Biomedical Signal Processing and Control 112 (2026) 108494

Contents lists available at ScienceDirect

Biomedical Signal Processing and Control

journal homepage: www.elsevier.com/locate/bspc

A novel five-term 3D chaotic system with two squared nonlinearities and its secure communication application for biomedical data

Abdullah Gokyildirim [a,*], Uğur Erkin Kocamaz [b], Haris Calgan [c]

[a] Department of Electrical and Electronics Engineering, Faculty of Engineering and Natural Sciences, Bandırma Onyedi Eylül University, Bandirma, Balikesir, 10200, Turkiye
[b] Department of Computer Technologies, Vocational School of Karacabey, Bursa Uludağ University, Karacabey, Bursa, 16700, Turkiye
[c] Department of Electrical and Electronics Engineering, Faculty of Engineering, Balıkesir University, Cagis, Balikesir, 10145, Turkiye

ARTICLE INFO

Keywords:
Secure communication
Simple chaotic systems
Bifurcation
Squared nonlinearity
Electronic circuit
Biomedical data encryption

ABSTRACT

Ensuring secure communication of biomedical data has become increasingly important due to its sensitive nature. Chaotic systems, with their inherent unpredictability and sensitivity to initial conditions, offer a promising approach for secure data encryption. This study introduces a novel five-term chaotic system that includes two squared nonlinearities, a unique configuration not previously reported in the literature. The system's dynamics are analyzed through equilibrium points, stability, bifurcation diagrams, and Lyapunov Exponents (LEs), where the Kaplan–Yorke dimension is found to be 2.1471 under selected parameters, confirming strong chaotic behavior. An electronic implementation of the system is achieved using standard analog components, validating its physical feasibility. The system is then applied to encrypt biomedical signals and images. In secure ECG signal transmission tests conducted on a Raspberry Pi, synchronization is achieved within 4 s using Sliding Mode Control (SMC). The encryption algorithm demonstrates high key sensitivity and a large key space. For biomedical image encryption, the proposed method achieves a Number of Pixels Change Rate (NPCR) of 99.56% and a Unified Average Changing Intensity (UACI) of 33.31%, indicating strong encryption performance. These results confirm that the proposed chaotic system is efficient, lightweight, and highly suitable for secure biomedical communication.

1. Introduction

Biomedical data holds significant value in diagnostics within healthcare systems. This data, including patients' diagnostic results, can be stored in the form of digital signals and images. Such data frequently includes sensitive information, such as personal data of patients. Therefore, ensuring the security of the storage and transmission of this information is crucial to safeguard the privacy of patients. While conventional encryption schemes provide protection during transmission, preventing unauthorized access and protecting entire content still pose significant challenges due to certain limitations. In this context, chaos-based cryptography presents a promising array of methods that offer advantages over traditional encryption methods [1]. Encryption techniques employing chaotic systems utilize synchronization of chaotic systems to generate random signals for encryption. Therefore, utilizing a new chaotic system plays a crucial role in biomedical data encryption applications and increases security.

After Lorenz discovered and identified chaotic behavior in a meteorology-based system [2], Rössler [3], Chua [4], Chen [5], and many other new chaotic systems have been introduced to the literature. In 1984, Hoover proposed the first three-dimensional five-term chaotic system with a simplification of Nosé's system, which became known as the Nosé–Hoover chaotic system [6,7]. In 1994, Sprott searched for three-dimensional chaotic systems with five terms and two quadratic nonlinearities, and found this system along with four other systems [8,9]. Thus, it is also named as the Sprott-A chaotic flow. It has two quadratic nonlinearities, one of them is a squared term. It is one of the important chaotic systems due to its simplicity. In 1997, Sprott discovered the simplest dissipative chaotic flow [10]. It is a jerk system and has only one nonlinearity (a squared term). Then, Sprott searched and found many jerk chaotic systems [11,12]. Afterwards, the research of small chaotic systems has caught a lot of attention from scientists, and several five-term chaotic systems have been discovered [13–28]. These systems have different characteristics such as including trigonometric functions [11,12,27], sign functions [17,22,23], absolute-values [11,12,14,20], and exponential [16,28] nonlinearities. They can also include squared [9–14,18,19,22–24,26], cubic [11,12,15,18,19], and

* Corresponding author.
E-mail addresses: agokyildirim@bandirma.edu.tr (A. Gokyildirim), ugurkocamaz@uludag.edu.tr (U.E. Kocamaz), haris.calgan@balikesir.edu.tr (H. Calgan).

https://doi.org/10.1016/j.bspc.2025.108494
Received 19 March 2025; Received in revised form 8 July 2025; Accepted 2 August 2025
Available online 15 August 2025

quartic [25] terms. It is remarkable that most of the five-term 3D chaotic systems have a squared term. Interestingly, none of them has two squared terms. In existing literature, systems with two or more squared terms are typically found in chaotic systems consisting of six or more terms [29–39]. Motivated by this observation, the present work introduces a novel five-term 3D chaotic system, uniquely characterized by two squared nonlinear terms.

Chaotic systems are highly favored in cryptography applications due to their sensitivity to initial conditions and system parameters, as well as their unpredictability, high randomness, deterministic nature, and noise-like structure. As a result, they have gained significant popularity in this area [40–43]. The effectiveness of chaos-based cryptography in transmitting biomedical data has been demonstrated, leading to its widespread use in encrypting such information [44]. Chaotic systems have been applied in various encryption tasks, including dorsal hand vein image encryption [45], fingerprint image encryption [46], encryption–decryption and transmission of electrocardiography (ECG) and electromyography (EMG) signals [1], encryption–decryption of COVID-19 X-ray images [47], multi-mode synchronization-based medical image encryption [48] and more. It can be inferred from reported studies that some well-known chaotic systems are used in biomedical data encryption applications. Recently, newly discovered chaotic systems have been used in various encryption applications. Tsafack et al. have proposed a novel chaotic map and employed it in internet of health things [49]. Lin et al. have presented a hyperchaotic memristive ring neural network consisting of four neurons and one non-ideal flux-controlled memristor [50]. They also developed a medical image encryption scheme using hardware implemented with a field-programmable gate array. Ramar et al. have represented a new chaotic jerk system for biomedical image encryption [51]. Chai et al. have introduced a new 5-scroll Rössler hyperchaotic system and explored its application in secure transmission of natural and medical images using block compressive sensing [52]. Ding et al. have proposed a fractional-order memristor-coupled Hindmarsh–Rose neurons model and used for a medical image encryption algorithm based on the region of interest [53]. That approach leverages the unique dynamics of the fractional-order system and memristor coupling to enhance encryption performance and security, targeting specific areas within medical images to optimize the encryption process. Additionally, the recent literature includes studies on encryption applications for various biomedical images, such as iris [54], fingerprint [55], and brain MRI [56] images.

In the present work, a novel five-term 3D chaotic flow is introduced, which includes two squared nonlinear terms, one other quadratic nonlinearity, and two linear terms. The aim in designing this chaotic system is to create a five-term structure with the simplest possible configuration. Following the previous work on a five-term 3D chaotic system with cubic nonlinearity [15], this study presents a distinct system configuration involving two squared nonlinear terms. To the best of our knowledge, such a configuration has not been reported before in a five-term structure. Implementing secure communication applications with a less well-known system is advantageous. Thus, the control signal used to synchronize master–slave systems will be more complex due to the inclusion of two nonlinear terms. Consequently, it will be more challenging for individuals unfamiliar with the equation to solve it, thereby enhancing the security level. Additionally, despite its five-term structure, the chaotic system maintains its simplicity. Moreover, having five terms is beneficial for electronic circuit applications. Applications for the encryption of biomedical data based on this newly discovered simple chaotic system may be of interest, especially when secure communication is required to protect patient privacy. Therefore, the highlights of this study are summarized as follows in terms of contributions:

- A novel chaotic system is proposed, featuring only five terms and incorporating two squared nonlinear terms, making it unique in this aspect.
- Two different operating conditions are determined to conduct dynamic analyses such as phase portraits, Lyapunov Exponents (LEs), bifurcation diagrams, and stability analysis.
- The existence of chaotic flows is verified by means of circuit implementations using standard components.
- Chaotic synchronization is designed based on Sliding Mode Control (SMC) technique.
- Secure communication of ECG signals is designed and implemented on a Raspberry Pi computer.
- A biomedical image encryption–decryption scheme is designed and tested.

The rest of this paper is organized as follows: In Section 2, the differential equations of the novel chaotic system are given and its time series, phase planes, LEs and bifurcation diagrams are demonstrated. In Section 3, the applicability of the novel chaotic system is verified through electronic circuit implementation. In Section 4, engineering applications of biomedical data such as secure communication of biomedical signals and encryption–decryption of biomedical images are conducted. Section 5 discusses the limitations of study. Finally, conclusions are given in Section 6.

2. The novel five-term chaotic system with two squared nonlinearities

2.1. Modeling of the system

The differential equations of the novel five-term chaotic system are expressed by

$$\begin{aligned} \dot{x} &= yz, \\ \dot{y} &= ay^2 - bx, \\ \dot{z} &= cx^2 - dz, \end{aligned} \tag{1}$$

where a, b, c, and d are the system parameters. When $a = 1$, $b = 1$, $c = 5.2$, $d = 1$ and the initial conditions $x(0), y(0), z(0) = (0.5, 0.75, 1)$ are set for the system parameters, system (1) generates chaotic attractors, as depicted in Fig. 1.

2.2. Lyapunov exponents and bifurcation diagrams

LEs and bifurcation diagrams are essential concepts in nonlinear systems. The sensitivity of a dynamic system to initial conditions can be quantified by LEs spectra. Positive LEs indicate chaos and sensitivity to initial conditions, while negative exponents lead to stability. Bifurcation diagrams, on the other hand, visually represent the impact of a parameter change on the system's behavior. They help in understanding the complex and often unpredictable behavior that can arise in nonlinear systems, revealing transitions, bifurcations, and the emergence of chaotic patterns. To observe the dynamic behavior of the newly discovered system, LEs and bifurcation diagrams are separately computed for four parameter values. In all bifurcation and Lyapunov analyses in this section, a step size of 0.01 s was used. The results are depicted in Fig. 2. On the other hand, dynamic analyses are examined for cases where certain parameter values of the system are considered together. Fig. 3 illustrates the results of LEs and bifurcation diagrams for the scenarios where the parameter values are $c = d$, $a = b = d$, and $a = b = c = d$, respectively. The boxes within the bifurcation diagrams present detailed bifurcation maps showing the transitions from periodic states to chaotic states. Additionally, the Poincaré section plots for the system parameter c equals to 5.2 are shown in Fig. 4.

In this case, chaotic motions are examined where the values of the system's four parameters are around 0.2. Fig. 5 depicts LEs and the corresponding bifurcation diagram for the parameter values of b, c, and d equal to 0.2. According to the bifurcation diagram in Fig. 5, when a is 0.193, the system depicts chaotic behavior. The phase planes obtained for $a = 0.193$ are presented in Fig. 6. Furthermore, time series of x, y, and z obtained for different initial conditions are shown in Fig. 7. The

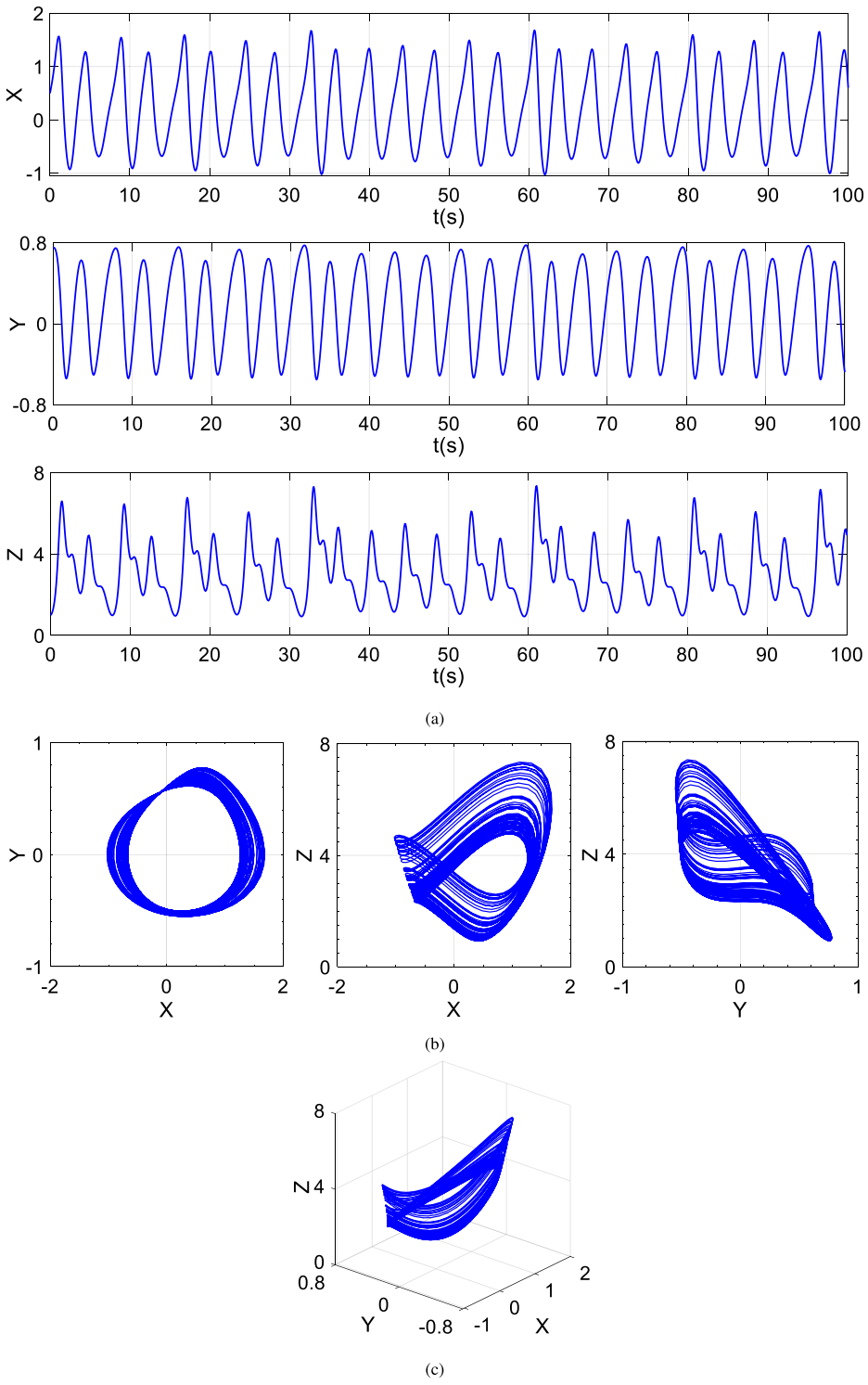

Fig. 1. Chaotic time series and phase plots of system (1) for $a = 1$, $b = 1$, $c = 5.2$, and $d = 1$: (a) Time series when $t(s)$ in the range [0,100] seconds, $h = 0.001$. (b) 2D and, (c) 3D phase portraits.

dynamic analysis indicates that system parameter values around 0.2 are more suitable for further applications. When comparing the Figs. 1 and 7, it is evident that the system exhibits less oscillations with parameter values around 0.2 within the same time frame. This low-frequency behavior can be advantageous for cryptographic applications in Section 4.

