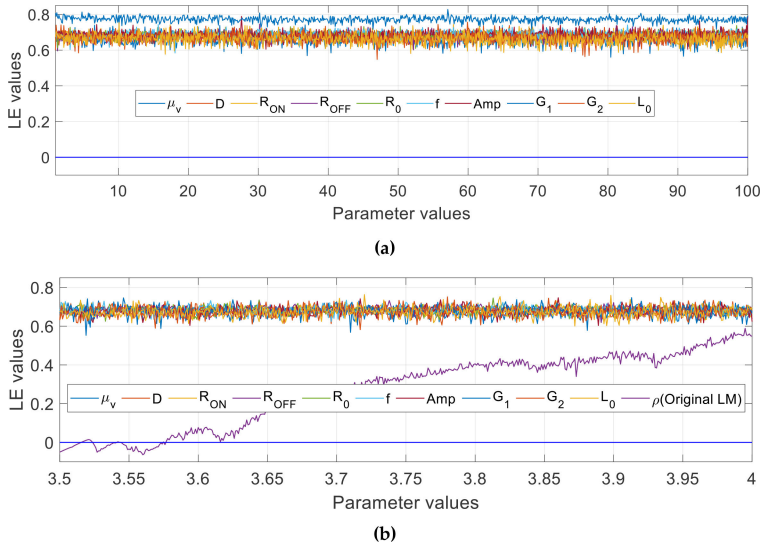


FIGURE 2. (a) Impact of LCM parameter variations on LE values. (b) Comparison in terms of LE values between the original LM and the proposed LCM.

The Arduino Nano has a small size (approximately 45 mm long, 18 mm wide, and 7 grams weight), low-cost and low power consumption [67]. This makes it a good choice for Internet of Things (IoT) projects where both limited space and battery life are important [68]. The Arduino Nano has 14 digital input/output pins, 8 analog inputs, 16 MHz ceramic resonator, and a Mini-B USB connection. It can be powered via a regulated 5V external power supply. The Arduino Nano is built around the ATmega328P microcontroller, which boasts a versatile set of features making it well-suited for a wide array of computational tasks. It offers 32 KB of flash memory and 2 KB of SRAM, along with 10-bit analog-to-digital converters. Furthermore, the ATmega328P provides robust support for various arithmetic and logical operations. The open-source Arduino Software (IDE) is used to compile and upload the software script (in C language) to the Arduino Nano board.

The LCM model described by Eq. (5) is implemented on the Arduino Nano by writing it in C and uploading it through the Arduino IDE. The model's outputs, which are numerical floating values in the range [0-1], are then transmitted via serial communication to the laptop and collected using the open-source Ard-Spreadsheet tool [6]. The communication utilizes a baud rate of 9600 bits/s. The LCM sketch consumes 4400 bytes (14%) of program storage space and the global variables use 208 bytes (10%) of

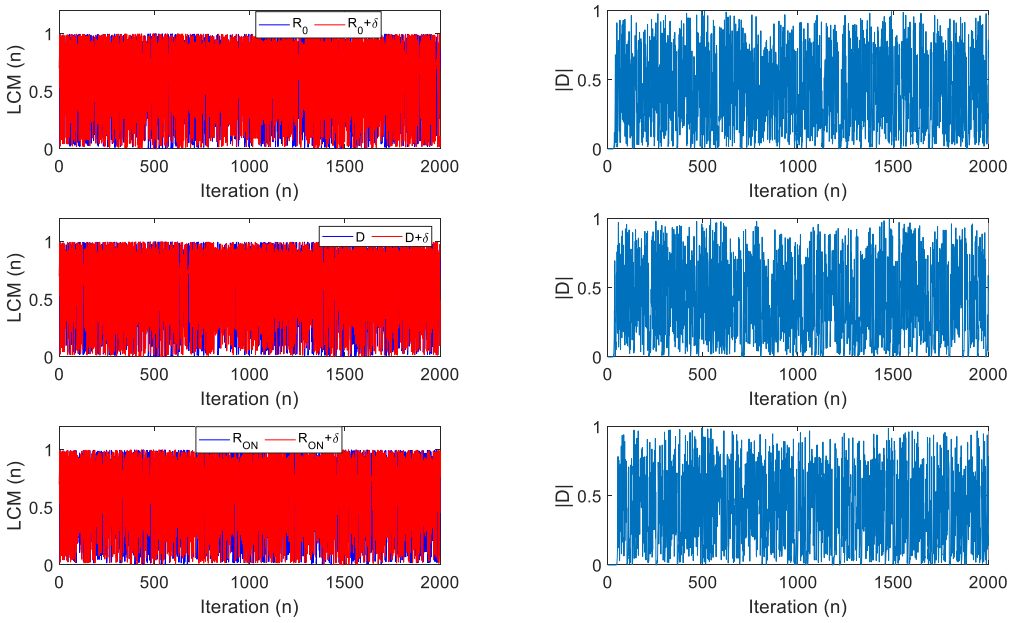


FIGURE 3. (a) Original LCM sequences and those influenced by a variation of $\delta = 10^{-6}$ in LCM control parameters. (b) The absolute difference between the original and influenced sequences.

dynamic memory, which means that the LCM code is optimal in terms of memory usage.

After successfully implementing the LCM on the Arduino Nano, the crucial next step is to verify its chaotic behavior, particularly its sensitivity to initial conditions and control parameters. This will involve analyzing the real-time sequence obtained via the serial monitor.

D. SENSITIVITY OF THE LCM CONTROL PARAMETERS

In real-world applications, the control parameters of chaotic systems serve as security keys. It is therefore predicted that even small variations in these parameters will induce significant changes in the output of the LCM model. To verify this assumption, a chaotic sequence of length L =2000 is initially generated using LCM with the following control parameter values: $\mu_v = 10^{-14}, D = 10 \times 10^{-9}, R_{ON} = 200, R_{OFF} = 40 \times 10^3, R_0 = 2 \times 10^3, G_1 = 8, G_2 = 9, f = 1, Amp = 5$ and $L_0 = 0.3$. Subsequently, each parameter is individually varied by $\delta = 10^{-6}$, and the chaotic sequence is regenerated for each variation. This enables the assessment of the impact of small parameter modification on the resulting chaotic sequences.

It's important to note that the ATmega328P microcontroller can perform arithmetic operations with up to approximatively 7 decimal places of precision for floating-point values. For this, $\delta = 10^{-6} < 10^{-7}$ is chosen to maintain the numerical stability and precision for the LCM output sequences while remaining compatible with the Arduino Nano's capabilities. However, some decimal numbers cannot be accurately represented in binary, and therefore rounding errors may occur when storing and performing calculations with them.

Figure 3(a) displays the first 2000 values of original chaotic sequence generated using the LCM algorithm with the ones generated after a small control parameters variation. In Figure 3(b), we plot the difference in absolute value following the small parameter variation.

The results in Figure 3 demonstrates that even slight changes in the LCM parameters significantly alter the chaotic map output, highlighting its high sensitivity to its control parameters variation. The achieved results confirm the potential use of the LCM control parameters as security keys in cryptosystems.

The following test is designed to further investigate the pseudo-random nature of LCM-based sequences for possible application in digital signal encryption.

E. NIST TEST

This section presents the performance of the NIST (National Institute of Standards and Technology) Statistical Test Suite (STS) for the proposed LCM. The NIST STS is commonly used to assess the random behavior of binary chaotic sequences. There are 15 random statistical tests in the NIST STS, as listed in Table 2.

In this analysis, 200 binary sequences are generated via LCM implemented on Arduino Nano. Each sequence size is 10^6 bits. Next, the average p-value of these sequences is computed and then reported in Table 2. Generally, when p is higher or equal to α^{-1} with $\alpha = 0.01$, then the sequence is considered to pass the test and is therefore considered pseudo-random according to Bassham III et al. [69]. The achieved results in Table 2, with high proportions (close to 1), are a positive indicator regarding the LCM map's ability to generate random sequences over long periods. Therefore,

TABLE 2. Results of NIST test obtained through the proposed LCM.

Statistical Test	p-value	Proportion	Result
Frequency (Monobit)	0.7450	0.9850	Passed
Block Frequency	0.3916	0.9940	Passed
Runs	0.5511	0.9980	Passed
Long Runs of Ones	0.6902	0.9920	Passed
Rank	0.5011	0.9920	Passed
Spectral DFT	0.6987	0.9910	Passed
Non-overlapping Template Matching	0.1819	0.9920	Passed
Overlapping Template Matching	0.9081	0.9950	Passed
Maurer's "Universal Statistical"	0.8911	0.9840	Passed
Linear complexity	0.2613	0.9900	Passed
Serial 1	0.4188	0.9920	Passed
Serial 2	0.5845	0.9940	Passed
Approximate Entropy	0.2123	0.9910	Passed
Cusum-Forward	0.2679	0.9940	Passed
Cusum-Reverse	0.4001	0.9900	Passed
Random Excursions	0.5788	0.9890	Passed
Random Excursions Variant	0.1900	0.9930	Passed

the LCM-based sequences have the potential to be used effectively in high-security data encryption systems.

Following the verification of the chaotic behavior of the LCM, the next section explores its practical application in a real-world scenario: encrypting bio-signals within the IoMT domain.

V. PROPOSED LIGHTWEIGHT ENCRYPTION SYSTEM FOR SECURE BIO-SIGNAL COMMUNICATION

This section includes the design of the proposed bio-signal cryptosystem software and its implementation on a low-cost microcontroller-based embedded system. The implementation is provided to showcase the efficiency gains achievable on resource-constrained environment.

A. SOFTWARE DESIGN FOR THE PROPOSED CRYPTOSYSTEM

Securing the exchange of sensitive medical data, including bio-signals, in the IoMT presents unique challenges due to resource constraints on devices and real-time data transmission requirements. With the aim to address these concerns, high-performance lightweight software design for bio-signal encryption is presented in the current section. Figure 4 shows the diagram of the proposed cryptographic system phases and further details are described below.

The encryption process of the proposed scheme unfolds in the following key steps:

1) DATA PREPARATION

This step involves downloading pre-processed bio-signals data from medical devices into a local database before its secure transmission. It should be noted that each bio-signal sample used in this work is an unsigned positive integer represented on 8-bits.

2) DATA PRE-PROCESSING

Limited processing power and hardware limitations in IoMT devices, necessitate segmenting the bio-signal into smaller portions. For this, the input signal, S, is divided into equal-sized segments. Each segment holds L samples, typically of few samples (e.g., 16, 32, 64), because of memory limitations of the device. The segment size can be adopted for achieving a trade-off between security and reliability of the developed security algorithm.

3) CONFUSION PROCESS

In digital signal encryption, confusion disrupts connections between adjacent samples, thwarting attacks that exploit such dependencies. Guessing samples based on neighbors, a key attack strategy, becomes much harder, hindering efforts to break the encryption through statistical analysis. For this reason, the current process is crucial when it comes to developing a secure encryption system.

Inspired by recent studies introduced by Daoui et al. [27], [43], [70] praising its fast execution and ability to disrupt information, our system employs a chaotic circular shift-based confusion for the input bio-signals. This technique effectively scrambles sample values, hindering attempts to exploit patterns and significantly enhancing encryption security. Algorithm 1 (see Appendix section) details the chaotic circular shift confusion applied to each input signal segment.

4) DIFFUSION PROCESS

The present algorithm's stage involves diffusing the previously confused segment to further enhance security and resist statistical attacks. For this purpose, the next operation is performed for each sample in the confused segment:

$$Diff(i) = SegC(i) \times \text{mod}(L(i) \times 10^5, 256); i \in N \quad (7)$$

where $SegC(i)$ is the confused signal sample, $L(i)$ represents a chaotic value generated by the proposed LCM at the i^{th} iteration and *mod* denotes the modular function.

After the diffusion process, the encrypted signal can be transmitted via IoMT channels to authorized receivers.

5) DECRYPTION PHASE

At the receiver's side, the decryption phase, mirroring the encryption steps, is performed to retrieve the original signal. Consequently, the authorized user must employ security keys that are symmetrical to the ones used in the encryption phase.

B. LOW-COST EMBEDDED SYSTEM IMPLEMENTATION OF THE PROPOSED CRYPTOSYSTEM

By providing an embedded system implementation of the proposed cryptosystem can offer a valuable tool for exploring and validating the effectiveness of our scheme for secure bio-signal data transmission, with potential benefits for patient privacy, healthcare applications, and research & development in the IoMT.

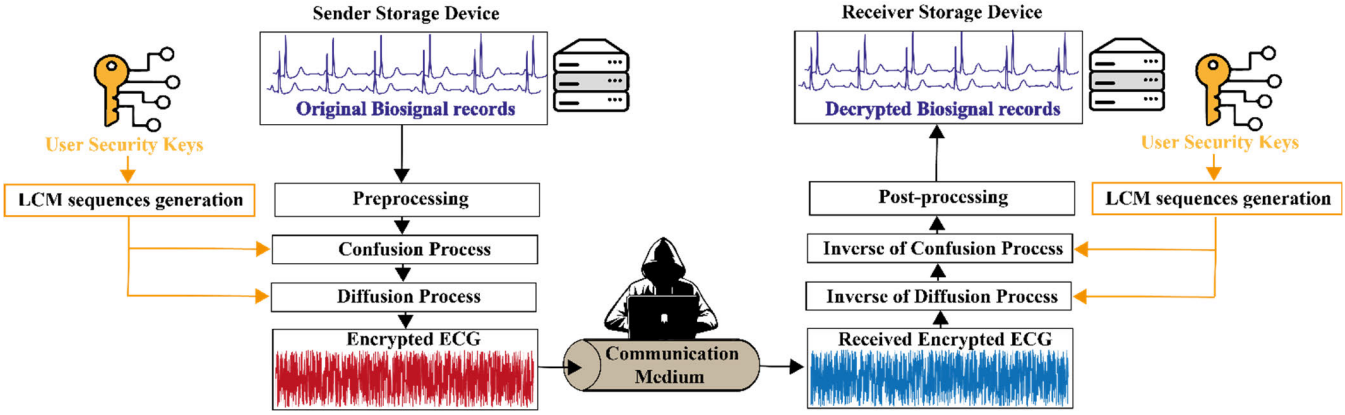


FIGURE 4. Diagram of the proposed LCM-based bio-signal cryptosystem phases.

In the current work, two Arduino Nano boards equipped with ATmega328P microcontrollers, two Bluetooth H-05 modules and two SD cards supported by two SD card modules are used for prototyping our cryptosystem. Figure 5 depicts the embedded system components used to prototype the proposed cryptosystem.

1) ARDUINO NANO BOARDS

The Arduino Nano, renowned for its miniature size, affordability, and power efficiency, forms the core hardware of our project. Equipped with the ATmega328P microcontroller.

In this work, the ATMega328P is used to demonstrate the feasibility of implementing the proposed LCM and lightweight cryptosystem on resource-constrained devices. Future deployments could benefit from exploring more powerful microcontrollers (e.g., ESP32, STM32F4, Raspberry Pi Pico) for performance improvements.

It is important to note that the 8-bit architecture of the ATMega328P hinders its ability to efficiently perform floating-point calculations. Lacking a dedicated Floating-Point Unit (FPU), the microcontroller relies on software emulation to perform floating-point calculations, which are significantly slower and less precise. Despite this limitation the ATMega328P can be successfully used to implement the proposed LCM and other discrete chaotic maps introduced by Ávalos-Ruíz et al. [71], Hoang et al. [72], and Ablay [73], even though these maps are often based on floating-point calculations.

2) MICRO SD CARDS AND THEIR MODULES

Microcontrollers like the ATMega328P play a crucial role in the IoMT. However, their limited onboard memory often restricts their use in complex healthcare projects requiring extensive data storage. This is where SD cards come in, offering gigabytes of space to store sensor data, such as biomedical signals. For efficient data storage in our wireless cryptosystem, SD cards are utilized to hold both the transmitted and the received signals.

SD cards with a storage capacity of 2 GB and write speeds of up to approximately 1.5 MB/s are used in this work. However, depending on the size of the bio-signal database to be securely transmitted between the sender and the receiver, SD cards with higher storage capacities and higher write speeds can be suitable.

3) BLUETOOTH MODULES

Offers a valuable and versatile communication tool for various IoMT applications, particularly in short-range, low-power scenarios. In the proposed encryption scheme, Bluetooth is used as the supporting communication medium to transfer data between the sender and receiver. In this context, Bluetooth's Primary-Secondary architecture is used to create secure communication channel between the sender and receiver devices.

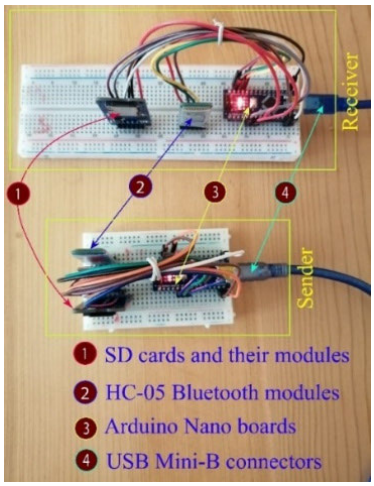
In the current work, two HC-05 Bluetooth modules are used and configured in a primary-secondary communication mode. The baud rate 38400 bps is selected to establish the communication between these modules, balancing data transfer speed with power consumption for the low-power nature of the HC-05. Furthermore, the distance between the sender and receiver is limited to less than 10 meters due to the use of Bluetooth communication, which offers short-range wireless capabilities.

HC-05 Bluetooth modules effectively demonstrate the wireless communication between the sender and the receiver in our work. However, for IoMT applications requiring high data transmission speed over longer range, alternative options such as Wi-Fi module become more suitable [40].

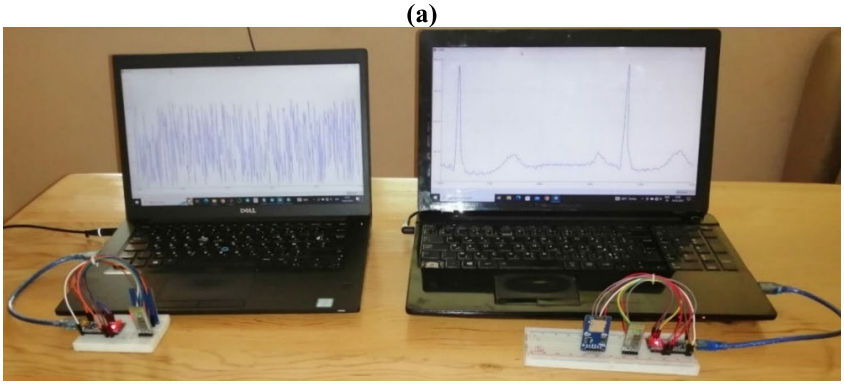
4) MONITOR SCREENS

Provide a visual interface for users and administrators to interact with encryption and decryption processes, enhancing the user experience and contributing to the effective implementation of cryptographic security measures through visual feedback. While visual representation on monitors enhances the user experience, it is not essential for the core functionality of our cryptosystem.

During development, we used two personal laptop screens: one for the sender to view the encrypted signal before



(a)



(b)

FIGURE 5. (a) Used sender/receiver hardware components for prototyping the proposed cryptosystem. (b) The proposed embedded cryptosystem in real-time functionality.

transmission, and another for the receiver to view the decrypted signal. These screens are valuable for monitoring the system, but they are not necessary for its operation and can be eliminated once functionality is ensured.

The next section of our work is devoted to the presentation of the simulation results generated by the proposed encryption system.

VI. SIMULATION RESULTS

This section evaluates the performance of the proposed cryptosystem. For this purpose, bio-signals including electrocardiograms (ECG), blood pressure signals (BP), electroencephalograms (EEG), electromyograms (EMG), etc. are obtained from the public PhysioBank ATM dataset [74] to be used in the simulation tests. It's important to note that PhysioBank stores various bio-signals acquired with different sampling rates and bit depths. For this reason, we normalize the selected bio-signals to the range [0-255]. This ensures that each sample is represented by 8-bit depth. This preprocessing step offers the next advantages:

(i) Reduced Memory Footprint: Bio-signal data from PhysioBank can be quite large, especially with high sampling rates and bit depths. Normalizing to 8 bits significantly reduces the memory required to store and process the data. This is crucial for resource-constrained embedded systems like the ATmega328P, which typically have limited memory capacity.

(ii) Improved Processing Efficiency: Lower bit depth data requires less processing power to manipulate and analyze. This translates to faster execution times and lower power consumption, both of which are essential considerations for battery-powered devices.

(iii) Compatibility with ATmega328P Architecture: The ATmega328P microcontroller is an 8-bit architecture, meaning it natively works with 8-bit data units. By normalizing to 8 bits, we ensure seamless integration and processing of the bio-signals on this platform.

It is also important to mention that the software algorithm for the proposed lightweight encryption system is written in the C programming language and then implemented on both the sender (Arduino Nano primary) and receiver (Arduino Nano secondary) boards to evaluate its performance.

After preprocessing, the bio-signals are stored on the Primary's SD card. The Primary's Arduino Nano then encrypts them, transmits them wirelessly over Bluetooth, and the Secondary's Arduino Nano decrypts them and stores them on the SD card. The received encrypted signals are also stored on the receiver's SD card for further analysis.