Fig. 7 shows that the system's behavior varies depending on the initial conditions. This indicates that unpredictability will be high in biomedical encryption applications to be performed in Section 4. As a result of the simulations, it is determined that the most appropriate operating conditions for the realization of the system's electronic circuit occur when all of the system parameters have values around 0.2. The

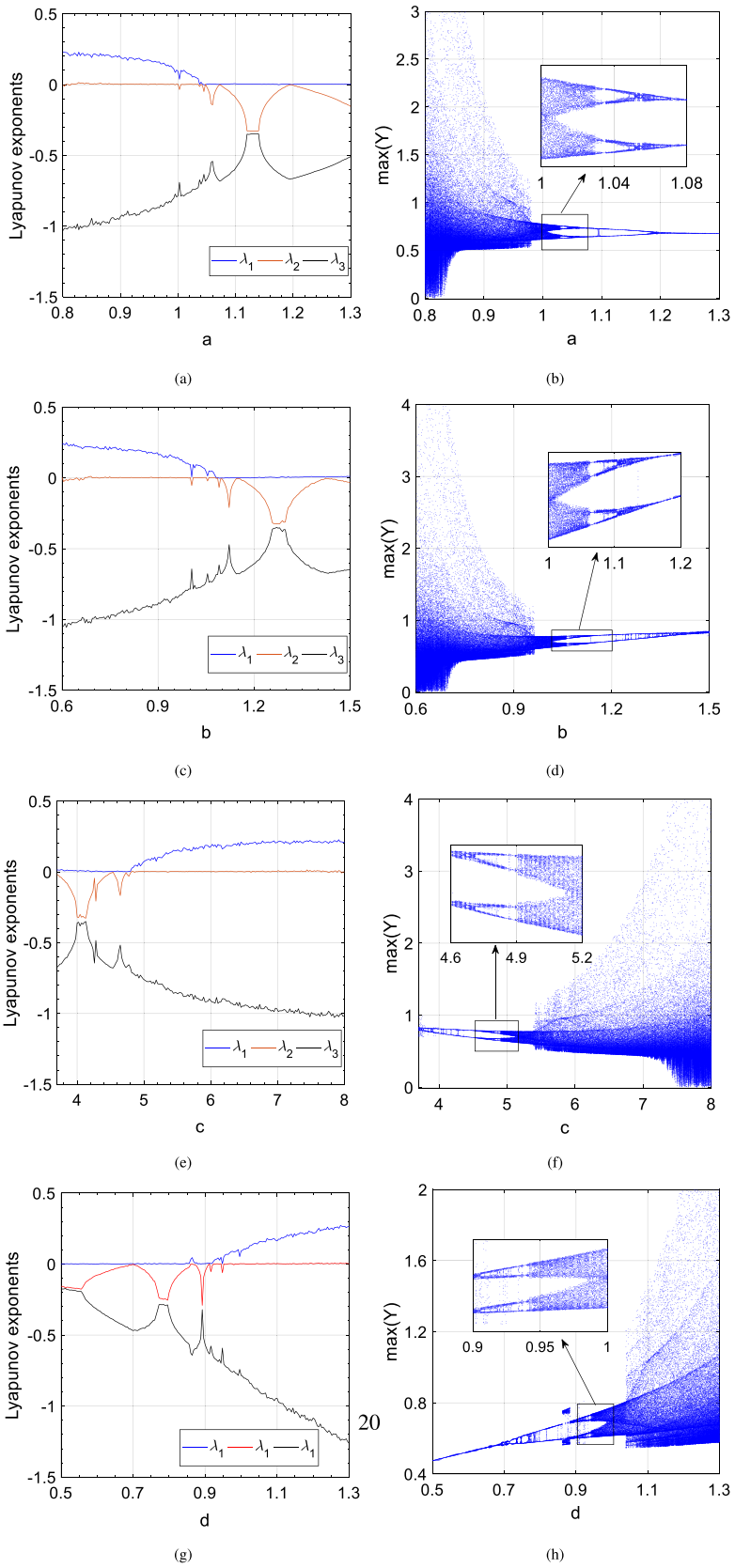

Fig. 2. LEs and bifurcation maps for (a–b) a parameter with $b = 1$, $c = 1$, and $d = 1$, (c–d) b parameter with $a = 1$, $c = 1$, and $d = 1$, (e–f) c parameter with $a = 1$, $b = 1$, and $d = 1$, (g–h) d parameter with $a = 1$, $b = 1$, and $c = 1$.

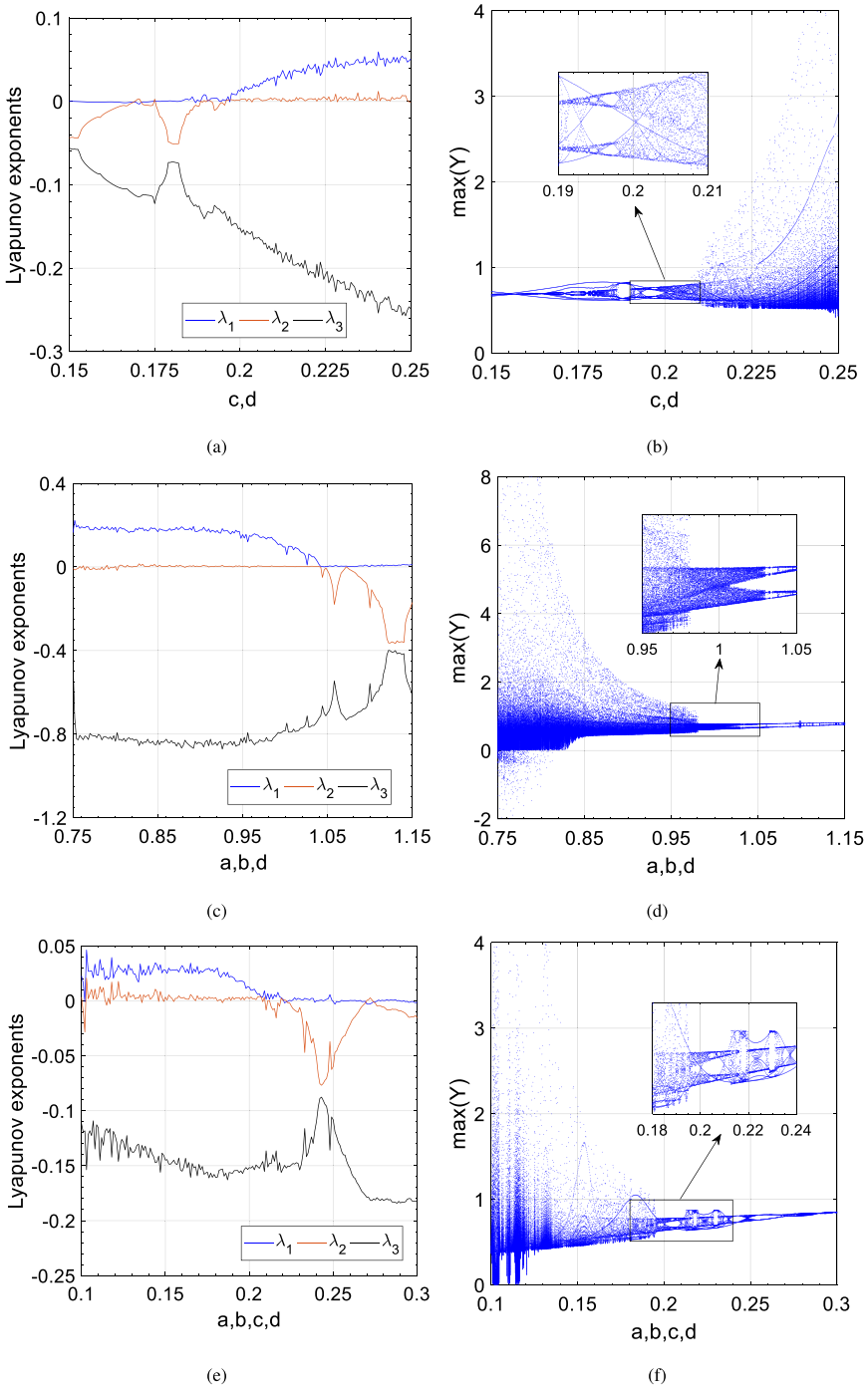

Fig. 3. LEs and bifurcation maps for (a–b) parameters $c = d$ with $a = 0.2$, and $b = 0.2$, (c–d) parameters $a = b = d$ with $c = 5.2$, (e–f) parameters $a = b = c = d$.

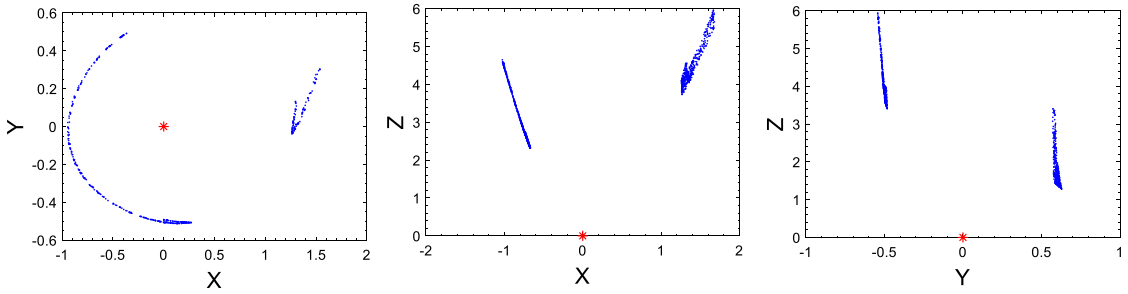

Fig. 4. Poincaré section plots of chaotic system (1) with $a = 1$, $b = 1$, $c = 5.2$, and $d = 1$ in (a) x–y phase portrait at $z = 4$, (b) x–z phase portrait at $y = 0$, (c) y–z phase portrait at $x = 0$.

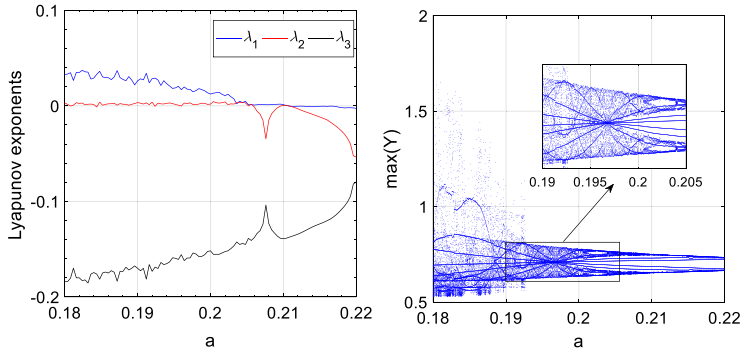

Fig. 5. LEs and bifurcation maps for a parameter with $b = 0.2$, $c = 0.2$, and $d = 0.2$.

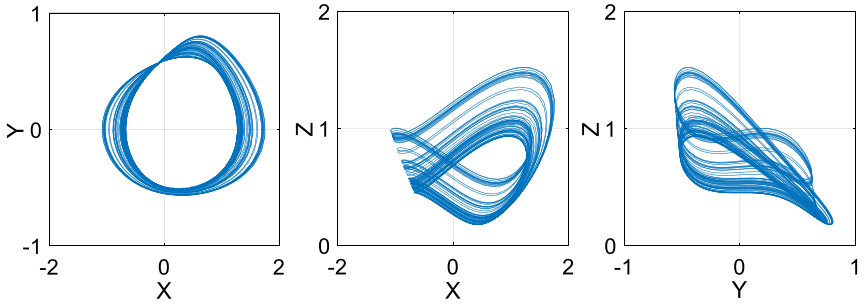

Fig. 6. Phase portraits of chaotic system (1) with $a = 0.193$, $b = c = d = 0.2$ and $t = 50 - 1500$s.

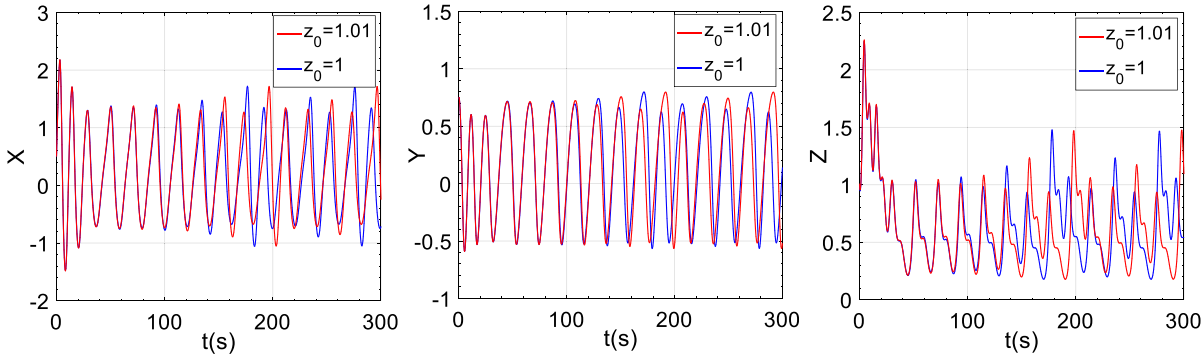

Fig. 7. Sensitivity to initial conditions of chaotic system (1) with $a = 0.193$, $b = 0.2$, $c = 0.2$, $d = 0.2$, $x(0) = 0.5$, $y(0) = 0.75$, and $z(0) = 1$, 1.01.

Table 1
The LEs, eigenvalues and D_{KY} for different cases.

The System (1)	LE $\{\lambda_1, \lambda_2, \lambda_3\}$	Eigenvalues $\{\mu_1, \mu_2, \mu_3\}$	D_{KY}
Case A ($a = b = d = 1, c = 5.2$)	{0.09, 0, –0.779}	{0, 0, –1}	2.1155
Case B ($a = b = c = d = 0.22$)	{0.00083, 0, –0.1495}	{0, 0, –0.22}	2.0055
Case C ($a = 0.193, b = c = d = 0.2$)	{0.024, 0, –0.1631}	{0, 0, –0.2}	2.1471

circuit of the system with market components will be implemented in the next section.

2.3. Stability analysis

By setting $\dot{x} = 0$, $\dot{y} = 0$, $\dot{z} = 0$, the equilibria can be calculated by solving the system (1) as follows:

$$\begin{cases} yz = 0, \\ ay^2 - bx = 0, \\ cx^2 - dz = 0. \end{cases} \tag{2}$$

Thus, this chaotic system has only the zero equilibrium point: E_0(0, 0, 0). Next, dynamic analyses are carried out for two cases determined by the system parameter values.

Case-A: $a = 1$, $b = 1$, $c = 5.2$ and $d = 1$ and initial conditions are taken as $\{x(0), y(0), z(0)\} = \{0.5, 0.75, 1\}$.

In this case, the LEs of the system (1) can be obtained as $\lambda_1 = 0.09$, $\lambda_2 = 0$, and $\lambda_3 = -0.779$. Since $\lambda_1 < -\lambda_3$ of the system (1) is met, the system is dissipative. If a dissipative system's maximum LE is positive, the system exhibits chaotic behavior [57]. Hence, the novel system (1) shows a chaotic attractor. Furthermore, the Kaplan–Yorke dimension (D_{KY}) is determined for the system (1) as follows:

$$D_{KY} = j + \frac{\sum_{i=1}^{j} \lambda_i}{\left|\lambda_{j+1}\right|} \tag{3}$$

According to Eq. (3), D_{KY} of the system (1) in Case A is calculated as 2.1155 where $j = 2$. Linearization of the system (1) at E_0(0, 0, 0) results in the eigenvalues as $\mu_{1,2} = 0$ and $\mu_3 = -1$. This proves that E_0(0, 0, 0) is a non-hyperbolic saddle–node equilibrium.

Case-B: $a = b = c = d = 0.22$ and initial conditions are set to $\{x(0), y(0), z(0)\} = \{0.5, 0.75, 1\}$.

When all parameter values are set to 0.22, $\lambda_1 = 0.00083$, $\lambda_2 = 0$, and $\lambda_3 = -0.1495$, respectively. Substituting the LEs into Eq. (3) yields $D_{KY} = 2.0055$. The eigenvalues are determined as $\mu_{1,2} = 0$ and $\mu_3 = -0.22$.

Case-C: $a = 0.193$, $b = 0.2$, $c = 0.2$, $d = 0.2$ and $\{x(0), y(0), z(0)\} = \{0.5, 0.75, 1\}$.

In this instance, the LEs of the system (1) can be derived as $\lambda_1 = 0.024$, $\lambda_2 = 0$, and $\lambda_3 = -0.1631$. The linearization of system (1) at E_0(0, 0, 0) yields eigenvalues $\mu_{1,2} = 0$ and $\mu_3 = -0.2$, indicating that E_0(0, 0, 0) represents a non-hyperbolic saddle–node equilibrium. Table 1 shows the LEs, eigenvalues and D_{KY} for all the cases described above.

3. Electronic circuit implementation

Following numerous simulations conducted in the ORCAD-Pspice program, utilizing the bifurcation diagrams presented in the previous section, optimal resistance values dependent on parameters and capacitance values are obtained for the implementation of the analog circuit. Accordingly, the schematic diagram of the electronic circuit designed for system (1), which is approximately consistent with the bifurcation diagram in Fig. 4 and phase portraits in Fig. 5, is given in Fig. 8 with corresponding resistance and capacitance values.

The circuit includes only a minimum number of passive circuit elements, consists of 5 resistors and 3 capacitors. Additionally, three AD633 multiplier integrated circuits and TL081 op-amps are used. All the circuit components used are readily available in the market [58].

Considering the electronic circuit diagram, the dimensionless equations of the system (1) is reformulated as below:

$$\begin{aligned} RC\dot{v}_x &= \frac{Rv_y v_z}{10R_1}, \\ RC\dot{v}_y &= \frac{R(v_y)^2}{10R_2} - \frac{Rv_x}{R_3}, \\ RC\dot{v}_z &= \frac{R(v_x)^2}{10R_4} - \frac{Rv_z}{R_5}, \end{aligned} \tag{4}$$

where the values of passive elements are $R_1 = 40$ kΩ, $R_2 = 222.23$ kΩ, $R_3 = 2$ MΩ, $R_4 = 200$ kΩ, $R_5 = 2$ MΩ and $C_1 = C_2 = C_3 = C = 1$ nF. The DC supply source values are chosen as $V_P = -V_N = 15$ V, and the time scale factor R_C is 0.4 ms. $x(0) = 0.5$, $y(0) = 0.75$, and $z(0) = 1$ are selected as initial conditions. In Fig. 9, the relationships between the voltages across the X, Y, and Z terminals are observed using the OrCAD-PSpice program for the time range t = 0–300 ms, with a maximum step size of 0.1 ms. Terminal voltage values are also examined with a maximum step size of 0.7 ms. The phase planes and FFT graphs of the novel attractor for the time range t = 0–300 ms, with a maximum step size of 0.7 ms, are shown in Fig. 10.

To demonstrate the applicability of the newly discovered system (1), it is implemented electronically. The oscilloscope views and the analog circuit constructed on the electronic board are depicted in Fig. 11. Consequently, the oscilloscope measurements are highly consistent with the OrCAD-Pspice results.

4. Secure communication applications of the novel chaotic system using biomedical data

In this section, secure communication and image encryption applications are implemented using the proposed novel chaotic system. Biomedical data are utilized for both applications. A synchronized system is created to securely transmit biomedical information by considering the dependency of chaotic systems on initial values. Subsections detail the secure transmission of ECG signals and various biomedical image encryption–decryption applications.

4.1. Secure communication of ECG signals

In this study, electrocardiography (ECG) is utilized for the secure communication of biomedical signals. A classical SMC is applied to synchronize master–slave chaotic systems, adjusting the controller based on the error to achieve system synchronization. Fig. 12 illustrates the schema of the secure communication system. The primary side employs the chaotic masking method, utilizing z_1 in the encryption algorithm. x_1 and y_1 are utilized for chaos synchronization through the SMC and are consequently transmitted to the slave system. Eqs. (5) and (6) define the master and slave chaos systems, respectively.

$$\begin{aligned} \dot{x}_1 &= y_1 z_1, \\ \dot{y}_1 &= a y_1^2 - b x_1, \\ \dot{z}_1 &= c x_1^2 - d z_1, \end{aligned} \tag{5}$$

$$\begin{aligned} \dot{x}_2 &= y_2 z_2, \\ \dot{y}_2 &= a y_2^2 - b x_2 + u, \\ \dot{z}_2 &= c x_2^2 - d z_2. \end{aligned} \tag{6}$$

In Eqs. (5) and (6), subscriptions '1' and '2' denote the master and slave system, respectively. Upon successful synchronization, the states

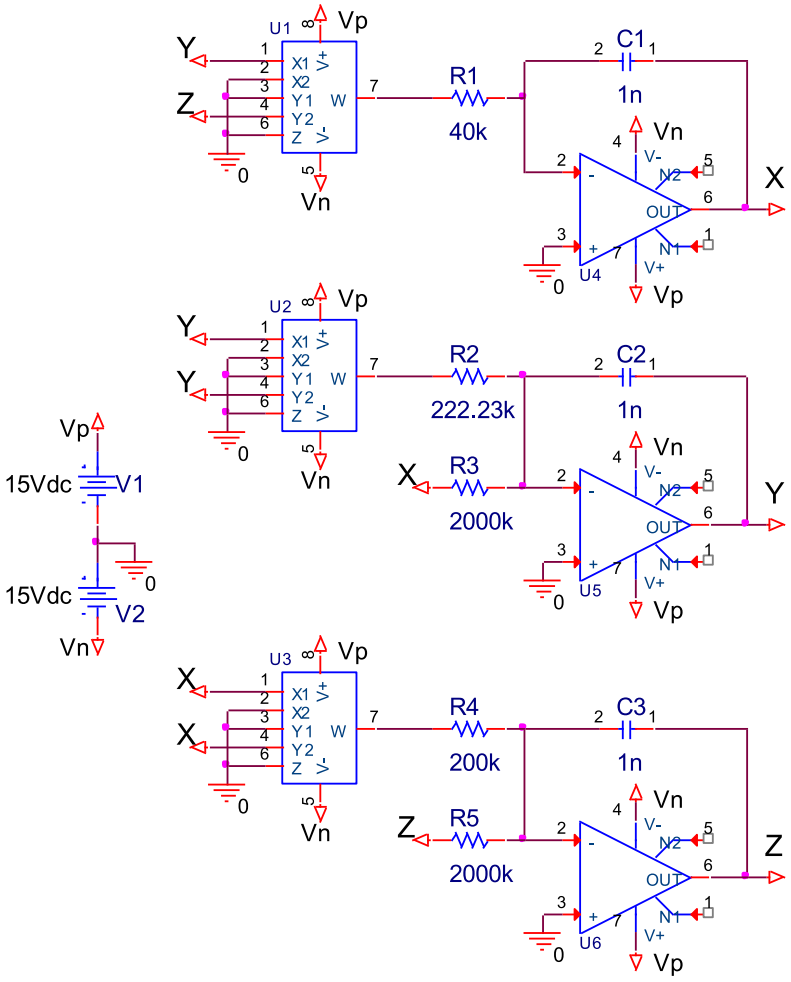

Fig. 8. ORCAD-Pspice schematic of system (1).

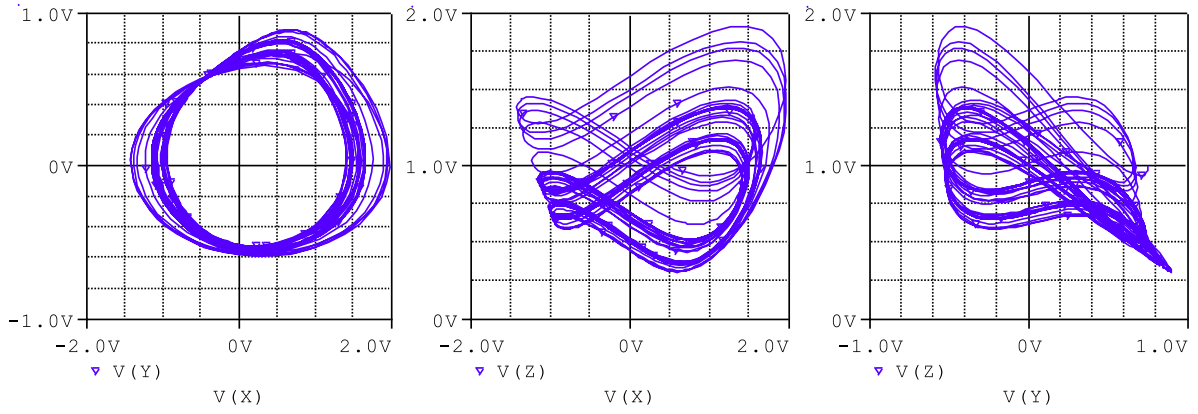

Fig. 9. Phase portraits of chaotic system (1) generated using OrCAD-Pspice program for a simulation time of t = 300 ms with a maximum step size of 0.1 ms.

of the system (6) must result in the same response with the system (5). Therefore, designing a controller plays a crucial role in chaotic synchronization. u stands for control signal in Eq. (6) and adjusted based on the SMC technique in this study where error signals are calculated as $e_1 = x_2 - x_1$, $e_2 = y_2 - y_1$, $e_3 = z_2 - z_1$. Eq. (7) defines the error system.

$$\begin{aligned} \dot{e}_1 &= z_2 e_2 + y_1 e_3, \\ \dot{e}_2 &= a(y_2^2 - y_1^2) - b e_1 + u + \Delta(t), \\ \dot{e}_3 &= c(x_2^2 - x_1^2) - d e_3. \end{aligned} \tag{7}$$

where $\Delta(t)$ represents the external disturbance and model uncertainty. It is assumed to be bounded as in Eq. (8), with δ denoting the upper bound of the disturbance. Although synchronization performance in chaotic systems is significantly influenced by unknown time delays, disturbances, and uncertainties with unknown boundaries and time-varying parameters [59,60], this study considers only external disturbances with a known upper bound.