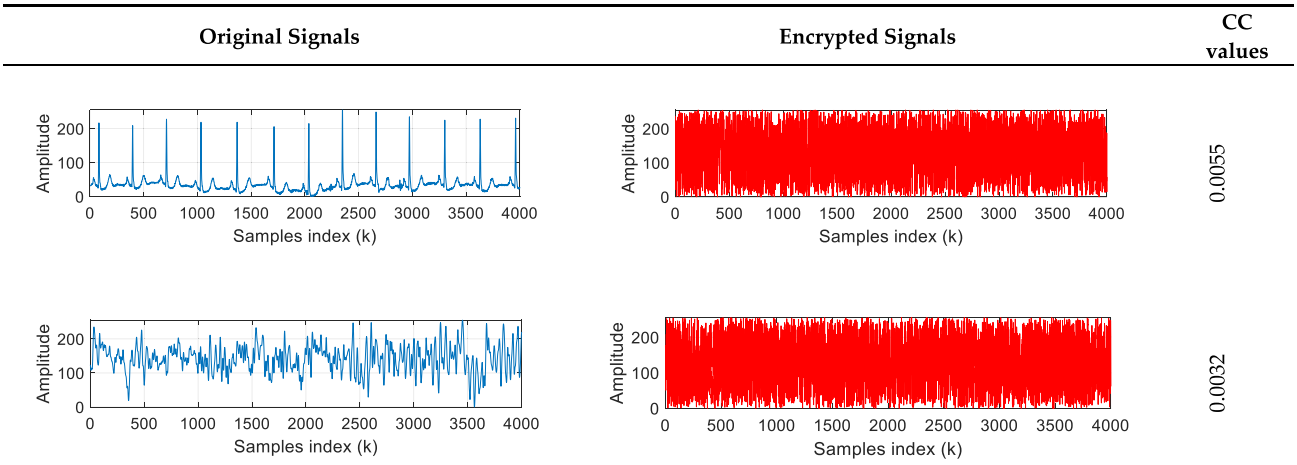


FIGURE 6. Original bio-signals with their encrypted versions and CC values.

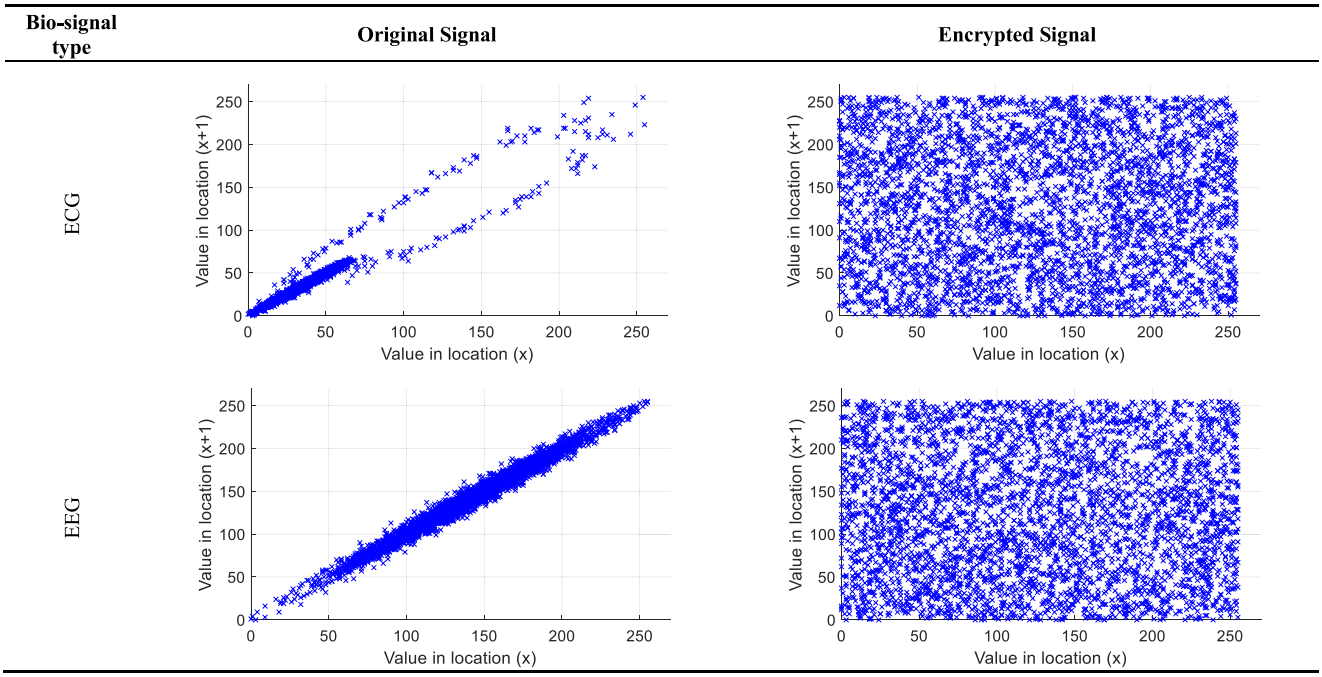


FIGURE 7. Autocorrelation diagrams of the input ECG labeled ≪ 106 ≫ and EEG labeled ≪ 124 ≫ and their corresponding encrypted versions.

A. KEY SPACE ANALYSIS

Demonstrating the encryption scheme's resistance to brute-force attacks from modern computers necessitates key space analysis. Generally, larger key size typically leads to a larger key space, making brute-force attacks more challenging. The sensitivity of security key components to small variations can indirectly influence the effective key space of a cryptosystem.

The proposed cryptosystem uses a security key consisting of 10 components $KEY = \{R_0, \mu_v, D, R_{ON}, R_{OFF}, f, Amp, G_1, G_2, L0\}$, each of which is sensitive to any variation of 10^{-6}. Thus, the total key space of the proposed cryptosystem is $10^{(6\times10)} = 10^{60} \approx 2^{200}$.By exploiting this space, a key with 100 hexadecimal values (400-bit) can be constructed. This key is largely sufficient to resist brute-force attacks through modern computers [75].

B. CORRELATION ANALYSIS

Most secure cryptosystems aim to produce seemingly random ciphertext, in which no statistical patterns or relationships exist between the plaintext and the ciphertext or among different ciphertext blocks. To assess this property, we perform the current analysis to investigate the correlation between adjacent values in the ciphertexts generated by our scheme.

For this analysis, bio-signals of various type are arbitrary selected from the dataset used in the current work. Next, the absolute correlation coefficient (CC) between adjacent values of both the original signals and their encrypted versions is

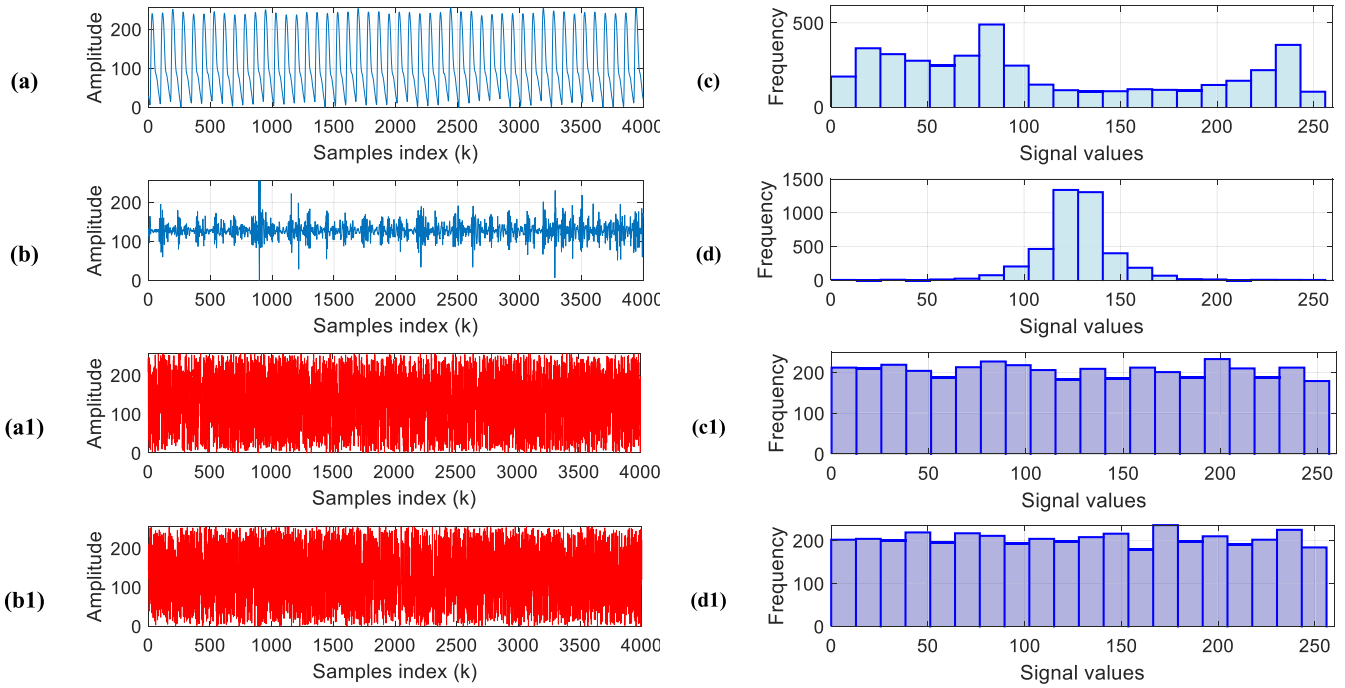


FIGURE 8. (a) PPG labeled ≪ bidmc07 ≫, (b) PPG labeled ≪ fetal_PCG_p01_GW_36 ≫. (a1), (b1) encrypted version of (a), (b). (c), (d), (c1), (d1) Histograms corresponding to (a), (b), (a1) and (b1), respectively.

computed and (CC) presented in Figure 6. The absolute CC is computed via the next formula:

$$|CC| = \frac{|C(S_1, S_2)|}{\sqrt{V(S_1)}\sqrt{V(S_2)}} \tag{8}$$

where $C(S_1, S_2)$ represents the covariance value of S_1 and S_2 vectors. $V(S_1)$ and $V(S_2)$ are the variance values of S_1 and S_2. The CC value near zero indicates that the encryption algorithm is effective at reducing the correlation in the input signal.

Figure 7 displays the autocorrelation between 2000 adjacent values in the encrypted test signals. The achieved results clearly show that our scheme can significantly reduce the correlation between adjacent samples in the input signals, making it difficult for an attacker to predict useful information from a correlation analysis.