$$|\Delta(t)| \leq \delta. \tag{8}$$

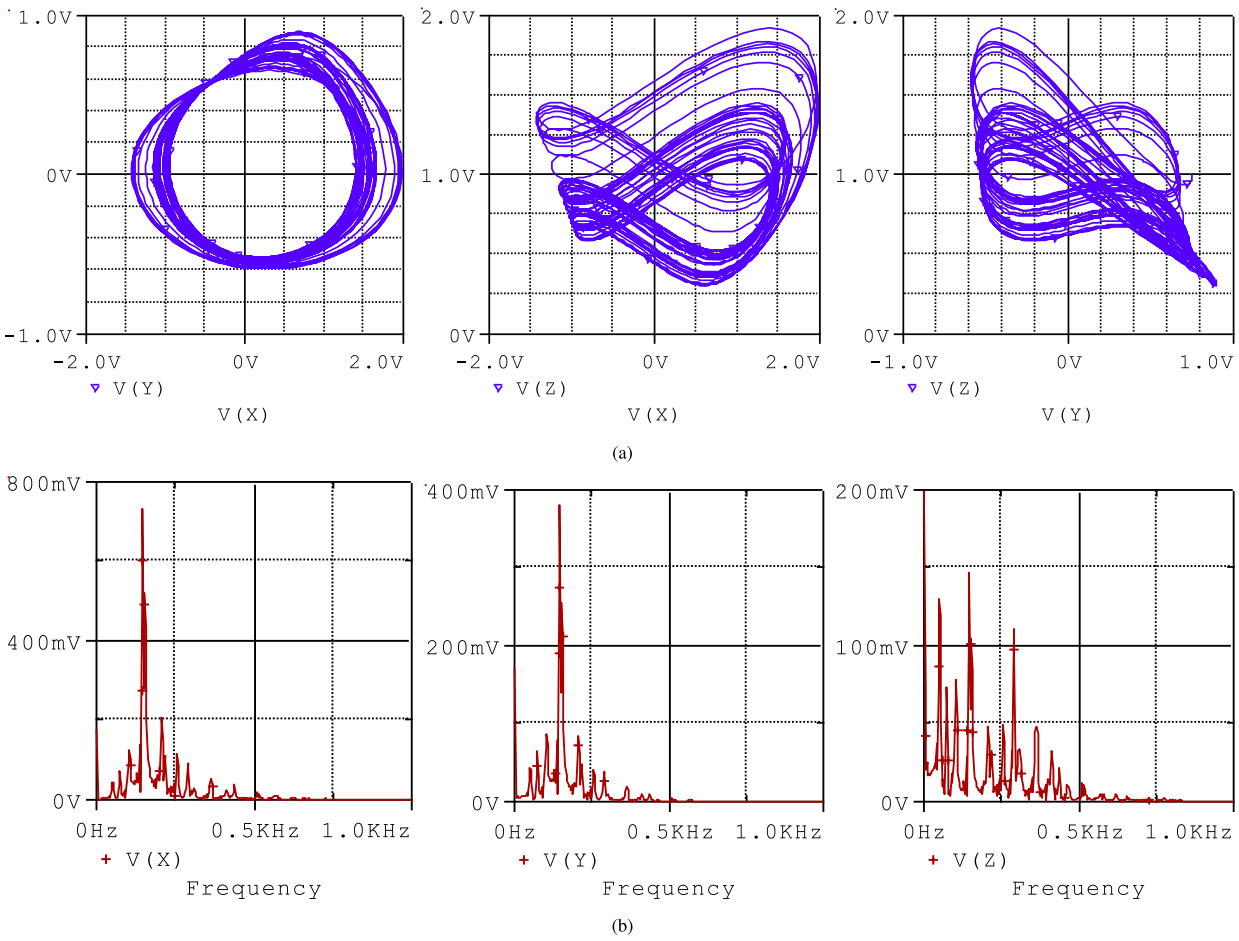

Fig. 10. Simulation results for chaotic system (1) using the OrCAD-Pspice program for a simulation time of t = 300 ms with a maximum step size of 0.07 ms: (a) Phase portraits, (b) FFT analyses.

SMC signal is formed by two parts, namely equivalent signal u_{eq} and switching signal u_{sw}. Since the sliding surface is defined as summation of errors as in Eq. (9)

$$s = e_1 + e_2 + e_3. \tag{9}$$

The equivalent signal can be determined by setting $\dot{s} = 0$, as shown below:

$$\begin{aligned} &\dot{s} = \dot{e}_1 + \dot{e}_2 + \dot{e}_3 = 0, \\ &\dot{s} = z_2 e_2 + y_1 e_3 + a(y_2^2 - y_1^2) - b e_1 + u + \Delta(t) + c(x_2^2 - x_1^2) - d e_3 = 0. \end{aligned} \tag{10}$$

Therefore, the u_{eq} is found as:

$$u_{eq} = -z_2 e_2 - y_1 e_3 - a(y_2^2 - y_1^2) + b e_1 - c(x_2^2 - x_1^2) + d e_3. \tag{11}$$

The switching signal can be defined as $u_{sw} = -(k + \delta) \cdot sign(s)$ in order to compensate for the upper bound of the disturbance, where k is a constant and $sign(\cdot)$ is calculated as given in Eq. (12).

$$sign(s) = \begin{cases} -1, & if\ s < 0, \\ 0, & if\ s = 0, \\ 1, & if\ s > 0. \end{cases} \tag{12}$$

Consequently, the designed SMC (u) is formed by summation of u_{eq} obtained in Eq. (11) and u_{sw} ($u = u_{eq} + u_{sw}$). The Lyapunov function given in Eq. (13) is used for proving the stability of the designed u as below [61]:

$$V(s) = \frac{1}{2} s^2, \quad \text{for } s = e_1 + e_2 + e_3, \tag{13}$$

where ($\dot{V} = s \cdot \dot{s}$) < 0 shows that the errors convergence to zero. Taking the time derivative of $V(s)$:

$$\dot{V} = s \cdot \dot{s}. \tag{14}$$

From the error dynamics in Eq. (7), and using $\dot{s} = \dot{e}_1 + \dot{e}_2 + \dot{e}_3$, following can be obtained:

$$\begin{aligned} &\dot{s} = z_2 e_2 + y_1 e_3 + a(y_2^2 - y_1^2) - b e_1 + u + \Delta(t) + c(x_2^2 - x_1^2) - d e_3, \\ &u = u_{eq} + u_{sw}. \end{aligned} \tag{15}$$

Substituting the expression of u_{eq} and u_{sw}:

$$\begin{aligned} &u_{eq} = -z_2 e_2 - y_1 e_3 - a(y_2^2 - y_1^2) + b e_1 - c(x_2^2 - x_1^2) + d e_3, \\ &u_{sw} = -(k + \delta) \cdot \text{sign}(s). \end{aligned} \tag{16}$$

Substituting into $\dot{s}$:

$$\begin{aligned} \dot{s} &= z_2 e_2 + y_1 e_3 + a(y_2^2 - y_1^2) - b e_1 + u_{eq} + u_{sw} + \Delta(t) + c(x_2^2 - x_1^2) - d e_3 \\ &= z_2 e_2 + y_1 e_3 + a(y_2^2 - y_1^2) - b e_1 \\ &\quad + [-z_2 e_2 - y_1 e_3 - a(y_2^2 - y_1^2) + b e_1 - c(x_2^2 - x_1^2) + d e_3] \\ &\quad + u_{sw} + \Delta(t) + c(x_2^2 - x_1^2) - d e_3 \end{aligned} \tag{17}$$

Combining and simplifying, most terms cancel:

$$\dot{s} = u_{sw} + \Delta(t). \tag{18}$$

Thus, the Lyapunov derivative becomes:

$$\dot{V} = s \cdot \dot{s} = s \cdot \Delta(t) - (k + \delta)|s|. \tag{19}$$

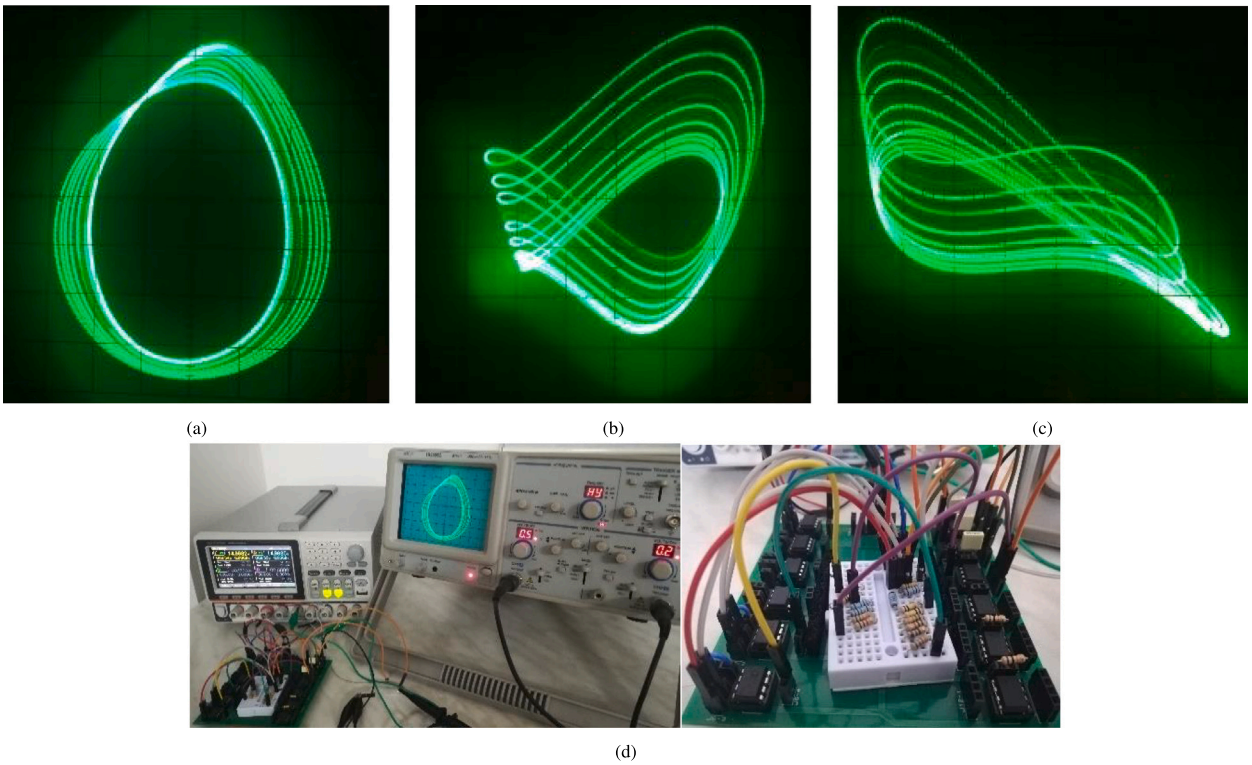

Fig. 11. Oscilloscope views of chaotic system (1): (a) v_x (0.5 V/div) versus v_y (0.2 V/div), (b) v_x (0.5 V/div) versus v_z (0.2 V/div), (c) v_y (0.2 V/div) versus v_z (0.2 V/div), and (d) the analog circuit on the electronic board.

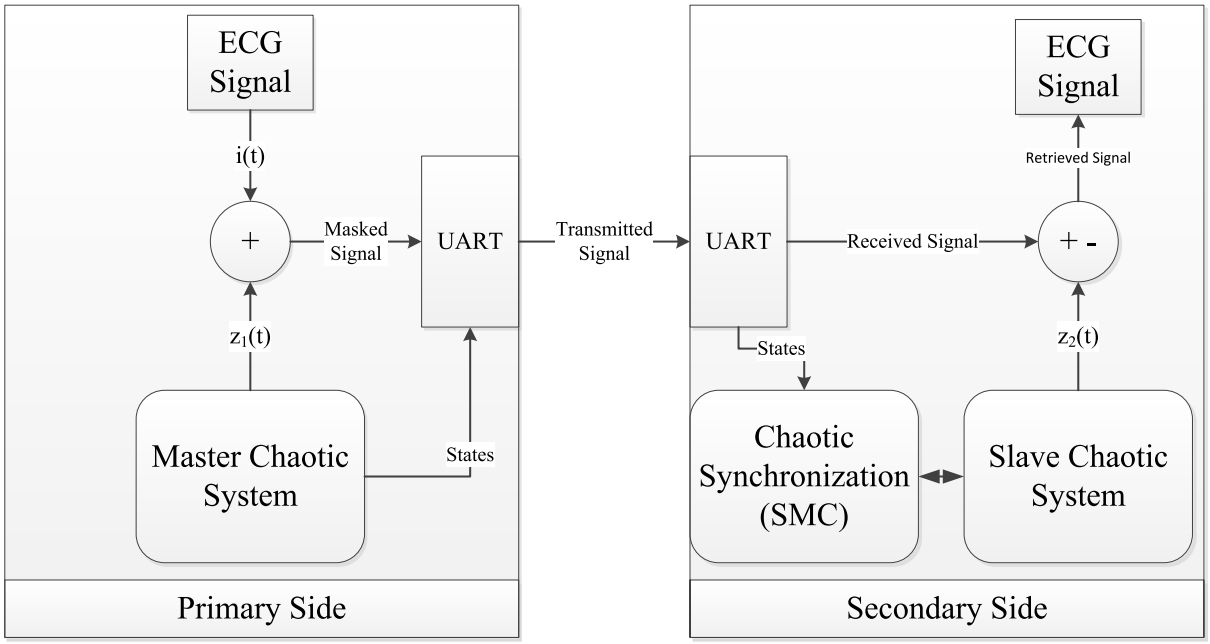

Fig. 12. Block diagram of secure communication of ECG signal.

Since $|\Delta(t)| \leq \delta$, we obtain:

$$\dot{V} \leq \delta|s| - (k+\delta)|s| = -k|s| < 0 \quad \text{for } k > 0. \tag{20}$$

This ensures that $\dot{V}$ is negative definite, and the sliding surface $s \to 0$ as $t \to \infty$. Note that the Lyapunov function $V(s) = \frac{1}{2}s^2$ is positive definite and radially unbounded, and its derivative $\dot{V}$ is negative definite under the condition $k > \delta$, which satisfies the criteria of Lyapunov's direct method for global stability. If the external disturbances are bounded as $|\Delta(t)| \leq \delta$, then $\dot{V} \leq (|\Delta(t)| - (k+\delta))|s| < 0$ is guaranteed provided that $k > \delta$. Under this condition, the system trajectories are driven toward the sliding surface, and the error dynamics are either asymptotically stable or ultimately bounded. Therefore, the designed SMC ensures robust convergence of the state errors, enabling secure communication performance. As the sliding surface $s = e_1 + e_2 + e_3$ converges to zero, it directly follows that the tracking errors e_1, e_2, and e_3 asymptotically converge to zero as $t \to \infty$. This guarantees

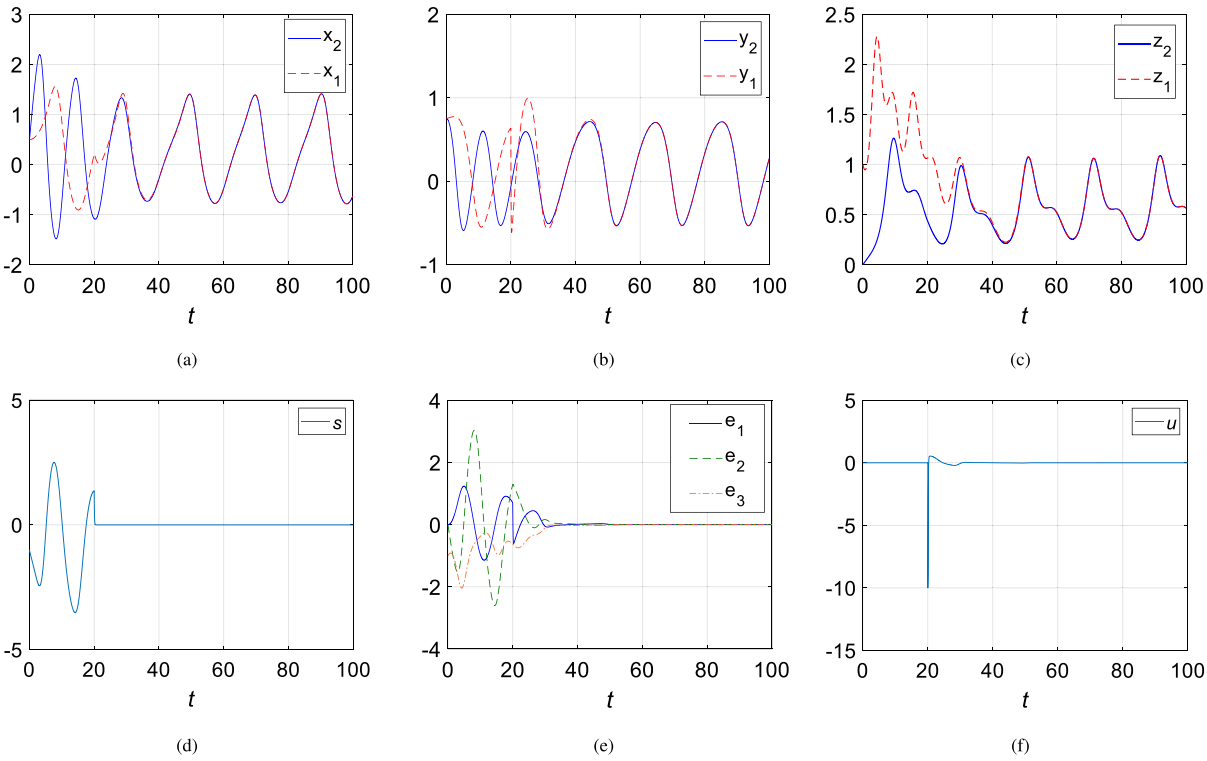

Fig. 13. SMC-based synchronization (a) x(t), (b) y(t), (c) z(t), (d) s(t), (e) e_1(t), e_2(t), e_3(t), (f) u(t).

that complete synchronization between the master and slave systems is analytically ensured, independent of the simulation results.

To verify the tracking dynamics of the SMC, simulation studies are conducted using MATLAB/Simulink program. In the simulation, the system parameter values $a = 0.193$, $b = 0.2$, $c = 0.2$, and $d = 0.2$ are chosen for both the master and slave systems. However, the initial values are set to $x_1(0) = 0.5$, $y_1(0) = 0.75$, $z_1(0) = 1$, $x_2(0) = 0.5$, $y_2(0) = 0.75$, and $z_2(0) = 0$. Fig. 13 illustrates the diagrams for comparisons of x_1, x_2, y_1, y_2, and z_1, z_2 as well as e_1, e_2 and e_3 respectively. Note that synchronization starts after $t = 20$ s in this simulation. To mitigate the chattering effect caused by the discontinuous nature of the signum function, a saturation function is employed in both the simulation and practical implementation.

The disturbance bound is identified as $\delta = 0.5$ based on the worst-case amplitude of the injected noise and perturbations. Therefore, the switching gain is set to $k = 20$ to ensure that the Lyapunov condition $\dot{V} < 0$ is satisfied for all $|\Delta(t)| \leq \delta$. To evaluate the robustness of the proposed SMC scheme under external disturbances, additional perturbations are introduced into the system. A bounded external disturbance with a maximum amplitude of -0.5 is applied to the system starting from $t = 20$ s and remains active until $t = 40$ s. These perturbations are consistent with the practical dynamic range of the system states, which oscillate between approximately -1.5 and $+2$. Fig. 14 shows the simulation results under the external disturbance. The simulation results indicate that the SMC, activated at $t = 10$ s, successfully achieves synchronization in a short time. Furthermore, when the disturbance is introduced, the control input s and synchronization errors quickly converge to values close to zero, demonstrating the effectiveness and robustness of the proposed control strategy.

In addition, the effect of parameter uncertainty on the system dynamics is also investigated. Specifically, deviations in the bifurcation parameter a are introduced to observe the impact on chaotic behavior. The results revealed that small changes in a caused the master system to exit the chaotic regime, which in turn disrupted the chaotic flow required for encryption. This led to a failure in the proper encryption of the information signal. Since the generation of chaotic flows critically depends on precise initial conditions and parameter settings, parameter uncertainty is not considered in this study. The focus is placed on maintaining the chaotic behavior necessary for secure communication, while robustness against external disturbances is demonstrated through the performance of the designed SMC controller.

During the implementation of secure communication, various microcontrollers like Arduino or STM32 Nucleo are utilized [62]. The streamlined programming of these microcontrollers presents a significant advantage in secure communication. Conversely, Raspberry Pi serves as a powerful lightweight computer that can be programmed effortlessly using the MATLAB Support Package for Raspberry Pi Hardware. Hence, in this study, the Raspberry Pi 4B computer is employed for real-time secure communication of the ECG signal. MATLAB/Simulink 2022a, featuring an external mode operation for real-time functionality, is utilized for programming the desired secure communication. The experimental setup is shown in Fig. 15. An ECG signal from the MIT-BIH arrhythmia dataset is employed [63]. The programming is executed and data is read from the dataset using Raspberry Pi. Subsequently, the primary side transmits this data to the secondary side using Universal Asynchronous Receiver/Transmitter (UART). The transmitted data is comprised of the modulated information signal (ECG signal) by the state variable z_1 of the master chaotic system. Following the completion of data transfer, synchronization errors are calculated, and the SMC is simultaneously activated on the secondary side. Ultimately, upon successful synchronization, the information signal is extracted from the received data by subtracting the state variable z_2.

All information signals, transmitted signals, and retrieved signals are measured using an oscilloscope. However, due to the absence of analog outputs on the Raspberry Pi computer, users are required to utilize a signal converter. Thus, as depicted in Fig. 15, even though data transmission occurs via serial communication, pulse width modulation to analog signal converter is employed to display these signals on the oscilloscope. Moreover, in order to overcome constraints imposed experimental working conditions, a scaling factor should be used. This provides better chaotic masking within the appropriate range of 0 to

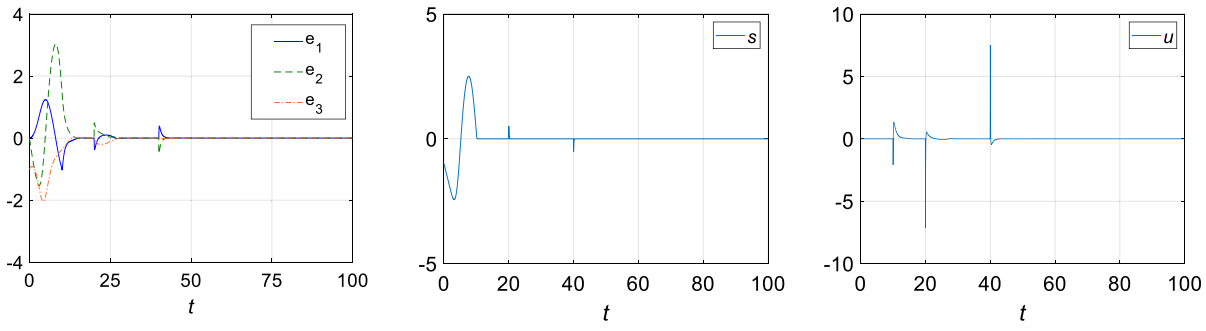

Fig. 14. SMC-based synchronization under external disturbance (a) e_1(t), e_2(t), e_3(t), (b) s(t), (c) u(t).

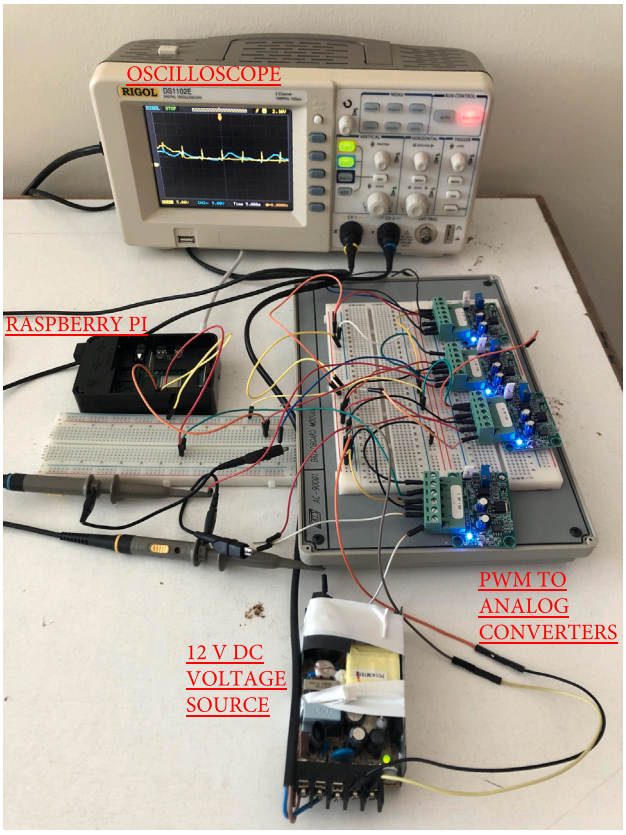

Fig. 15. Experimental set-up of secure communication system.

10 V. Hereby, an oscilloscope can be used to measure the encrypted and decrypted signals.

During the experimental studies, initial values are set as follows: $x_1(0) = 0.5$, $y_1(0) = 0.75$, $z_1(0) = 1$, $x_2(0) = 0.5$, $y_2(0) = 0.75$, and $z_2(0) = 0$, similar to the simulation studies. Both systems are initialized simultaneously, operating independently of the SMC, and generate chaotic signals. These signals originate from the novel five-term chaotic system with two squared nonlinearities, as elaborated in Section 2 along with the system parameters a, b, c and d which have the values 0.193, 0.2, 0.2, and 0.2, respectively. At $t = 10$ s, the synchronization process initiates by activating the controller. The parameter of the SMC given in Eq. (20) is defined as $k = 20$ while $\delta = 0.5$ through simulation studies. Real-time observation of the transmitted ECG signal, the modulated signal, and the retrieved signal is shown in Fig. 16, obtained through oscilloscope probes. Before $t = 10$ s, the master and slave chaotic systems demonstrate different chaotic flows as a result of their initial conditions. After SMC is activated at $t = 10$ s, SMC synchronizes the chaotics systems within 4 s. The real-time observation of scaled signals is illustrated in Fig. 16 with offsets. The original data is also scaled to improve the visibility of the ECG signal on the oscilloscope. The ECG signal is illustrated in Fig. 16a. Fig. 16b shows the masked and transmitted signal by UART channel. The retrieved signal on the secondary side is observed as given in Fig. 16c. It is observed from practical results that the secure communication of ECG signals is effectively achieved.

Compared to existing literature in chaotic masking of ECG signal, the proposed system demonstrates a favorable balance between complexity, synchronization speed, and real-time applicability. For instance, Liao et al. have employed a Lü chaotic system with a PD controller optimized via particle swarm optimization (PSO), requiring full state transmission for synchronization [1]. Although their method achieved synchronization within approximately 0.46 s, it introduced additional communication overhead and was sensitive to controller tuning. On the other hand, Le et al. have proposed an advanced scheme based on a Takagi–Sugeno fuzzy model of the Chen chaotic system, integrating adaptive SMC with a disturbance observer [64]. Their system exhibited very fast convergence (settling time ≈ 15 ms) and high disturbance rejection capability but at the cost of increased computational complexity and a discrete-time fuzzy framework. In contrast, our method utilizes a novel five-term chaotic system with squared nonlinearities and a conventional SMC approach, achieving robust synchronization within 4 s. Without requiring fuzzy modeling or full state sharing, it provides a simpler yet effective solution for secure ECG transmission in embedded real-time healthcare systems.

4.2. Secure communication of biomedical images

This section explores the encryption of a 240 × 360 biomedical image using a Random Number Generator (RNG) designed while utilizing the system (1). To accomplish this encryption, the required keys, comprising 0 s and 1 s, are regenerated from the random numbers generated by the system (1) when $a = 1$, $b = 1$, $c = 5.2$, $d = 1$ and the initial conditions $x(0)$, $y(0)$, $z(0) = 0.5, 0.75, 1$. For a decimal image to be used in encryption, a transformation process needs to take place. Bitwise logical operators cannot be applied to the decimal image. Hence, converting the image into binary format is the initial step in the image encryption process. Subsequently, the generated binary numbers and converted data are subjected to XOR operation. The main reason of using XOR is its significant advantages for scenarios facing memory constraints in encryption [65]. Furthermore, the successful passing of various tests by the used random numbers is one of the factors that increase the security in image encryption. Fig. 17 demonstrates the schema of designed biomedical image encryption–decryption scheme.

In this system, the SMC-based chaotic synchronization method outlined in Section 4.1 is employed. The reference trajectories given in Eq. (5) considered as the master chaotic system and Eq. (6) is

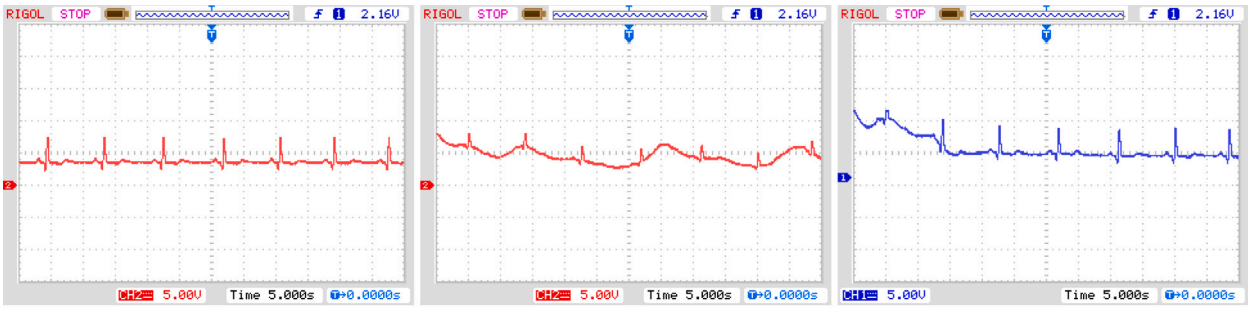

Fig. 16. The real-time secure communication of ECG signal: (a) Original ECG signal, (b) modulated signal transmitter by primary side, (c) the retrieved signal on the secondary side.