C. HISTOGRAM ANALYSIS

Histogram analysis is useful to assess the encryption algorithm's ability to resist statistical attacks. In the next test, two bio - signals are arbitrarily selected from the used dataset and then encrypted using the proposed scheme. The histograms of the original signals and their encrypted forms are plotted in Figure 8. The results in this figure show that the histograms of the encrypted signals are very different from those of the original ones. The result in this figure indicates that our algorithm can also make the histograms of its output signals nearly flat. Thus, attackers are unable to extract useful information by analyzing the histograms of the encrypted signals.

D. KEY SENSITIVITY ANALYSIS

Key sensitivity analysis is a critical step in designing secure and efficient signal encryption systems, especially when implemented on resource-constrained microcontrollers. It aids in assessing and enhancing the resilience of the encryption process against diverse attack vectors and environmental stressors.

To test the sensitivity of the proposed scheme's keys, the original security key is defined as

$$\begin{aligned} KEY &= \{\mu_v, D, R_{ON}, R_{OFF}, R_0, G_1, G_2, f, Amp, L_0\} \\ &= \{10^{-14}, 10\times10^{-9}, 200, 40 \\ &\quad \times10^3, 2\times10^3, 8, 9, 1, 5, 0.3\} \end{aligned}$$

During decryption, only one component is selected and modified by $\Delta = 10^{-6}$. Figure 9 displays an original ECG signal labeled "14046" that is encrypted, and then decrypted by using both the correct and wrong security keys. This figure also presents Percentage Root- Difference (PRD (%)) between the original signal and their decrypted forms. The PRD is defined as:

$$PRD(\%) = 100 \times \sqrt{\frac{\sum_{i=0}^{N}\left(\hat{s}_i - s_i\right)^2}{\sum_{i=0}^{N}\left(\hat{s}_i\right)^2}} \tag{9}$$

where $\hat{s}$ represents the decrypted form of s signal with length of N samples. When PRD = 0%, it means the decryption process is lossless.

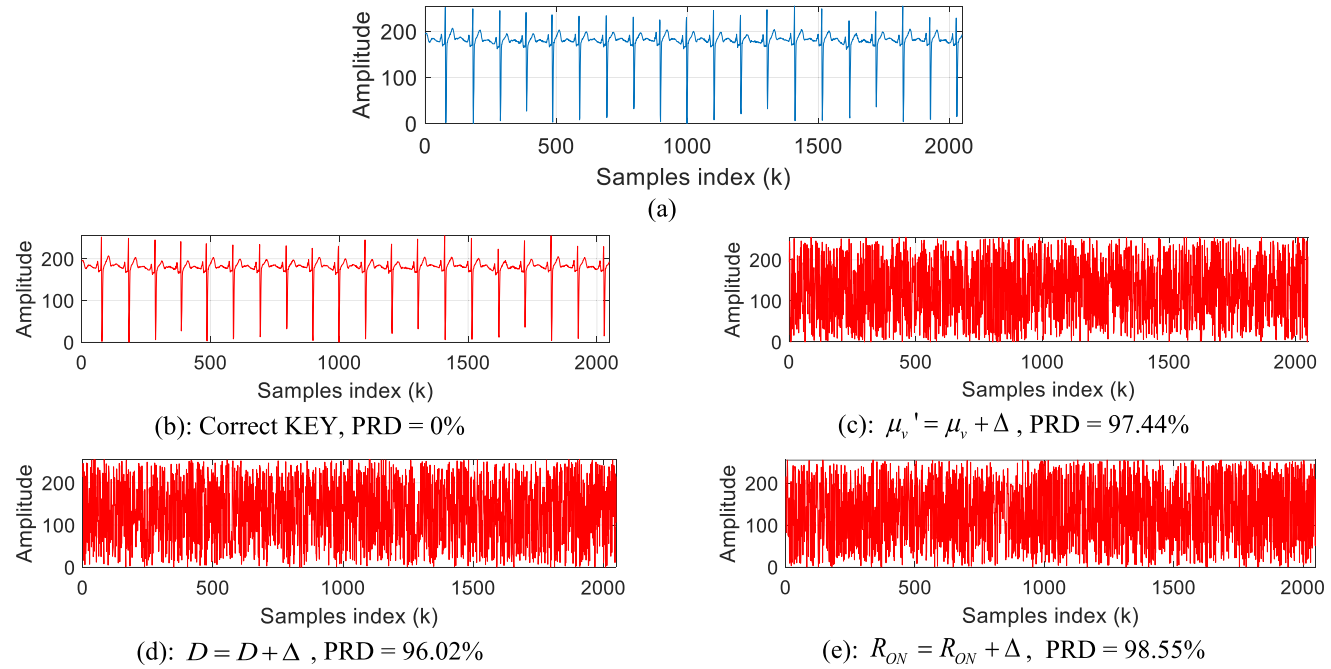


FIGURE 9. (a) Original ECG signal and its decrypted versions response to KEY component variation to (b) correct key, and (c)-(e) modified components by $\Delta = 10^{-6}$.

Table 3 presents the influence of KEY parameters on the decrypted signal. It shows the PRD values of the decrypted signals after varying each component.

The current analysis results reveals that even small variations in any component of the user's security key by $\Delta = 10^{-6}$ lead to a complete prevent in recovering the original signal. This demonstrates the proposed scheme's high sensitivity to its security key, making it highly resistant to brute-force attacks. In contrast, when the correct security key is used (Figure 9(b)), the decrypted signal is perfectly recovered, resulting in a PRD of 0%. This is because the proposed scheme is designed to be lossless. Indeed, the original signal is encrypted on the sender's side, transmitted over the Bluetooth channel, and then decrypted and stored on the receiver's side without any data loss.

E. ENTROPY ANALYSIS

This analysis calculates the entropy of ciphertexts to evaluate the randomness introduced by the proposed encryption system and assess its susceptibility to statistical attacks. Shannon entropy (E), defined by the following equation, is widely used to measure the entropy in a signal.

$$E = -\sum_{i=1}^{r} P(K_i) \log_2 \frac{1}{P(K_i)} \tag{10}$$

where K_i represent the sample values in the input bio-signal. Since the signal samples are represented on 8 bits, each K_i can have values in the range [0 – 255]. If all the signal samples are uniformly distributed across this range, then $E = 8$.

For this analysis, we used the test bio-signals shown in Figure 10. Then, they are encrypted using the proposed cryptosystem and the entropy of both the original and encrypted signals is computed. The results are reported in the same Figure.

TABLE 3. Influence of modified key parameters by $\Delta = 10^{-6}$ on decrypted signal quality (PRD%).

Modified key component	R_{OFF}	R_0	G_1	G_2	f	Amp	L_0
PRD (%)	95.12	94.9	99.0	96.4	98.0	93.8	94.3

Based on the results shown in Figure 10, it appears that the proposed cryptosystem can make the entropy of the encrypted signals close to the ideal value ($E = 8$). This suggests that the encrypted signals have values that are nearly random, making it difficult for attackers to extract useful information from them through entropy analysis.

F. ROBUSTNESS TO CLASSICAL ATTACKS

In accordance with Kerckhoffs' principle [76], it is assumed that the attacker has all information about the cryptosystem except for the security keys. Therefore, the attacker can utilize classical attacks such as known-plaintext, ciphertext-only, chosen-ciphertext, and chosen-plaintext attacks. Therefore, the attacker can utilize classical attacks (known-plaintext, ciphertext-only, chosen-ciphertext, and chosen-plaintext) to crack the cryptosystem [77].

The method of dynamic secret keys is adopted to ensure the robustness of the proposed algorithm against classical attacks [31], [78]. This method is employed in the following way:

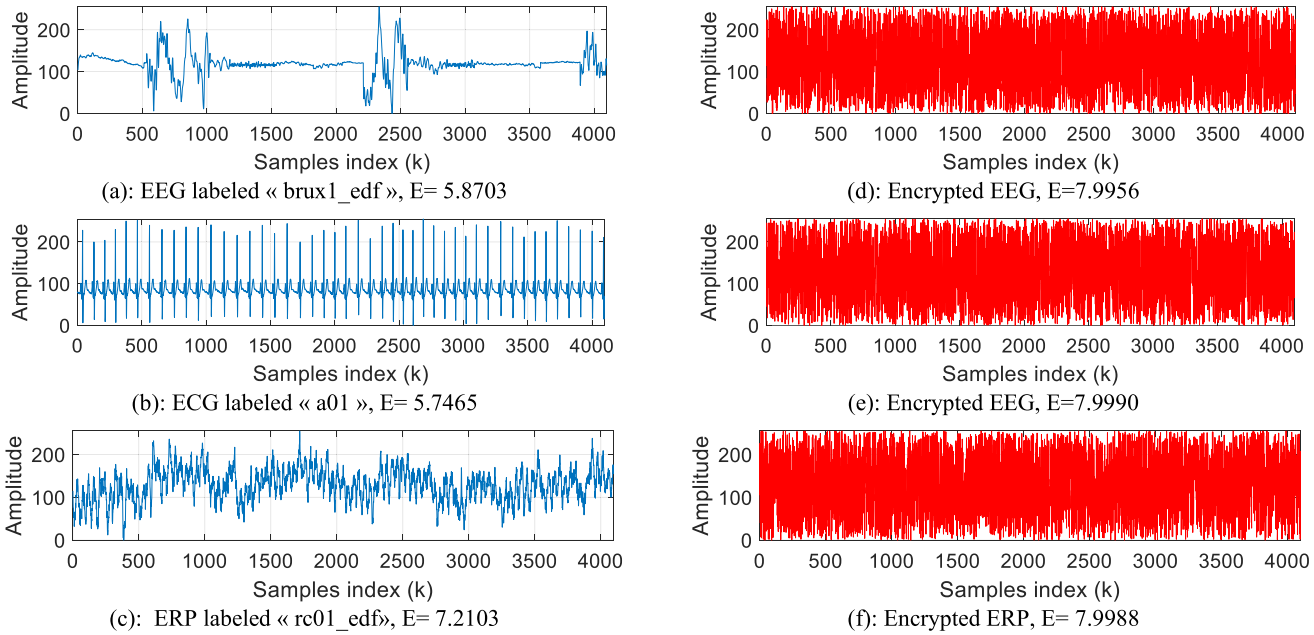


FIGURE 10. (a)-(c) Original bio-signals and (d)-(f) their corresponding encrypted versions, along with the associated entropy (E) values.

Define a user security key, denoted $KEY = \{\mu_v, D, R_{ON}, R_{OFF}, R_0, G_1, G_2, f, Amp, L_0\}$, to be communicated between the sender and the receiver.

For each input bio-signal, a component (R_{ON}, for instance) is chosen from KEY and its value is updated by a slight variation 10^{-6} at each iteration to get $KEY*$.

Use $KEY*$ in the encryption of the next bio-signal image in the dataset. Then, update $KEY*$ by a slight variation and use it in the encryption of the next bio-signal and so on.

By adopting this method, each signal is encrypted with a unique key, which can resist known attacks. Indeed, this method ensures that the cryptosystem always generates different ciphertexts for consecutive encryptions, even when encrypting the same input.

G. NPCR AND UACI ANALYSIS

The NPCR (Net Pixel Change Rate) and UACI (Unified Average Changing Intensity) are useful criteria for evaluating the ability of an encryption algorithm to resist a differential attack, which is generally a known plaintext attack. These criteria is exploited in the context of 1D signal encryption to measure the difference between ciphertexts of bio-signals. These criteria are defined as follows [79]:

$$NPCR = \frac{100}{L}\sum_{i=1}^{L} X_i \times 100 \text{with} X_i = \begin{cases} 0 & if\ \mathrm{E1}_i = \mathrm{E2}_i \\ 1 & if\ \mathrm{E1}_i \neq \mathrm{E2}_i \end{cases} \tag{11}$$

where L is the input signal length. When $NPCR = 100\%$ indicates that ciphertexts $E1$ and $E2$ are completely different.

$$UACI = \frac{100}{L}\sum_{i=1}^{L} |D| \times 100 \text{with} D = E1_i - E2_i \tag{12}$$

TABLE 4. Hardware resources used in our cryptosystem.

ATmega328P resources	Total	Used
Flash memory	30 720 bytes	12144 bytes (39%)
SRAM	2 048 bytes	1024 bytes (50%)

The UACI measures the difference in magnitude on average between $E1$ and $E2$ encrypted bio-signals.

H. RESOURCE ANALYSIS

Resource analysis plays a key role in successful implementation on a hardware. Indeed, we need to carefully consider the memory constraints, microcontroller architecture limitations, and communication protocol compatibility. These factors not only impact cost but also influence the application's performance and scalability. The analysis of the sketch information in Table 4 shows that the memory usage is within acceptable limits where the sketch uses 39% of program memory and 50% of dynamic memory.

I. TIMING ANALYSIS

Unlike traditional cryptosystems, embedded implementations face distinct challenges due to various speed constraints. These constraints arise from some factors including fluctuating, clock speeds, varying memory access times, and even external environmental influences.

With the aim of evaluating the encryption/decryption speed of the proposed cryptosystem, bio-signal segments, each containing 6000 samples, are selected from the MIT-BIH (Massachusetts Institute of Technology-Beth Israel Hospital) arrhythmia biomedical dataset. The encryption and decryption runtimes are measured on the sender and receiver

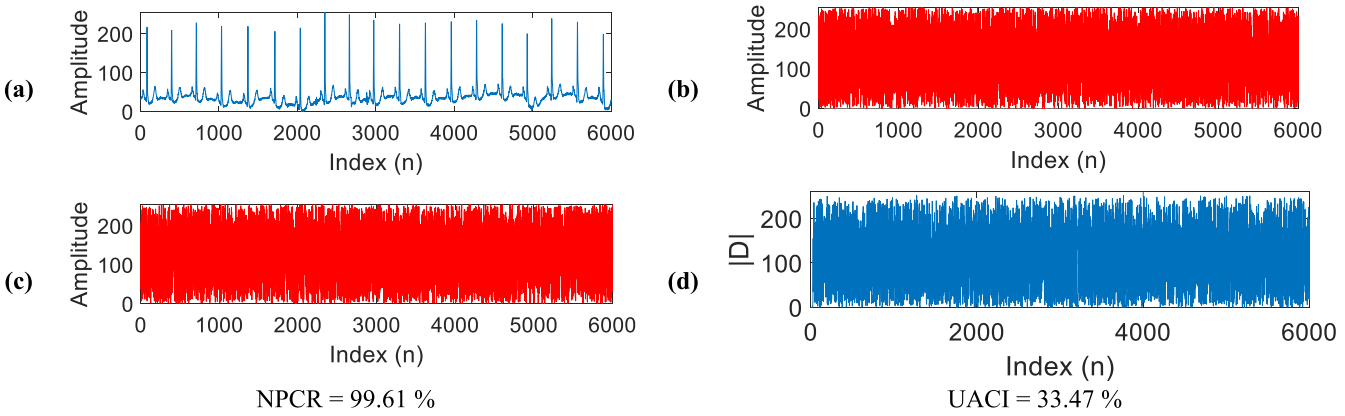


FIGURE 11. (a) Original ECG signal. (b)-(c) Two encrypted versions of the input signal. (d) the difference in absolute value between the encrypted signals with the corresponding NPCR and UACI values.

TABLE 5. runtime analysis of encryption and decryption algorithms on Arduino nano.

Label	Encryption runtime (s)	Decryption time (s)
« a04»	8.120	8.120
« brux1_edf »	8.122	8.121
«fetal_PCG_p01_GW_36 »	8.121	8.120
«rc01_edf»	8.119	8.119
Average runtime	**8.1205**	**8.120**

sides, respectively, using the proposed embedded system implementation. The results are shown in Table 5. From this table, it appears that the average runtime of the encryption/decryption phases of the test signals on the ATmega328P has an insignificant difference. This observation aligns with the fact that the proposed cryptosystem is symmetric. The computed speed is about 5.91 kbits/s. This speed is not high due to the limitations of the Arduino Nano microcontroller and the inherent limitations of Bluetooth communication bandwidth. This limitation opens the door to further research exploring the use of high-speed hardware. Additionally, process variations inherent to hardware manufacturing can also contribute to timing variations, as noted in related work by Alnuayri et al. [80].

J. COMPARATIVE ANALYSIS

This section compares the performance of our cryptosystem with recent chaos-based implementation used for bio-signal encryption. The performed comparison is shown in Tables 7 and 6. Based on this comparison, it can be concluded that most existing bio-signal encryption schemes are implemented on personal computers (PCs). However, PC-based implementations have several limitations, including the limited portability, high-power consumption, and high-cost. These limitations make them less suitable for real-world scenarios. Therefore, the development of secure and low-cost embedded systems implementing cryptosystems holds significant value in the IoMT domain. Indeed, these implementations offer key advantages, including cost-effectiveness, efficiency, low-power consumption, and a high level of security.

Compared to existing schemes, the proposed scheme offers the advantages of lower cost, which make improving its accessibility and facilitating wider adoption in the IoMT

domain. Moreover, the comparison reveals a significantly larger key space for our scheme compared to existing microcontroller-based implementations. This advantage stems from the utilization of ten control parameters within the proposed LCM map, making it particularly attractive for resource-constrained hardware implementations. In addition, this work provides a comprehensive analysis encompassing chaotic behavior, cryptosystem performance, and microcontroller implementation. This analysis provides a holistic understanding of the proposed cryptosystem, leading to increased confidence in its security and the identification of its potential issues.

While the proposed bio-signal cryptosystem offers several advantages, as previously mentioned, its encryption speed (5.91 kb/s) is limited compared to other schemes. Our scheme also exhibits low robustness in noisy environments. This limitation arises from its implementation in the spatial domain. In future work, exploring transform-based domain implementations could overcome this limitation.

It's important to note that our solution is designed to be adaptable. This allows for replacing the ATmega328P microcontrollers used in this work with more sophisticated options, such as the STM32F4 series, ESP32 family, or Raspberry Pi Pico family. This is particularly beneficial for applications requiring faster processing speeds, especially real-time encryption. In such applications, the processing speed (encryption/decryption) typically needs to be at least as fast as the sampling speed to prevent data backlog and ensure timely operation, according to Kuo et al. [81].

The encryption performance of our scheme is also compared with similar excellent ones presented in [79], [82], [83], and [84]. The comparison is performed in terms of average absolute CC values, average NPCR (%), average UACI (%), average Shannon entropy, and average PRD (%).

TABLE 6. Comparison between the proposed cryptosystem with similar chaos-based ones.

Schemes	Proposed	Murillo-Escobar et al. [79]	Algarni et al. [82]	Lin et al. [83]	Murillo-Escobar et al. [84]
Chaotic map analysis					
Used Chaotic system dimension	1D	2D	1D and 2D	1D	2D
Number of the used chaotic map parameters	10	4	4	2	4
Lyapunov Exponent	✓	✓	-	✓	-
Bifurcation diagrams	✓	✓	-	✓	-
Control parameters sensitivity	✓	✓	-	-	-
Statistical NIST	✓	✓	-	-	-
Scheme's security analysis					
Key sensitivity	✓	✓	-	-	✓
Autocorrelation	✓	✓	✓	-	✓
Information entropy	✓	✓	-	-	✓
Robustness to differential attacks	✓	✓	-	-	✓
Histogram	✓	✓	✓	✓	✓
NPCR and UACI	✓	✓	-	-	-
Key space	400-bit	276-bit	-	256-bit	416-bit
Noise robustness	-	-	✓	✓	✓
Implementation environment					
Used microcontroller	ATmega328P Microcontroller	MCF51MM256 microcontroller	-	-	-
Embedded system implementation?	✓	✓	-	-	-
Encryption Speed	5.91 kb/s	6 Mb/s	-	-	-

TABLE 7. Performance comparison between the proposed cryptosystem with similar chaos-based ones in terms of average absolute CC values, NPCR (%), UACI (%), Shannon entropy, and PRD (%).

Schemes	Proposed	Murillo-Escobar et al. [79]	Algarni et al. [82]	Lin et al. [83]	Murillo-Escobar et al. [84]
Absolute CC values	0.0040	0.0042	0.0612	0.0207	0.0041
NPCR (%)	99.61	99.80	99.72	99.68	99.82
UACI (%)	33.47	33.20	33.78	99.71	33.68
Shannon Entropy	7.98	7.91	7.87	7.85	7.98
PRD (%)	0	0	0.06	0.08	0

For the present comparison, we randomly selected 20 bio-signals, each containing L = 10000 samples, from the dataset [74].

The comparison results are shown in Table 6. Based on these results, we can conclude that our scheme exhibits competitive performance: the CC values tend towards zero, NPCR and UACI are near the ideal values of 99.6094% and 33.4635%, respectively, in accordance with [85]. Additionally, Shannon entropy tends towards 8.

The comparative study indicate also that our scheme and those presented in [79] and [84] are lossless since PRD = 0%. In contrast, the methods in [82] and [83] introduce some degradation in the decrypted signal quality (PRD > 0%), which is undesirable for sensitive data like bio-signals.