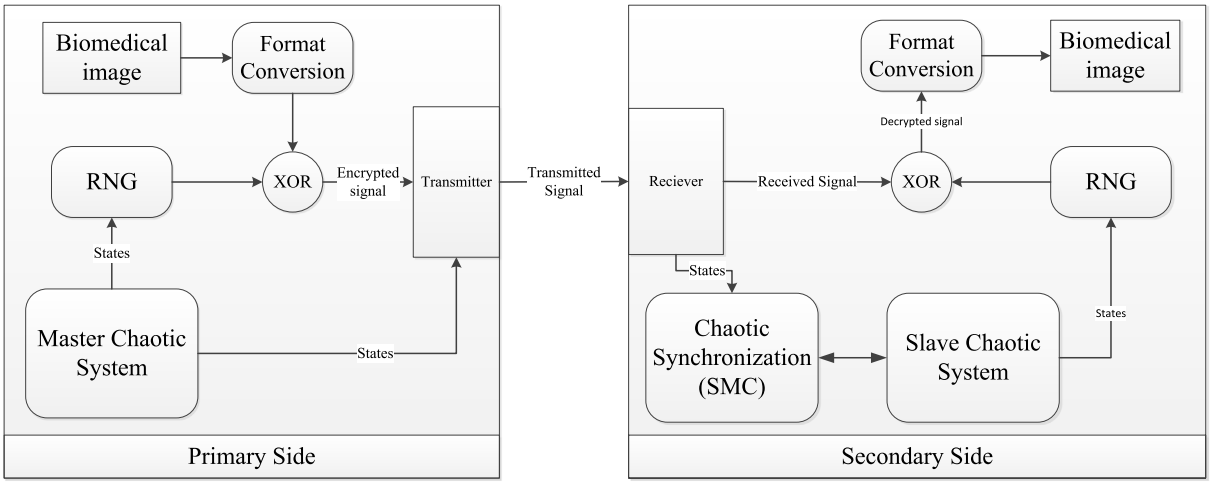

Fig. 17. Block diagram of secure communication of biomedical data.

considered as the slave chaotic system. As depicted in Fig. 17, the generation of random numbers constitutes a critical aspect of the image encryption algorithm. Acquiring 32-bit floating-point numbers using Eq. (5) in accordance with IEEE 754-2019 standard [66] is the initial stage of RNG design. Therefore, fourth-order Runge–Kutta algorithm is executed with a sampling interval of 0.0001. However, for statistical tests, a larger quantity of generated numbers is required. The NIST-800-22 provides a comprehensive suite of 16 statistical tests, each designed to assess different aspects of randomness in random or pseudorandom number sequences. Random numbers which pass these tests successfully can be deemed reliable for particular applications. In this study, the 32-bit floating-point numbers from the outputs of system (5) are utilized, employing $x \oplus z$ to improve randomness. Due to their increased complexity, the rightmost bits are employed to ensure success. The RNG design process is deemed successful upon obtaining favorable outcomes. NIST-800-22 test results of the designed RNG are reported in Table 2, which displays that each test demonstrates successful outcomes. All P-values in Table 2 exceed 0.001, suggesting that the generated random numbers are suitable for encryption applications.

Although the P-values show some variation, ranging from 0.12 to 0.91, this fluctuation is expected because each NIST test is designed to evaluate different statistical properties (e.g., uniformity, entropy, periodicity, or linear complexity). Such variation is a typical feature of pseudorandom sequences derived from deterministic chaotic systems and does not indicate weakness in randomness quality. Since all P-values remain above the minimum threshold, and the pass rate is 100%, the overall randomness of the proposed system is statistically reliable and appropriate for encryption. Note that the same RNG design is implemented on the secondary side for use in the decryption process, utilizing the outputs of system (6).

Table 2
NIST-800-22 tests results of the novel chaotic system-based RNG design.

Statistical test	P-value	Proportion	Result
Frequency	0.350485	10/10	Pass
Block frequency	0.534146	10/10	Pass
Cumulative sums	0.122325	10/10	Pass
Runs	0.350485	10/10	Pass
Long runs of ones	0.911413	10/10	Pass
Rank	0.531660	10/10	Pass
FFT	0.534146	10/10	Pass
Non-overlapping templates	0.739918	9/10	Pass
Overlapping templates	0.350485	10/10	Pass
Universal	0.278905	10/10	Pass
Approximate entropy	0.350485	10/10	Pass
Random excursions	0.129152	10/10	Pass
Random excursions Variant	0.177465	10/10	Pass
Linear complexity	0.904769	9/10	Pass
Serial-1	0.739918	10/10	Pass
Serial-2	0.122325	10/10	Pass
Pass rate	16/16	16/16	16/16

To decrypt the encrypted data, it is necessary to reconstruct the keys used in encryption. This requires successful synchronization between the systems (5) and (6). Without this synchronization, decrypting the data becomes impractical. Once the synchronization process is successfully achieved, the original medical image can be obtained by performing the XOR operation between the generated random numbers on the secondary side and the received data. Meanwhile, the decrypted image is obtained in binary format. Finally, by converting the binary data to a decimal image, the biomedical image is obtained. The pseudo

code of entire secure communication algorithm for biomedical images is given in Algorithm 1.

Algorithm 1 Pseudo code of Secure Communication of Biomedical Images

START
%Primary Side
Input the 240x360 biomedical image
Convert biomedical image to 86400x1 decimal data
Convert decimal 86400x1 data to 86400x8 binary format
Generate the decimal random number using master chaotic system
Convert the decimal random numbers to 86400x8 binary format
for $i = 1$ to 86400 **do**
  for $j = 1$ to 8 **do**
    encrypteddata(i, j) ← img$(i, j)\oplus$ primaryrandomnumbers(i, j)
  end for
end for
Transmit encrypted data and states of the master chaotic system to the receiver
%Secondary Side
Receive encrypted data and chaotic states
Synchronize slave chaotic system using received states
Generate the decimal random number using slave chaotic system
Convert the decimal random numbers to 86400x8 binary format
for $i = 1$ to 86400 **do**
  for $j = 1$ to 8 **do**
    decrypteddata(i, j) ← encrypteddata$(i, j)\oplus$ secondaryrandomnumbers(i, j)
  end for
end for
Convert the 86400x8 binary decrypted data to size 240x360 image
EXIT

In this study, image encryption is conducted using two distinct biomedical images: a biomedical iris image and a biomedical X-ray chest image. The iris image and X-ray image used for analyzing the designed biometric encryption scheme are sourced from the CASIA-IrisV1 database by the Chinese Academy of Sciences Institute of Automation (CASIA) [67] and the tuberculosis chest X-ray database [68], respectively. Both images are sized at 240 × 360 pixels. The decimal values within these matrices are converted into 86 400 × 8 matrix containing binary numbers, which is then encrypted using generated binary numbers. The outcomes for the encryption–decryption of biomedical iris and chest X-ray images are illustrated in Figs. 18 and 19, respectively. Histogram distributions of the original, encrypted and decrypted images are given in Figs. 18a, b, c and 19a, b, c, respectively. The successful encryption of these images can be ensured by the uniform histogram values. The figures presented in Figs. 18b and 19b illustrate the images undergoing encryption via the XOR process. Figs. 18c and 19c demonstrate no alteration between the original and decrypted images.

The quality of the decrypted images is evaluated using two objective image quality metrics, Mean Squared Error (MSE) and Structural Similarity Index (SSIM), calculated between the original and decrypted images. For both the biomedical iris and chest X-ray images, the MSE is 0 and the SSIM is 1.0000, indicating perfect reconstruction with no pixel-wise or structural distortion. These results confirm that the proposed encryption–decryption algorithm achieves lossless recovery and fully preserves the original image content. To assess the effectiveness of the encryption phase in obfuscating visual information, MSE and SSIM values are also calculated between the original and encrypted images. The biomedical iris image yields an MSE of 7191.10 and an SSIM of 0.0097, while the chest X-ray image exhibits an even higher MSE of 11 984.73 and an SSIM of 0.0065. These significant degradations in visual similarity confirm that the encrypted images are

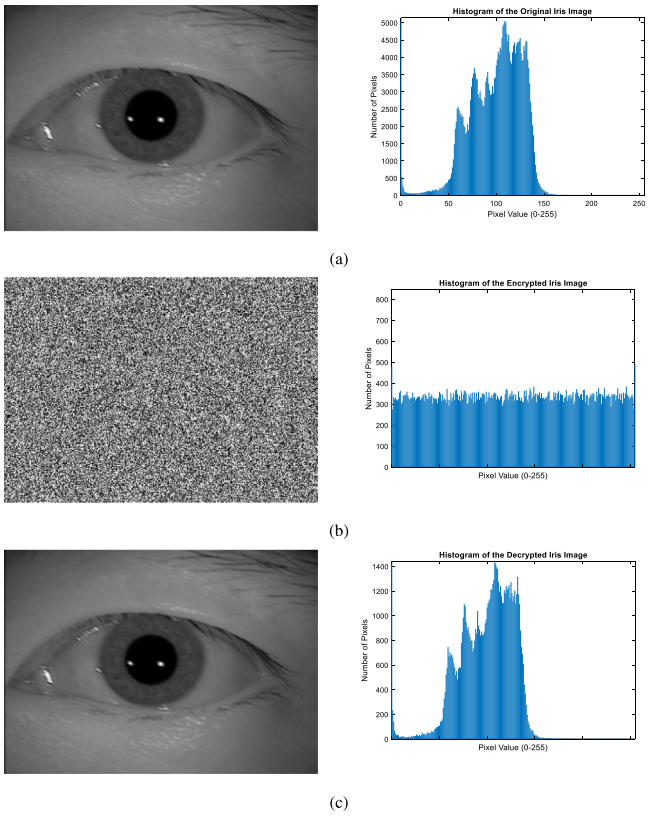

Fig. 18. Encryption of biomedical iris image: (a) Original iris image and its histogram, (b) encrypted iris image and its histogram, (c) decrypted iris image and its histogram.

substantially different from the originals, reinforcing the strength of the encryption scheme. The combined evidence demonstrates that the proposed method ensures both high security and perfect fidelity, which is essential for sensitive applications such as medical imaging systems.

4.2.1. Security analysis of encryption scheme

To assess the performance of the biometric image encryption scheme using the novel system, various analyses are applied in addition to histogram analysis. These include statistical and attack analyses such as key space, correlation, key sensitivity, and entropy analysis. The results are compared with the current studies in the literature.

Key space analysis. Key space analysis is an essential aspect of evaluating the security of an image encryption algorithm. The key space is the total number of possible keys available for use in the encryption process. A large key space ensures that the encryption algorithm remains resistant to brute-force attacks, where an attacker attempts every possible key until the correct one is found. In the context of image encryption, a robust algorithm should have a sufficiently large key space to guarantee security against such exhaustive search attacks [55]. The key space should be large enough to make brute-force attacks computationally infeasible. Generally, a key space of at least 2^{100} considered secure. In this encryption process, the key parameters are $x(0)$, $y(0)$, $z(0)$, a, b, c, d. With the IEEE floating point standard [66], the key size becomes $10^{(15 \times 7)}$, which is approximately close to 2^{299}. It is shown in Table 3 that the obtained key space value meets the recommended value of 2^{100} for encryption algorithms as compared to existing papers in the literature.

Computational resource and time-space analysis. In addition to key space analysis, practical implementation aspects such as computational resource requirements and time-space efficiency were also thoroughly

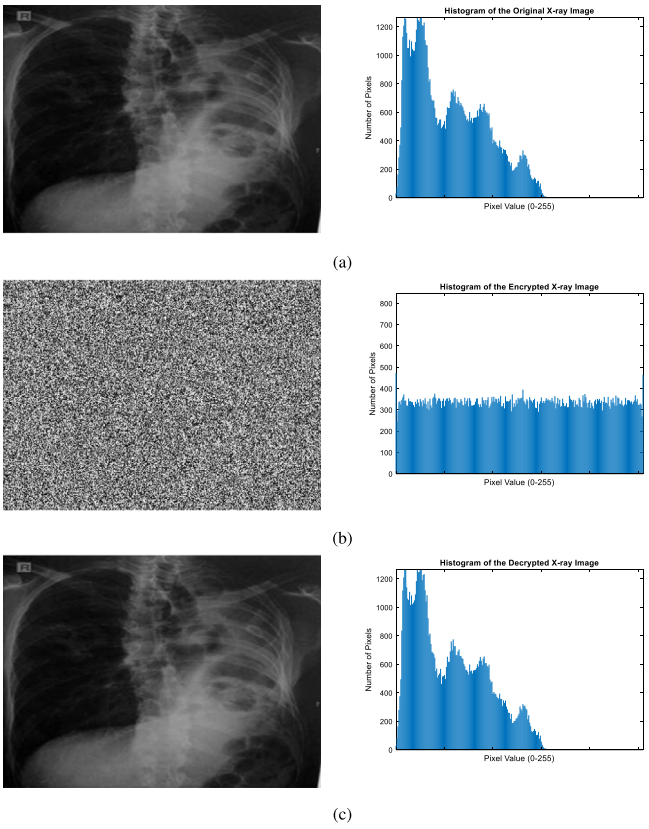

Fig. 19. Encryption of biomedical chest X-ray image: (a) Original chest X-ray image and its histogram, (b) encrypted chest X-ray image and its histogram, (c) decrypted chest X-ray image and its histogram.

Table 3
Comparison of key space value with existing papers.

Method	Key space
Proposed	2^{299}
Ramar et al. [51]	2^{298}
Emin et al. [56]	2^{349}
Gokyildirim et al. [54]	2^{352}

evaluated. To emulate a resource-constrained environment, the proposed encryption and decryption algorithms were implemented on a Raspberry Pi 4B platform. Experimental results demonstrated that the system is both lightweight and efficient, rendering it highly suitable for embedded and real-time biomedical applications.

For instance, encryption of a 256 × 256 grayscale Chest X-ray image is completed in approximately 0.0004 s, while decryption took only 0.0002 s. Similarly, for a Biomedical Iris image, encryption and decryption times are measured at 0.0003 and 0.0001 s, respectively. Throughout the entire process, the encryption memory usage remained at 0.12 MB and the decryption phase used only 0.02 MB, resulting in a total memory footprint of just 0.14 MB.

These results indicate that the algorithm maintains high computational efficiency while delivering a strong level of security, ensured by the large key space ($\approx 2^{299}$). This balance between lightweight implementation and robust cryptographic performance makes the proposed method highly promising for deployment in low-power medical devices and other embedded systems.

Correlation analysis. The correlation coefficient analysis serves as a critical metric in the field of image encryption to evaluate the effectiveness of the encryption algorithm. An effective image encryption technique must ensure that the correlation between adjacent pixels in the encrypted image is significantly reduced compared to the original image. This reduction in correlation is essential to prevent any statistical patterns from being discernible, thus enhancing the security and robustness of the encryption method. The correlation coefficient, denoted as r quantifies the degree of correlation between adjacent pixels in horizontal, vertical, and diagonal directions. It is calculated using the following formula [69]:

$$r_{xy} = \frac{\mathrm{Cov(x,y)}}{\sqrt{\mathrm{Var}(x).\mathrm{Var}(y)}} \tag{21}$$

where r_{xy} is the correlation coefficient between two pixels x and y. $\mathrm{Cov}(x, y)$ stands for the covariance of x and y, defined as

$$\mathrm{Cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}). \tag{22}$$

$\mathrm{Var}(x)$ and $\mathrm{Var}(y)$ are the variances of x and y, respectively, defined as:

$$\begin{aligned} \mathrm{Var}(x) &= \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2, \\ \mathrm{Var}(y) &= \frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2. \end{aligned} \tag{23}$$

In Fig. 17, $\bar{x}$ and $\bar{y}$ are the mean values of x and y, respectively. N is the total number of pixel pairs considered in the analysis. In an unencrypted image, these correlation coefficients are typically close to 1, indicating strong correlation. Conversely, an encrypted image should exhibit correlation coefficients near 0, signifying that the pixels are no longer linearly related, thus indicating successful encryption.

In this study, a comprehensive correlation coefficient analysis on encrypted images is conducted to assess the effectiveness of the presented encryption algorithm. The correlation coefficients in Table 4 show that the values for the encrypted images are close to zero. Additionally, Figs. 20 and 21 illustrate the homogeneous distribution in the encrypted images. Thus, the presented algorithm ensures robust encryption and is compatible with the existing papers given in Table 4.

Table 4
Correlation coefficient values of original and encrypted biomedical images.

Test image	Direction	Original image	Encrypted image
Biomedical iris image	H	0.9927	−0.0051
	V	0.9836	−0.0079
	D	0.9851	0.0027
Biomedical chest X-ray image	H	0.9937	−0.0105
	V	0.9923	−0.0127
	D	0.9865	0.0061
Ramar et al. [51]	H	0.9792	−0.0041
	V	0.9815	−0.0053
	D	0.9591	−0.0002
Emin et al. [56]	H	0.9709	0.0237
	V	0.9644	0.0135
	D	0.9380	0.0232
Gokyildirim et al. [54]	H	0.9664	0.0010
	V	0.9772	0.0009
	D	0.9584	0.0020

Key sensitivity analysis. Key sensitivity analysis measures how a small change in the encryption key affects the encrypted image. An effective encryption algorithm should exhibit high key sensitivity, meaning that even a slight alteration in the key should result in a significantly different encrypted image. This property ensures that unauthorized parties cannot decrypt the image without the exact encryption key, thereby enhancing the algorithm's resistance to brute-force attacks.

When encrypting an image, even a minor modification to the encryption key should produce a drastically different encrypted image. This can be quantified using metrics such as the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity

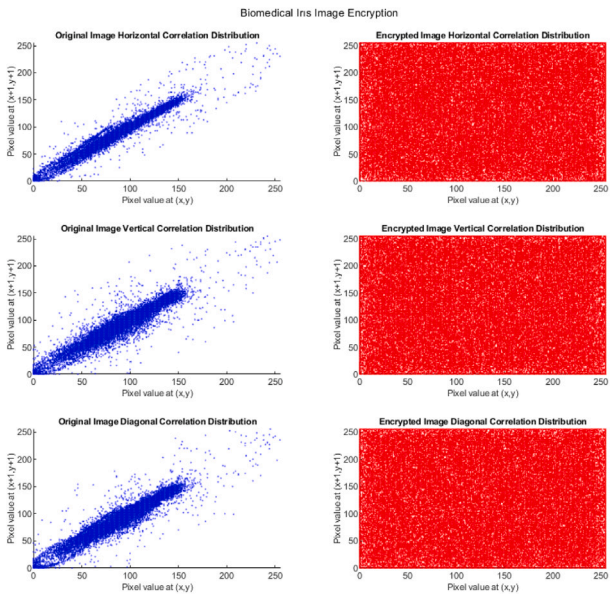

Fig. 20. Correlation distributions of original and encrypted biomedical iris image.

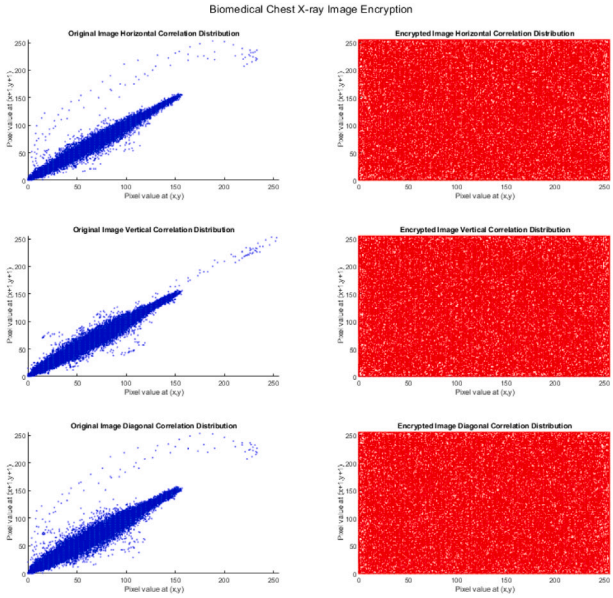

Fig. 21. Correlation distributions of original and encrypted chest X-ray image.

(UACI). NPCR measures the percentage of different pixel values between two encrypted images generated with slightly different keys, while UACI measures the average intensity difference between these images. These metrics are calculated, separately, as follows [55]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100, \tag{24}$$

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{L-1} \times 100 \tag{25}$$

where $D(i,j)$ is defined as:

$$D(i,j) = \begin{cases} 0 & \text{if } C_1(i,j) = C_2(i,j) \\ 1 & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \tag{26}$$

$C_1(i,j)$ and $C_2(i,j)$ represent the pixel values at position (i,j) in the two encrypted images. M and N are dimensions of the images. L is the grayscale level of the image. In image encoding applications, the NPCR value should generally exceed 90%, and the UACI value should exceed 33% [54]. It is seen from the key sensitivity results given in Table 5 that the NPCR and UACI values in the encrypted images meets the expected criteria.

Table 5
NPCR and UACI values.

Test image	NPCR (%)	UACI (%)
Biomedical iris image	99.58	33.59
Biomedical chest X-ray image	99.56	33.63
Ramar et al. [51]	99.58	33.53
Emin et al. [56]	99.61	33.31
Gokyildirim et al. [54]	99.60	33.50

Information entropy analysis. Information entropy is a fundamental concept in cryptography used to evaluate the randomness and unpredictability of encrypted data. It denoted as H and measures the uncertainty associated with a random variable. For an image, it quantifies the unpredictability of pixel values. The entropy H of a source S with N possible states (in this case, pixel values) is given by [54]:

$$H(S) = \sum_{i=1}^{N} P(s_i)\log_2 P(s_i) \tag{27}$$

where $P(s_i)$ is the probability of occurrence of the ith state (pixel value). For a grayscale image, each pixel can take a value from 0 to 255, resulting in 256 possible states. In an ideally encrypted image, each pixel value should have an equal probability of occurring, which would result in the highest possible entropy of 8 bits. This indicates that every pixel value is equally likely, and the image appears as random noise to any observer without the decryption key. High entropy values (close to 8) indicate that the encrypted image has a high level of randomness, making it resistant to various cryptographic attacks. The obtained high entropy values for the iris image and chest X-ray images are 7.9558 and 7.9601, respectively. These values prove that the designed algorithm is resistant to statistical inferences.

Comparison with related works. Compared to existing image encryption studies in the literature, the proposed scheme achieves competitive performance in terms of key space, correlation reduction, key sensitivity, and entropy. As presented in Table 3, the key space of the proposed system reaches 2^{299}, which is comparable with or exceeds values reported by Ramar et al. [51] and Emin et al. [56]. In Table 4, correlation coefficients for the encrypted images are near zero, outperforming some existing methods, especially in diagonal directions. The high NPCR and UACI values shown in Table 5 confirm the scheme's sensitivity to small key variations, which is crucial for resisting differential attacks. Additionally, the entropy values obtained (>7.95) approach the theoretical maximum of 8, indicating strong randomness in encrypted data. Unlike some previous methods that rely on hybrid or high-complexity transformations, the proposed scheme provides a lightweight yet robust encryption mechanism by leveraging the chaotic behavior of a five-term system with squared nonlinearities and binary masking. This balance between computational simplicity and cryptographic strength makes it suitable for resource-constrained biomedical systems.

5. Limitations of the study

Although the proposed five-term chaotic system demonstrates favorable characteristics, such as simplicity, uniqueness due to its two squared nonlinear terms, and successful application in biomedical data encryption, this study has several limitations that warrant consideration:

- The synchronization mechanism is based on a nonlinear sliding mode control (SMC) approach. While this method ensures synchronization even in the presence of uncertainties and disturbances, the use

of a single-state control to reduce computational complexity leads to an increased settling time. In many practical and engineering systems, including biological, physical, electrical, chemical, and communication systems, various uncertainties and time delays are unavoidable [70]. These factors can significantly alter the dynamic behavior and increase the complexity of system models [71], which the current approach does not fully account for.

• The encryption algorithm employs a basic XOR operation. The cryptographic performance of the proposed chaotic system should be evaluated against modern standards (e.g., AES, RSA) in terms of speed, robustness, and resource consumption.

• The study focuses exclusively on an integer-order system. The potential benefits of employing fractional-order dynamics, such as increased complexity and enhanced security [72], remain unexplored.

• Real-time implementation of the encryption algorithm has been validated only in a wired environment. Its applicability in wireless communication systems is yet to be investigated.

• Only 2D grayscale biomedical images were used in this study. The encryption of more complex data formats, such as 3D DICOM images or RGB biomedical images, has not been addressed.

These limitations highlight opportunities for future research aimed at enhancing the generalizability, efficiency, and resilience of the proposed system in broader secure communication contexts.

6. Conclusion

In this paper, encryption applications based on a newly discovered simple chaotic system are implemented for biomedical data, where secure communication is crucial due to patient privacy concerns. To achieve this, dynamic analyses are first conducted to examine the chaotic behavior of the novel system. This system consists of only five terms, including two squared nonlinear terms, which makes it structurally unique. Simulation results demonstrate that under appropriate operating conditions, ECG signals and biomedical images can be effectively encrypted and decrypted. The effectiveness of the designed image encryption scheme is validated through histogram analysis, key space analysis, correlation analysis, key sensitivity analysis, and information entropy analysis. Additionally, the electronic circuit implementation using standard components confirms the system's feasibility for hardware-based applications. However, the synchronization process, essential for secure communication, relies on a nonlinear SMC mechanism using a single-state control signal. While this reduces computational complexity, it comes at the cost of longer settling times. This trade-off represents a significant limitation of the current implementation.

Future work directions include several promising areas: (i) investigating the fractional-order version of the system to reveal more complex dynamic behaviors and potentially enhance encryption security; (ii) benchmarking the proposed chaotic encryption algorithm against modern cryptographic standards such as AES or RSA in terms of speed, robustness, and efficiency; (iii) extending the system to wireless communication environments to assess real-time performance under different transmission conditions; (iv) exploring the encryption of more complex biomedical data formats, including 3D DICOM and RGB images, to generalize the method across diverse clinical imaging modalities. (v) examining the impact of communication and control time delays on system synchronization and encryption reliability, which would enhance the applicability of the proposed method in practical networked environments.

In conclusion, the proposed five-term chaotic system with two squared nonlinear terms presents a promising foundation for secure biomedical data communication and offers a rich landscape for future research and development.

CRediT authorship contribution statement

Abdullah Gokyildirim: Writing – original draft, Validation, Software, Methodology, Investigation, Conceptualization. **Uğur Erkin Kocamaz:** Writing – review & editing, Supervision, Software, Methodology, Conceptualization. **Haris Calgan:** Writing – original draft, Software, Methodology, Funding acquisition, Conceptualization.

Funding

This study is funded by the Scientific Research Projects Unit of Balikesir University (Grant no. BAP 2024/022).