VII. CONCLUSION

This work proposes a novel 1D chaotic map based on the HP discrete memristor coupled with the logistic map. The proposed map exhibits high sensitivity to small variations in its ten control parameters. Following the validation of the proposed LCM chaotic behavior using Lyapunov exponents and bifurcation diagrams, it is implemented on a low-cost, resource-constrained microcontroller. The chaotic behavior of LCM is then evaluated using NIST randomness tests and parameter sensitivity analysis. The test results demonstrate that the LCM maintains its chaotic behavior, and its parameter sensitivity is approximately 10^{-6}. The proposed LCM is then employed as the core component in designing a new lightweight confusion-diffusion scheme for encrypting biomedical signals. To demonstrate the potential of the proposed cryptosystem in real-world scenarios, a low-cost embedded system implementation for secure wireless bio-signal communication is presented. The extensive simulation and comparison results demonstrate two key findings: (i) The proposed LCM, implemented on a low-cost microcontroller, exhibits good chaotic behavior. (ii) The implementation of the proposed cryptosystem on an embedded system offers both cost-effectiveness and high security.

While our work offers several advantages, it also presents two main drawbacks: (i) the low encryption speed. This limitation arises from the use of a resource-constrained microcontroller. (ii) The low resistance to noise attacks: This vulnerability requires further investigation in future work.

Algorithm 1 Proposed Confusion of Bio- Signal Segment Using Circular Shifting and Chaotic LCM Sequences

Input:
Seg: Bio-signal segment of size $L = N \times M$ with $N = M = 5$
Output:
SegC: Confused Bio-signal segment
Main_function
Step 1:
Reshape ***'Seg'*** vector into a 2D matrix ***'Seg_2D'*** with dimensions $N \times M$
Step 2:
Use Eq. (5) to generate a chaotic LCM-based sequence ***'CS'*** of size K=N+M
Step 3:
Divide the chaotic sequence ***'CS'*** into two parts:
X: The first ***N*** elements of ***'CS'*** ($X = \lfloor CS\ (0toN - 1) \times N \rfloor$)
Y: The last ***M*** elements of ***'CS'*** ($Y = \lfloor CS\ (NtoM - 1) \times M \rfloor$)
Step 4:
For each row ***'i'*** in the ***'Seg_2D'*** matrix:
Use ***Circular_Shift*** function to circularly shift the values according
to the corresponding value in ***X[i]***
Step 5:
For each row ***'j'*** in the ***'Seg_2D'*** matrix:
Use ***Circular_Shift*** function to circularly shift the values according
to the corresponding value in ***Y[j]***
Step 6:
Reshape the modified ***'Seg_2D'*** matrix into ***'SegC'*** vector with length L
Step 7:
Return the confused ECG segment ***'SegC'***
end Main_function
Function: Circular_Shift
Step 1:
For a given vector ***'Vector'*** and number of positions to shift ***'positions'***,
calculate the length n of the vector.
Step 2:
Initialize a new vector ***'shiftedVector'*** of length n.
Step 3:
For each element ***'i'*** in the ***'Vector'***:
Calculate the new index ***'newIndex'*** as ***'(i + positions - 1) mod n + 1'***
Assign the value of ***'Vector[i]'*** to ***'shiftedVector[newIndex]'***.
Step 4:
Return the ***'shiftedVector'***
end Circular_Shift function

Recognizing the limitations of our work, future endeavors will prioritize two key areas: (i) enhancing encryption speed by exploring alternative implementations or hardware platforms that go beyond resource-constrained microcontrollers, and (ii) improving the security level and the robustness to noise. Additionally, investigations into alternative microcontroller-based implementations for encrypting various multimedia data will be conducted, especially for real-time signal encryption. Moreover, future work will explore performance optimization of the proposed cryptosystem, focusing on reducing energy consumption, improving encryption/decryption speed, and other relevant metrics in the IoMT. In addition, we will investigate the hardware implementation of our cryptosystem on an FPGA and compare its performance with the current work.

APPENDIX

In Algorithm 1, the symbol $\lfloor . \rfloor$ refers to the rounding operation and mod is the modular function.

AUTHOR CONTRIBUTIONS

Conceptualization, Achraf Daoui; methodology, Ahmed A. Abd El-Latif; software, Mohamed Yamni, and Achraf Daoui; validation, Pawel Plawiak, and Osama Alfarraj; formal analysis, Mohamed Yamni, and Ahmed A. Abd El-Latif; investigation, Achraf Daoui, and Pawel Plawiak; resources, Osama Alfarraj; data curation, Paweł Pławiak, and Osama Alfarraj; writing—original draft preparation, Achraf Daoui, Mohamed Yamni, and Ahmed A. Abd El-Latif; writing—review and editing, Achraf Daoui, and Ahmed A. Abd El-Latif; visualization, X.X.; supervision, Ahmed A. Abd El-Latif; project administration, Osama Alfarraj; funding acquisition, Pawel Plawiak. All authors have read and agreed to the published version of the manuscript.

INFORMED CONSENT STATEMENT

Not applicable

DATA AVAILABILITY STATEMENT

All data will be available upon reasonable request.

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

REFERENCES

[1] A. Daoui, H. Karmouni, M. Sayyouri, H. Qjidaa, M. Maaroufi, and B. Alami, "New robust method for image copyright protection using histogram features and Sine Cosine Algorithm," *Exp. Syst. Appl.*, vol. 177, Sep. 2021, Art. no. 114978.

[2] J. Fridrich and M. Goljan, "Digital image steganography using stochastic modulation," *Proc. SPIE*, vol. 5020, pp. 191–202, Jun. 2003.

[3] I. Koyuncu and A. T. Ozcerit, "The design and realization of a new high speed FPGA-based chaotic true random number generator," *Comput. Electr. Eng.*, vol. 58, pp. 203–214, Feb. 2017, doi: 10.1016/j.compeleceng.2016.07.005.

[4] M. Yamni, A. Daoui, and A. A. A. El-Latif, "Efficient color image steganography based on new adapted chaotic dynamical system with discrete orthogonal moment transforms," *Math. Comput. Simul.*, Feb. 2024, doi: 10.1016/j.matcom.2024.01.023.

[5] M. Yamni, A. Daoui, P. Plawiak, H. Mao, O. Alfarraj, and A. A. A. El-Latif, "A novel 3D reversible data hiding scheme based on integer-reversible Krawtchouk transform for IoMT," *Sensors*, vol. 23, no. 18, p. 7914, Jan. 2023, doi: 10.3390/s23187914.

[6] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: A survey," *IEEE Access*, vol. 8, pp. 131723–131740, 2020, doi: 10.1109/ACCESS.2020.3009876.

[7] L. Sousa, S. Antao, and P. Martins, "Combining residue arithmetic to design efficient cryptographic circuits and systems," *IEEE Circuits Syst. Mag.*, vol. 16, no. 4, pp. 6–32, 4th Quart., 2016, doi: 10.1109/MCAS.2016.2614714.

[8] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," in *Proc. Int. Conf. Electron., Commun. Comput. Eng. (ICECCE)*, Nov. 2014, pp. 83–93, doi: 10.1109/ICECCE.2014.7086640.

[9] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021, doi: 10.1109/ACCESS.2021.3052867.

[10] E. Dong, M. Yuan, S. Du, and Z. Chen, "A new class of Hamiltonian conservative chaotic systems with multistability and design of pseudo-random number generator," *Appl. Math. Model.*, vol. 73, pp. 40–71, Sep. 2019, doi: 10.1016/j.apm.2019.03.037.

[11] D. Ding, W. Wang, Z. Yang, Y. Hu, J. Wang, M. Wang, Y. Niu, and H. Zhu, "An n-dimensional modulo chaotic system with expected Lyapunov exponents and its application in image encryption," *Chaos, Solitons Fractals*, vol. 174, Sep. 2023, Art. no. 113841, doi: 10.1016/j.chaos.2023.113841.

[12] K. Hayden, E. Olson, and E. S. Titi, "Discrete data assimilation in the Lorenz and 2D Navier-Stokes equations," *Phys. Nonlinear Phenom.*, vol. 240, no. 18, pp. 1416–1425, Sep. 2011, doi: 10.1016/j.physd.2011.04.021.

[13] A. H. Bukhari, M. A. Z. Raja, N. Rafiq, M. Shoaib, A. K. Kiani, and C.-M. Shu, "Design of intelligent computing networks for nonlinear chaotic fractional Rossler system," *Chaos, Solitons Fractals*, vol. 157, Apr. 2022, Art. no. 111985, doi: 10.1016/j.chaos.2022.111985.

[14] M. Alqhtani, M. M. Khader, and K. M. Saad, "Numerical simulation for a high-dimensional chaotic Lorenz system based on Gegenbauer wavelet polynomials," *Mathematics*, vol. 11, no. 2, p. 472, Jan. 2023, doi: 10.3390/math11020472.

[15] Q. Li and L. Chen, "An image encryption algorithm based on 6-dimensional hyper chaotic system and DNA encoding," *Multimedia Tools Appl.*, vol. 83, no. 2, pp. 5351–5368, Jan. 2024, doi: 10.1007/s11042-023-15550-3.

[16] B. Sun, C. Zhang, Q. Peng, and B. Du, "Color image encryption algorithm based on 5D memristive chaotic system and group scrambling," *Optik*, vol. 287, Sep. 2023, Art. no. 171132, doi: 10.1016/j.ijleo.2023.171132.

[17] Q. Lai and Y. Liu, "A cross-channel color image encryption algorithm using two-dimensional hyperchaotic map," *Exp. Syst. Appl.*, vol. 223, Aug. 2023, Art. no. 119923.

[18] A. V. Tutueva, E. G. Nepomuceno, A. I. Karimov, V. S. Andreev, and D. N. Butusov, "Adaptive chaotic maps and their application to pseudo-random numbers generation," *Chaos, Solitons Fractals*, vol. 133, Apr. 2020, Art. no. 109615, doi: 10.1016/j.chaos.2020.109615.

[19] A. V. Tutueva, A. I. Karimov, L. Moysis, C. Volos, and D. N. Butusov, "Construction of one-way hash functions with increased key space using adaptive chaotic maps," *Chaos, Solitons Fractals*, vol. 141, Dec. 2020, Art. no. 110344, doi: 10.1016/j.chaos.2020.110344.

[20] A. V. Tutueva, L. Moysis, V. G. Rybin, E. E. Kopets, C. Volos, and D. N. Butusov, "Fast synchronization of symmetric Hénon maps using adaptive symmetry control," *Chaos, Solitons Fractals*, vol. 155, Feb. 2022, Art. no. 111732, doi: 10.1016/j.chaos.2021.111732.

[21] A. Tutueva, L. Moysis, V. Rybin, A. Zubarev, C. Volos, and D. Butusov, "Adaptive symmetry control in secure communication systems," *Chaos, Solitons Fractals*, vol. 159, Jun. 2022, Art. no. 112181, doi: 10.1016/j.chaos.2022.112181.

[22] W. Cao, H. Cai, and Z. Hua, "*n*-dimensional chaotic map with application in secure communication," *Chaos, Solitons Fractals*, vol. 163, Oct. 2022, Art. no. 112519.