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

[1] T.L. Liao, H.C. Chen, C.Y. Peng, Y.Y. Hou, Chaos-based secure communications in biomedical information application, Electron. 10 (3) (2021) 359.
[2] E.N. Lorenz, Deterministic nonperiodic flow, J. Atmos. Sci. 20 (2) (1963) 130–141.
[3] O.E. Rössler, An equation for continuous chaos, Phys. Lett. A 57 (5) (1976) 397–398.
[4] T. Matsumoto, A chaotic attractor from Chua's circuit, IEEE Trans. Circuits Syst. 31 (12) (1984) 1055–1058.
[5] G. Chen, T. Ueta, Yet another chaotic attractor, Int. J. Bifurc. Chaos 9 (07) (1999) 1465–1466.
[6] W.G. Hoover, Canonical dynamics: Equilibrium phase-space distributions, Phys. Rev. A 31 (3) (1985) 1695.
[7] S. Nosé, A unified formulation of the constant temperature molecular dynamics methods, J. Chem. Phys. 81 (1) (1984) 511–519.
[8] W.G. Hoover, Remark on some simple chaotic flows, Phys. Rev. E 51 (1) (1995) 759.
[9] J.C. Sprott, Some simple chaotic flows, Phys. Rev. E 50 (2) (1994) R647.
[10] J. Sprott, Simplest dissipative chaotic flow, Phys. Lett. A 228 (4–5) (1997) 271–274.
[11] J. Sprott, Some simple chaotic jerk functions, Am. J. Phys. 65 (6) (1997) 537–543.
[12] J.C. Sprott, Simple chaotic systems and circuits, Am. J. Phys. 68 (8) (2000) 758–763.
[13] G. Ablay, Chaos in PID controlled nonlinear systems, J. Electr. Eng. Technol. 10 (4) (2015) 1843–1850.
[14] P.H. Chang, D. Kim, Introduction and synchronization of a five-term chaotic system with an absolute-value term, Nonlinear Dynam. 73 (2013) 311–323.
[15] A. Gokyildirim, U.E. Kocamaz, Y. Uyaroglu, H. Calgan, A novel five-term 3D chaotic system with cubic nonlinearity and its microcontroller-based secure communication implementation, AEU-Int. J. Electron. Commun. 160 (2023) 154497.
[16] G.Q. Huang, Analysis and circuit simulation of new five terms chaotic system, Appl. Mech. Mater. 275 (2013) 825–829.
[17] C. Li, J.C. Sprott, W. Thio, H. Zhu, A unique signum switch for chaos and hyperchaos, in: Proc. 7th International Conference on Physics and Control, PhysCon 2015, Istanbul, Turkey, 2015.
[18] J. Maaita, C.K. Volos, I. Kyprianidis, I. Stouboulos, The dynamics of a cubic nonlinear system with no equilibrium point, J. Nonlinear Dyn. 2015 (1) (2015) 257923.
[19] B. Munmuangsaen, B. Srisuchinwong, J.C. Sprott, Generalization of the simplest autonomous chaotic system, Phys. Lett. A 375 (12) (2011) 1445–1450.
[20] B. Munmuangsaen, J.C. Sprott, W.J.C. Thio, A. Buscarino, L. Fortuna, A simple chaotic flow with a continuously adjustable attractor dimension, Int. J. Bifurc. Chaos 25 (12) (2015) 1530036.
[21] B. Munmuangsaen, B. Srisuchinwong, A new five-term simple chaotic attractor, Phys. Lett. A 373 (44) (2009) 4038–4043.
[22] J. Sprott, Ergodicity of one-dimensional oscillators with a signum thermostat, Comput. Methods Sci. Technol. 24 (2018) 169–176.

[23] J. Sprott, Variants of the Nosé–Hoover oscillator, Eur. Phys. J. Spec. Top. 229 (6) (2020) 963–971.
[24] C. Toncharoen, B. Srisuchinwong, A heart-sound-like chaotic attractor and its synchronization, in: 2009 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, Vol. 1, IEEE, 2009, pp. 407–410.
[25] S. Vaidyanathan, S. Pakiriswamy, A 3-D novel conservative chaotic system and its generalized projective synchronization via adaptive control, J. Eng. Sci. Technol. Rev. 8 (2) (2015).
[26] V. Varshney, S. Sabarathinam, K. Thamilmaran, M. Shrimali, A. Prasad, Existence and control of hidden oscillations in a memristive autonomous duffing oscillator, in: Nonlinear Dynamical Systems with Self-Excited and Hidden Attractors, 2018, pp. 327–344.
[27] F. Yu, C.H. Wang, Y. Hu, J.W. Yin, Projective synchronization of a five-term hyperbolic-type chaotic system with fully uncertain parameters, Acta Phys. Sin. 61 (6) (2012) 060505.
[28] F. Yu, C. Wang, Q. Wan, Y. Hu, Complete switched modified function projective synchronization of a five-term chaotic system with uncertain parameters and disturbances, Pramana 80 (2013) 223–235.
[29] T. Gotthans, J. Petržela, New class of chaotic systems with circular equilibrium, Nonlinear Dynam. 81 (2015) 1143–1149.
[30] S. Jafari, J. Sprott, V.T. Pham, C. Volos, C. Li, Simple chaotic 3D flows with surfaces of equilibria, Nonlinear Dynam. 86 (2016) 1349–1358.
[31] C. Li, J. Sprott, Chaotic flows with a single nonquadratic term, Phys. Lett. A 378 (3) (2014) 178–183.
[32] M. Molaie, S. Jafari, J.C. Sprott, S.M.R.H. Golpayegani, Simple chaotic flows with one stable equilibrium, Int. J. Bifurc. Chaos 23 (11) (2013) 1350188.
[33] V.T. Pham, S. Vaidyanathan, C.K. Volos, A.T. Azar, T.M. Hoang, V. Van Yem, A three-dimensional no-equilibrium chaotic system: Analysis, synchronization and its fractional order form, in: Fractional Order Control and Synchronization of Chaotic Systems, 2017, pp. 449–470.
[34] V.T. Pham, S. Jafari, C. Volos, T. Kapitaniak, A gallery of chaotic systems with an infinite number of equilibrium points, Chaos Solitons Fractals 93 (2016) 58–63.
[35] S. Vaidyanathan, A novel 3-D jerk chaotic system with three quadratic nonlinearities and its adaptive control, Arch. Contol. Sci. 26 (1) (2016) 19–47.
[36] S. Vaidyanathan, A seven-term novel 3-D jerk chaotic system with two quadratic nonlinearities and its adaptive backstepping control, in: Advances in Chaos Theory and Intelligent Control, Springer, 2016, pp. 581–607.
[37] S. Vaidyanathan, A.T. Azar, Adaptive control and synchronization of Halvorsen circulant chaotic systems, in: Advances in Chaos Theory and Intelligent Control, Springer, 2016, pp. 225–247.
[38] D. Veeman, A. Alanezi, H. Natiq, S. Jafari, A.A. Abd El-Latif, A chaotic quadratic oscillator with only squared terms: Multistability, impulsive control, and circuit design, Symmetry 14 (2) (2022) 259.
[39] Z. Wei, J. Sprott, H. Chen, Elementary quadratic chaotic flows with a single non-hyperbolic equilibrium, Phys. Lett. A 379 (37) (2015) 2184–2187.
[40] R. Parvaz, Y.K. Yengejeh, Y. Behroo, A new 4D chaos system with an encryption algorithm for color and grayscale images, Int. J. Bifurc. Chaos 32 (14) (2022) 2250214.
[41] L. Xiong, F. Yang, X. An, X. Zhang, Hyperchaotic system with application to image encryption, Int. J. Bifurc. Chaos 32 (13) (2022) 2250191.
[42] S. Zhou, Y. Qiu, G. Qi, Y. Zhang, A new conservative chaotic system and its application in image encryption, Chaos Solitons Fractals 175 (2023) 113909.
[43] G. Zhao, H. Zhao, Y. Zhang, X. An, A new memristive system with extreme multistability and hidden chaotic attractors and with application to image encryption, Int. J. Bifurc. Chaos 34 (01) (2024) 2450010.
[44] W. Lv, J. Chen, Q. Li, X. Xu, C. Fu, An efficient medical image encryption scheme utilizing nonuniform cellular automaton, Int. J. Bifurc. Chaos 33 (10) (2023) 2350119.
[45] M.Z. Yildiz, O. Boyraz, E. Guleryuz, A. Akgul, I. Hussain, A novel encryption method for dorsal hand vein images on a microcomputer, IEEE Access 7 (2019) 60850–60867.
[46] S.Y.D. Nezhad, N. Safdarian, S.A.H. Zadeh, New method for fingerprint images encryption using DNA sequence and chaotic tent map, Optik 224 (2020) 165661.
[47] S. Bhattacharjee, M. Gupta, B. Chatterjee, Time efficient image encryption-decryption for visible and Covid-19 X-ray images using modified chaos-based logistic map, Appl. Biochem. Biotechnol. 195 (4) (2023) 2395–2413.
[48] A.A.K. Javan, M. Jafari, A. Shoeibi, A. Zare, M. Khodatars, N. Ghassemi, R. Alizadehsani, J.M. Gorriz, Medical images encryption based on adaptive-robust multi-mode synchronization of Chen hyper-chaotic systems, Sens. 21 (11) (2021) 3925.
[49] N. Tsafack, S. Sankar, B. Abd-El-Atty, J. Kengne, K. Jithin, A. Belazi, I. Mehmood, A.K. Bashir, O.Y. Song, A.A. Abd El-Latif, A new chaotic map with dynamic analysis and encryption application in internet of health things, IEEE Access 8 (2020) 137731–137744.
[50] H. Lin, C. Wang, L. Cui, Y. Sun, X. Zhang, W. Yao, Hyperchaotic memristive ring neural network and application in medical image encryption, Nonlinear Dynam. 110 (1) (2022) 841–855.
[51] R. Ramar, S. Vaidyanathan, A. Akgul, B. Emin, A new chaotic jerk system with cubic and hyperbolic sine nonlinearities and its application to random number generation and biomedical image encryption, Sci. Iran. (2024) http://dx.doi.org/10.24200/sci.2024.63254.8303.
[52] X. Chai, G. Shang, L. Cao, D. Jiang, G. Long, Z. Gan, A novel multi-scroll hyperchaotic system applicable for visually secure image cryptosystem using block compressive sensing, Nonlinear Dynam. 112 (2) (2024) 1439–1468.
[53] D. Ding, S. Chen, H. Zhang, Z. Yang, F. Jin, X. Liu, Firing pattern transition of fractional-order memristor-coupled Hindmarsh–Rose neurons model and its medical image encryption for region of interest, Nonlinear Dynam. (2024) 1–26.
[54] A. Gokyildirim, S. Çiçek, H. Calgan, A. Akgul, Fractional-order sprott K chaotic system and its application to biometric iris image encryption, Comput. Biol. Med. 179 (2024) 108864.
[55] R. Subramanian, S. Çiçek, A. Akgul, G. Adam, A. Karthikeyan, K. Rajagopal, Dynamical analysis of a quadratic megastable chaotic oscillator and its application in biometric fingerprint image encryption, Complex. 2024 (1) (2024) 2005801.
[56] B. Emin, A. Akgul, F. Horasan, A. Gokyildirim, H. Calgan, C. Volos, Secure encryption of biomedical images based on Arneodo chaotic system with the lowest fractional-order value, Electron. 13 (11) (2024) 2122.
[57] M. Cencini, F. Cecconi, A. Vulpiani, Chaos: From Simple Models To Complex Systems, Vol. 17, World Scientific, 2010.
[58] A. Gokyildirim, Circuit realization of the fractional-order sprott K chaotic system with standard components, Fractal Fract. 7 (6) (2023) 470.
[59] A.A. Kekha Javan, A. Shoeibi, A. Zare, N. Hosseini Izadi, M. Jafari, R. Alizadehsani, P. Moridian, A. Mosavi, U.R. Acharya, S. Nahavandi, Design of adaptive-robust controller for multi-state synchronization of chaotic systems with unknown and time-varying delays and its application in secure communication, Sens. 21 (1) (2021) 254.
[60] A.A.K. Javan, A. Zare, Images encryption based on robust multi-mode finite time synchronization of fractional-order hyper-chaotic Rikitake systems, Multimedia Tools Appl. 83 (1) (2024) 1103–1123.
[61] A. Gokyildirim, H. Calgan, M. Demirtas, Fractional-order sliding mode control of a 4D memristive chaotic system, J. Vib. Control 30 (7–8) (2024) 1604–1620.
[62] A. Gokyildirim, A. Akgul, H. Calgan, M. Demirtas, Parametric fractional-order analysis of Arneodo chaotic system and microcontroller-based secure communication implementation, AEU-Int. J. Electron. Commun. 175 (2024) 155080.
[63] G.B. Moody, R.G. Mark, The impact of the MIT-BIH arrhythmia database, IEEE Eng. Med. Biol. Mag. 20 (3) (2001) 45–50.
[64] M.C. Le, Q.D. Nguyen, S.-C. Huang, et al., Electrocardiogram signal secure transmission via a wireless communication protocol of chaotic systems based on adaptive sliding mode control and disturbance observer, IEEE Access 11 (2023) 145373–145385.
[65] H. Calgan, Incommensurate fractional-order analysis of a chaotic system based on interaction between dark matter and dark energy with engineering applications, Phys. A 635 (2024) 129490.
[66] IEEE standard for floating-point arithmetic, in: IEEE Std 754-2019 (Revision of IEEE 754-2008), IEEE, New York, 2019, http://dx.doi.org/10.1109/IEEESTD.2019.8766229, URL https://standards.ieee.org/standard/754-2019.html.
[67] Casia-irisv1, 2023, http://biometrics.idealtest.org/.
[68] T. Rahman, A. Khandakar, M.A. Kadir, K.R. Islam, K.F. Islam, R. Mazhar, T. Hamid, M.T. Islam, S. Kashem, Z.B. Mahbub, et al., Reliable tuberculosis detection using chest X-ray with deep learning, segmentation and visualization, IEEE Access 8 (2020) 191586–191601.
[69] B. Emin, Z. Musayev, Chaos-based image encryption in embedded systems using Lorenz–Rossler system, Chaos Theory Appl. 5 (3) (2023) 153–159.
[70] A. Zare, S.Z. Mirrezapour, M. Hallaji, A. Shoeibi, M. Jafari, N. Ghassemi, R. Alizadehsani, A. Mosavi, Robust adaptive synchronization of a class of uncertain chaotic systems with unknown time-delay, Appl. Sci. 10 (24) (2020) 8875.
[71] M. Rasouli, A. Zare, M. Hallaji, R. Alizadehsani, The synchronization of a class of time-delayed chaotic systems using sliding mode control based on a fractional-order nonlinear PID sliding surface and its application in secure communication, Axioms 11 (12) (2022) 738.
[72] S. Iqbal, J. Wang, A novel fractional-order 3-D chaotic system and its application to secure communication based on chaos synchronization, Phys. Scr. 100 (2) (2025) 025243.