[23] Y. Zhong and J. Gu, "Lightweight block ciphers for resource-constrained environments: A comprehensive survey," *Future Gener. Comput. Syst.*, vol. 157, pp. 288–302, Aug. 2024, doi: 10.1016/j.future.2024.03.054.

[24] E. G. Nepomuceno, A. M. Lima, J. Arias-Garcia, M. Perc, and R. Repnik, "Minimal digital chaotic system," *Chaos, Solitons Fractals*, vol. 120, pp. 62–66, Mar. 2019, doi: 10.1016/j.chaos.2019.01.019.

[25] O. A. Khashan, R. Ahmad, and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks," *Ad Hoc Netw.*, vol. 115, Apr. 2021, Art. no. 102448, doi: 10.1016/j.adhoc.2021.102448.

[26] M. SaberiKamarposhti, A. Ghorbani, and M. Yadollahi, "A comprehensive survey on image encryption: Taxonomy, challenges, and future directions," *Chaos, Solitons Fractals*, vol. 178, Jan. 2024, Art. no. 114361, doi: 10.1016/j.chaos.2023.114361.

[27] A. Daoui, M. Yamni, S. A. Chelloug, M. A. Wani, and A. A. A. El-Latif, "Efficient image encryption scheme using novel 1D multiparametric dynamical tent map and parallel computing," *Mathematics*, vol. 11, no. 7, p. 1589, 2023.

[28] A. Daoui and A. A. A. El-Latif, "Multimedia security through 1D chaotic systems: Review and analysis," in *Recent Advancements in Multimedia Data Processing and Security: Issues, Challenges, and Techniques*. Hershey, PA, USA: IGI Global, 2023, pp. 1–31, doi: 10.4018/978-1-6684-7216-3.ch001.

[29] B. Bao, K. Rong, H. Li, K. Li, Z. Hua, and X. Zhang, "Memristor-coupled logistic hyperchaotic map," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 8, pp. 2992–2996, Aug. 2021, doi: 10.1109/TCSII.2021.3072393.

[30] S. Shao, J. Li, P. Shao, and G. Xu, "Chaotic image encryption using piecewise-logistic-sine map," *IEEE Access*, vol. 11, pp. 27477–27488, 2023, doi: 10.1109/ACCESS.2023.3257349.

[31] A. Daoui, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Robust image encryption and zero-watermarking scheme using SCA and modified logistic map," *Exp. Syst. Appl.*, vol. 190, Mar. 2022, Art. no. 116193.

[32] M. Wang, X. Wang, C. Wang, S. Zhou, Z. Xia, and Q. Li, "Color image encryption based on 2D enhanced hyperchaotic logistic-sine map and two-way Josephus traversing," *Digit. Signal Process.*, vol. 132, Jan. 2023, Art. no. 103818, doi: 10.1016/j.dsp.2022.103818.

[33] Q. Lai, L. Yang, and G. Chen, "Design and performance analysis of discrete memristive hyperchaotic systems with stuffed cube attractors and ultraboosting behaviors," *IEEE Trans. Ind. Electron.*, vol. 71, no. 7, pp. 7819–7828, Jul. 2024, doi: 10.1109/TIE.2023.3299016.

[34] F. Wang and F. Wang, "Floating memcapacitor based on knowm memristor and its dynamic behaviors," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 12, pp. 5134–5138, Dec. 2022, doi: 10.1109/TCSII.2022.3201225.

[35] Q. Lai, L. Yang, G. Hu, Z.-H. Guan, and H. H.-C. Iu, "Constructing multiscroll memristive neural network with local activity memristor and application in image encryption," *IEEE Trans. Cybern.*, pp. 1–10, 2024, doi: 10.1109/TCYB.2024.3377011.

[36] Q. Lai, Z. Wan, H. Zhang, and G. Chen, "Design and analysis of multiscroll memristive hopfield neural network with adjustable memductance and application to image encryption," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 10, pp. 7824–7837, Oct. 2023, doi: 10.1109/TNNLS.2022.3146570.

[37] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, "The missing memristor found," *Nature*, vol. 453, p. 7191, May 2008, doi: 10.1038/nature06932.

[38] W. Feng, Y. Qin, S. Zhao, and D. Feng, "AAoT: Lightweight attestation and authentication of low-resource things in IoT and CPS," *Comput. Netw.*, vol. 134, pp. 167–182, Apr. 2018, doi: 10.1016/j.comnet.2018.01.039.

[39] A. Musaddiq, Y. B. Zikria, O. Hahm, H. Yu, A. K. Bashir, and S. W. Kim, "A survey on resource management in IoT operating systems," *IEEE Access*, vol. 6, pp. 8459–8482, 2018.

[40] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in IoMT communications: A survey," *Sensors*, vol. 20, no. 17, p. 4828, Jan. 2020, doi: 10.3390/s20174828.

[41] J. P. A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier, and A. Chehab, "Securing Internet of Medical Things systems: Limitations, issues and recommendations," *Future Gener. Comput. Syst.*, vol. 105, pp. 581–606, Apr. 2020, doi: 10.1016/j.future.2019.12.028.

[42] M. O. U. Islam and S. A. Parah, "Fast and lightweight image cryptosystem for IoMT applications," *Internet Things*, Feb. 2024, Art. no. 101083, doi: 10.1016/j.iot.2024.101083.

[43] A. Daoui, M. Yamni, H. Karmouni, M. Sayyouri, H. Qjidaa, S. Motahhir, O. Jamil, W. El-Shafai, A. D. Algarni, N. F. Soliman, and M. H. Aly, "Efficient biomedical signal security algorithm for smart Internet of Medical Things (IoMTs) applications," *Electronics*, vol. 11, no. 23, p. 3867, 2022.

[44] Y. Athavale and S. Krishnan, "Biosignal monitoring using wearables: Observations and opportunities," *Biomed. Signal Process. Control*, vol. 38, pp. 22–33, Sep. 2017, doi: 10.1016/j.bspc.2017.03.011.

[45] S. Bharati, P. Podder, M. R. H. Mondal, and P. K. Paul, "Applications and challenges of cloud integrated IoMT," in *Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications* (Studies in Systems, Decision and Control), A. E. Hassanien, A. Khamparia, D. Gupta, K. Shankar, and A. Slowik, Eds. Cham, Switzerland: Springer, 2021, pp. 67–85, doi: 10.1007/978-3-030-55833-8_4.

[46] I. Ud Din, A. Almogren, M. Guizani, and M. Zuair, "A decade of Internet of Things: Analysis in the light of healthcare applications," *IEEE Access*, vol. 7, pp. 89967–89979, 2019, doi: 10.1109/ACCESS.2019.2927082.

[47] A. Daoui, H. Mao, M. Yamni, Q. Li, O. Alfarraj, and A. A. A. El-Latif, "Novel integer shmaliy transform and new multiparametric piecewise linear chaotic map for joint lossless compression and encryption of medical images in IoMTs," *Mathematics*, vol. 11, no. 16, p. 3619, Jan. 2023, doi: 10.3390/math11163619.

[48] W. A. Yihyis, S. He, Z. Tang, and H. Wang, "A class of discrete memristor chaotic maps based on the internal perturbation," *Symmetry*, vol. 15, no. 8, p. 1574, Aug. 2023, doi: 10.3390/sym15081574.

[49] G. Li, H. Zhong, W. Xu, and X. Xu, "Two modified chaotic maps based on discrete memristor model," *Symmetry*, vol. 14, no. 4, p. 800, Apr. 2022, doi: 10.3390/sym14040800.

[50] M. Z. Talhaoui and X. Wang, "A new fractional one dimensional chaotic map and its application in high-speed image encryption," *Inf. Sci.*, vol. 550, pp. 13–26, Mar. 2021, doi: 10.1016/j.ins.2020.10.048.

[51] M. Z. Talhaoui, X. Wang, and A. Talhaoui, "A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme," *Vis. Comput.*, vol. 37, no. 7, pp. 1757–1768, Jul. 2021, doi: 10.1007/s00371-020-01936-z.

[52] J. Wang, L. Liu, M. Xu, and X. Li, "A novel content-selected image encryption algorithm based on the LS chaotic model," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8245–8259, Nov. 2022, doi: 10.1016/j.jksuci.2022.08.007.

[53] A. Belazi, S. Kharbech, M. N. Aslam, M. Talha, W. Xiang, A. M. Iliyasu, and A. A. A. El-Latif, "Improved Sine-Tangent chaotic map with application in medical images encryption," *J. Inf. Secur. Appl.*, vol. 66, May 2022, Art. no. 103131, doi: 10.1016/j.jisa.2022.103131.

[54] L. Zhu, D. Jiang, J. Ni, X. Wang, X. Rong, and M. Ahmad, "A visually secure image encryption scheme using adaptive-thresholding sparsification compression sensing model and newly-designed memristive chaotic map," *Inf. Sci.*, vol. 607, pp. 1001–1022, Aug. 2022, doi: 10.1016/j.ins.2022.06.011.

[55] X. Rong, D. Jiang, M. Zheng, X. Yu, and X. Wang, "Meaningful data encryption scheme based on newly designed chaotic map and P-tensor product compressive sensing in WBANs," *Nonlinear Dyn.*, vol. 110, no. 3, pp. 2831–2847, Nov. 2022, doi: 10.1007/s11071-022-07736-5.

[56] S. Zhu, X. Deng, W. Zhang, and C. Zhu, "Secure image encryption scheme based on a new robust chaotic map and strong S-box," *Math. Comput. Simul.*, vol. 207, pp. 322–346, May 2023, doi: 10.1016/j.matcom.2022.12.025.

[57] L. Liu and J. Wang, "A cluster of 1D quadratic chaotic map and its applications in image encryption," *Math. Comput. Simul.*, vol. 204, pp. 89–114, Feb. 2023, doi: 10.1016/j.matcom.2022.07.030.

[58] N. Charalampidis, A. Iatropoulos, and C. Volos, "Chaos based speech encryption using microcontroller," *Integration*, vol. 95, Mar. 2024, Art. no. 102128, doi: 10.1016/j.vlsi.2023.102128.

[59] S. Janakiraman, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller," *Microprocess. Microsyst.*, vol. 56, pp. 1–12, Feb. 2018, doi: 10.1016/j.micpro.2017.10.013.

[60] M. A. Murillo-Escobar, C. Cruz-Hernandez, F. Abundiz-Perez, and R. M. Lopez-Gutierrez, "Implementation of an improved chaotic encryption algorithm for real-time embedded systems by using a 32-bit microcontroller," *Microprocess. Microsyst.*, vol. 45, pp. 297–309, Sep. 2016, doi: 10.1016/j.micpro.2016.06.004.

[61] S. Fan, K. Li, Y. Zhang, H. Tan, Q. Fang, K. Han, and J. Wang, "A hybrid chaotic encryption scheme for wireless body area networks," *IEEE Access*, vol. 8, pp. 183411–183429, 2020.

[62] M. A. Murillo-Escobar, L. Cardoza-Avendano, R. M. Lopez-Gutierrez, and C. Cruz-Hernandez, "A double chaotic layer encryption algorithm for clinical signals in telemedicine," *J. Med. Syst.*, vol. 41, no. 4, p. 59, Apr. 2017, doi: 10.1007/s10916-017-0698-3.

[63] A. Pandey, B. Singh, B. S. Saini, and N. Sood, "A novel fused coupled chaotic map based confidential data embedding-then-encryption of electrocardiogram signal," *Biocybern. Biomed. Eng.*, vol. 39, no. 2, pp. 282–300, Apr. 2019, doi: 10.1016/j.bbe.2018.11.012.

[64] L. Chua, "Memristor—The missing circuit element," *IEEE Trans. Circuit Theory*, vol. 18, no. 5, pp. 507–519, Sep. 1971, doi: 10.1109/TCT.1971.1083337.

[65] A. G. Radwan, M. A. Zidan, and K. N. Salama, "HP memristor mathematical model for periodic signals and DC," in *Proc. 53rd IEEE Int. Midwest Symp. Circuits Syst.*, Aug. 2010, pp. 861–864.

[66] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, 2006.

[67] X. Yu, S. Park, D. Kim, E. Kim, J. Kim, W. Kim, Y. An, and S. Xiong, "A practical wearable fall detection system based on tiny convolutional neural networks," *Biomed. Signal Process. Control*, vol. 86, Sep. 2023, Art. no. 105325, doi: 10.1016/j.bspc.2023.105325.

[68] N. Al Bassam, S. A. Hussain, A. Al Qaraghuli, J. Khan, E. P. Sumesh, and V. Lavanya, "IoT based wearable device to monitor the signs of quarantined remote patients of COVID-19," *Inform. Med. Unlocked*, vol. 24, Jan. 2021, Art. no. 100588, doi: 10.1016/j.imu.2021.100588.

[69] A. Rukhin et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Special Publication 800-22, 2001, Revision 1, 2008. [Online]. Available: http://csrc.nist.gov/publications/nist-pubs/800-22-rev1/SP800-22rev1.pdf

[70] A. Daoui, M. Yamni, T. Altameem, M. Ahmad, M. Hammad, P. Plawiak, R. Tadeusiewicz, and A. A. A. El-Latif, "AuCFSR: Authentication and color face self-recovery using novel 2D hyperchaotic system and deep learning models," *Sensors*, vol. 23, no. 21, p. 8957, Jan. 2023, doi: 10.3390/s23218957.

[71] L. F. Avalos-Ruiz, C. J. Zuniga-Aguilar, J. F. Gomez-Aguilar, H. M. Cortes-Campos, and J. E. Lavin-Delgado, "A RGB image encryption technique using chaotic maps of fractional variable-order based on DNA encoding," *Chaos, Solitons Fractals*, vol. 177, Dec. 2023, Art. no. 114306, doi: 10.1016/j.chaos.2023.114306.

[72] D. V. Hoang, C. S. T. Dong, V. Van Huynh, V. T. Pham, R. Wang, H. Sun, and G. Grassi, "Building discrete maps with memristor and multiple nonlinear terms," *Integration*, vol. 90, pp. 126–130, May 2023, doi: 10.1016/j.vlsi.2023.01.013.

[73] G. Ablay, "Chaotic map construction from common nonlinearities and microcontroller implementations," *Int. J. Bifurc. Chaos*, vol. 26, no. 7, Jun. 2016, Art. no. 1650121, doi: 10.1142/S0218127416501212.

[74] *PhysioBank ATM*. Accessed: Feb. 28, 2024. [Online]. Available: https://archive.physionet.org/cgi-bin/atm/ATM

[75] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurc. Chaos*, vol. 16, no. 8, pp. 2129–2151, Aug. 2006, doi: 10.1142/S0218127406015970.

[76] N. K. Pareek, V. Patidar, and K. K. Sud, "Cryptography using multiple one-dimensional chaotic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 10, no. 7, pp. 715–723, 2005, doi: 10.1016/j.cnsns.2004.03.006.

[77] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, 2012, doi: 10.1016/j.sigpro.2011.10.023.

[78] A. Daoui, M. Yamni, H. Karmouni, M. Sayyouri, H. Qjidaa, M. Ahmad, and A. A. A. El-Latif, "Color stereo image encryption and local zero-watermarking schemes using octonion Hahn moments and modified Henon map," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8927–8954, 2022.

[79] D. Murillo-Escobar, C. Cruz-Hernandez, R. M. Lopez-Gutierrez, and M. A. Murillo-Escobar, "Chaotic encryption of real-time ECG signal in embedded system for secure telemedicine," *Integration*, vol. 89, pp. 261–270, Mar. 2023, doi: 10.1016/j.vlsi.2023.01.004.

[80] T. Alnuayri, S. Khursheed, A. L. H. Martínez, and D. Rossi, "Differential aging sensor using subthreshold leakage current to detect recycled ICs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 29, no. 12, pp. 2064–2075, Dec. 2021.

[81] S. M. Kuo, B. H. Lee, and W. Tian, *Real-Time Digital Signal Processing: Fundamentals, Implementations and Applications*. Hoboken, NJ, USA: Wiley, 2013.

[82] A. D. Algarni, N. F. Soliman, H. A. Abdallah, and F. E. A. El-Samie, "Encryption of ECG signals for telemedicine applications," *Multimedia Tools Appl.*, vol. 80, no. 7, pp. 10679–10703, Mar. 2021, doi: 10.1007/s11042-020-09369-5.

[83] C.-H. Lin, J.-X. Wu, P.-Y. Chen, C.-M. Li, N.-S. Pai, and C.-L. Kuo, "Symmetric cryptography with a chaotic map and a multilayer machine learning network for physiological signal infosecurity: Case study in electrocardiogram," *IEEE Access*, vol. 9, pp. 26451–26467, 2021, doi: 10.1109/ACCESS.2021.3057586.

[84] M. A. Murillo-Escobar, C. Cruz-Hernandez, L. Cardoza-Avendano, D. Murillo-Escobar, and R. M. Lopez-Gutierrez, "Multibiosignal chaotic encryption scheme based on spread spectrum and global diffusion process for e-health," *Biomed. Signal Process. Control*, vol. 78, Sep. 2022, Art. no. 104001, doi: 10.1016/j.bspc.2022.104001.

[85] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *J. Sel. Areas Telecommun. (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.

ACHRAF DAOUI was born in Taounate, Morocco, in 1991. He received the B.Eng. degree in electrical engineering and the M.S. degree in engineering science from the Faculty of Science, Université Sidi Mohammed Ben Abdellah, Fes, Morocco, in 2013 and 2018, respectively, and the Ph.D. degree in electrical engineering from the Laboratory of Engineering, Systems, and Applications, National School of Applied Sciences, Université Sidi Mohamed Ben Abdellah University, in 2022. His research interests include signal processing, image processing, pattern recognition, robotic control, and embedded systems. With over 49 publications, including book chapters, journal articles, and conference papers, he has made significant contributions to the field. Additionally, he serves as a Reviewer for several high-impact factor journals, such as *Pattern Recognition*, *Expert Systems with Applications*, *Artificial Intelligence Review*, and *Journal of Ambient Intelligence and Humanized Computing*.

MOHAMED YAMNI was born in Fes, Morocco, in 1993. He received the B.Eng. degree in electrical engineering, the M.S. degree in engineering science, and the Ph.D. degree in electrical engineering from FSDM, Université Sidi Mohammed Ben Abdellah, Fes, in 2022.

His scholarly contributions are evident through his extensive publication record, which comprises over 39 works, including book chapters, journal articles, and conference papers. His research interests include signal processing, image processing, pattern recognition, and embedded systems.

Dr. Yamni actively contributes to the academic community, as a reviewer for several prestigious journals with high impact factors.

PAWEŁ PŁAWIAK was born in Ostrowiec, Poland, in 1984. He received the B.Eng. and M.Sc. degrees in electronics and telecommunications and the Ph.D. degree (Hons.) in biocybernetics and biomedical engineering from the AGH University of Science and Technology, Kraków, Poland, in 2012 and 2016, and the D.Sc. degree in technical computer science and telecommunications from Silesian University of Technology, Gliwice, Poland, in 2020. He is currently the Dean of the Faculty of Computer Science and Telecommunications and an Associate Professor with the Cracow University of Technology, Kraków, and the Deputy Director for Research of the National Institute of Telecommunications, Warsaw, and an Associate Professor with the Institute of Theoretical and Applied Informatics, The Polish Academy of Sciences, Gliwice. He has published more than 50 articles in refereed international SCI-IF journals. His research interests include machine learning and computational intelligence (e.g., artificial neural networks, genetic algorithms, fuzzy systems, support vector machines, k-nearest neighbors, and hybrid systems), ensemble learning, deep learning, evolutionary computation, classification, pattern recognition, signal processing and analysis, data analysis and data mining, sensor techniques, medicine, biocybernetics, biomedical engineering, and telecommunications. He is an academic editor and a reviewer of many prestigious and reputed journals.

OSAMA ALFARRAJ received the master's and Ph.D. degrees in information and communication technology from Griffith University, in 2008 and 2013, respectively. He is currently a Professor of computer sciences with King Saudi University, Riyadh, Saudi Arabia. His current research interests include eSystems (eGov, eHealth, and ecommerce), cloud computing, and big data. He served as a Consultant and a member for Saudi National Team for Measuring E-Government, Saudi Arabia, for two years.

AHMED A. ABD EL-LATIF (Senior Member, IEEE) received the B.S. and M.S. degrees in computer science from Menoufia University, Egypt, and the Ph.D. degree in computer science from Harbin Institute of Technology, Harbin, China. He currently holds a staff position with Menoufia University, and Prince Sultan University, Saudi Arabia. He has published over 300 papers in quality journals and conference proceedings, including 15 books, with over 11 500 citations. He is the Head of the MEGANET 6G Lab Research in Russian Federation. He is the Founder and the Deputy Director of the Center of Excellence in Quantum and Intelligent Computing, Prince Sultan University. He has received many awards, including the State Encouragement Award in Engineering Sciences from Egypt in 2016, the Best Ph.D. Student Award from Harbin Institute of Technology, China, in 2013, and the Young Scientist Award from Menoufia University, in 2014. He is actively engaged in the scientific community, serving as the chair or the co-chair for several conferences and holding editorial positions in various quality journals. His research interests include quantum communications, cybersecurity, AIoT, AI-based image processing, information hiding, and applications of dynamical systems in cybersecurity.