



Biomedical Image Encryption with a Novel Memristive Chua Oscillator Embedded in a Microcontroller

Gabin Jeatsa Kitio^{1,2} · Alain Djomo Fanda³ · Idriss Rochinel Kemlenack Feulefack^{1,2} · Justin Roger Mboupda Pone²  · Romanic Kengne¹ · Alain Tiedeu^{3,4}

Received: 18 August 2022 / Accepted: 10 February 2023 / Published online: 3 March 2023
© The Author(s) under exclusive licence to Sociedade Brasileira de Física 2023

Abstract

In this paper, a chaos-based encryption/decryption scheme using a novel memristive Chua oscillator to protect medical images is presented. The novel Chua oscillator is constructed by using the active voltage memristor in the nonlinear branch of the Chua oscillator. The chaotic dynamics behaviors are investigated using 1-D, 2-D bifurcation diagrams, time traces, basin of attractions, and largest Lyapunov exponent plot. The study reveals that the novel memristive Chua oscillator exhibits versatile transitions to chaos with interesting dynamics like multistability, spiking, and bursting oscillations just to name a few. These remarkable features are experimentally confirmed by a laboratory microcontroller-based setup. Thereafter, a chaos-based cryptography algorithm designed for biomedical images is built using pseudorandom number generated from the oscillator. The robustness and security tests undergone by the algorithm yielded high sensitivity on the encryption keys and resisted noise contamination as well as data loss. These results are encouraging and prove that the chaos-based cryptosystem built with the memristive Chua circuit-generated pseudorandom number is suitable for securing images in a healthcare system.

Keywords Memristive Chua oscillator · Microcontroller implementation · Biomedical image encryption · Diffusion · Permutation · Security analyses

1 Introduction

Since chaotic circuits were discovered, considerable interests have arisen in developing and analyzing various circuits that exhibit chaos due to their importance in many fields of sciences and engineering [1, 2]. The idea of using chaotic oscillators to encrypt information dates back to Matthews

in 1989 [3]. Since then, many contributions in the literature have exploited the close relationship between chaos properties and cryptography [4–7] to propose chaos-based cryptosystems. In this regard, some famous chaotic circuits and systems have been used to supply pseudorandom numbers needed in the encryption algorithm build-up. Some of them are Lorentz system [8], Van der Pol oscillator [9, 10], jerk systems [11], and Chua circuit [12] just to name a few.

This work describes a simple novel Chua-based memristor oscillator, with digital circuit implementation, which exhibits some multistable chaotic attractors and its chaos-based encryption. It is well known that many simple circuits with different memristors have been developed because of the remarkable dynamics induced in these systems by the nonlinear resistor [13–16]. But the simple Chua circuit [17] development to build chaos-based encryption systems in the literature is not documented enough. One aim of this paper is to bridge this gap.

On the other hand, due to the growth of computer networks, storage devices, and imaging tools, the images, video, and texts have been extensively used in various fields [18]. As images are exchanged over public networks, they are

✉ Justin Roger Mboupda Pone
mboupdapone00@gmail.com

¹ Research Unit of Condensed Matter, Electronics and Signal Processing (RU-MACETS), Department of Physics, Faculty of Science, University of Dschang, P. O. Box 67, Dschang, Cameroon

² Electrical Engineering Department of IUT-FV of Bandjoun, Research Unit of Automation and Applied Computer (RU-AIA), University of Dschang, P.O. Box 134, Bandjoun, Cameroon

³ Ingénierie Mathématique Et Systèmes d'Information, National Advanced School of Engineering, University of Yaoundé I, P.O. Box 8390, Yaoundé, Cameroon

⁴ Signal, Image and Systems Laboratory, University of Yaoundé I, P.O. Box 8390, Yaoundé, Cameroon

exposed to various security threats such as eavesdropping, illegal modification, and duplication, just to name a few. In many domains such as diplomacy, military, and telemedicine, confidentiality challenges cannot be overemphasized.

In the e-healthcare domain, the quality of services has been improved due to the artificial intelligence-based biomedical systems [19]. With the advent of intelligent methods, biomedical data processing becomes easier and less error prone. Moreover, remote healthcare is also possible using the IoT infrastructure. Among the data used in e-health, the biomedical images are transmitted over public networks which are exposed to hackers. However, the protection of biomedical images over the network is always considered a challenge because they are exposed to hacker. The biomedical images are generally sensitive to external disturbances and small manipulation in the data may cause huge differences in the ultimate result. Wrong diagnosis can be life threatening in some scenarios or can be severe in almost every instance. Therefore, biomedical data security is one of the major challenges and hiding them is necessary during storage, manipulation, or transmission [20]. Moreover, securing medical images requires adequate techniques for protecting patient privacy. In the context of the COVID-19 pandemic, operational updates on COVID-19 of the World Health Organization stated that globally, there have been 661,545,258 confirmed cases of COVID-19, including 6,700,519 deaths [21]. It is worth noting to mention that, among medical imaging techniques, chest X-ray and computed tomography have been considered as a powerful tool to detect COVID-19 infections, especially in emerging cases of pregnant women and children [22]. This is why we suggest in this contribution an embedded Chua memristive oscillator that could be part of an IoT system for biomedical encryption.

Encryption is a technique to hide information and is intended to ensure confidentiality, integrity, and non-repudiation. Image encryption has received much attention in the last few years [18, 23, 24]. This is more needed for biomedical images, since they are part of human information [25, 26]. A review on medical image encryption has been proposed in refs [27–29]. The encryption schemes are based on substitution and permutation of pixels' images. The first step consists in changing the pixel value, while the second step consists in changing the position of the pixel image.

Over the years, a number of techniques have been used for cryptosystem development [30–33]: transform domain [34], evolutionary algorithm [35], deoxyribonucleic acid sequence [36], and others [37, 38]. Among the algorithms in the literature, chaos-based ones have experienced considerable growth, as chaos properties such as unpredictability, ergodicity, randomness, and extreme sensitivity to initial conditions and control parameters make them a good candidate for carrying out the confusion and diffusion operations

required to build robust cryptosystems [39]. Chaos theory has proved to be an excellent alternative to provide a fast, simple, and reliable image encryption scheme that has a high-enough degree of security [40]. For these reasons, chaos-based image encryption technology is very promising for real-time secure image and video communications in military, industrial, and commercial applications.

Some interesting references performed image encryption using 1D to 4D chaotic to hyperchaotic systems.

Neural networks for the encryption of medical images emerged [41–43], with some remarkable characteristics:

- (i) Chaotic brain-like dynamics of the coupled neural network which shows that the designed cryptosystem has several advantages in the key space, information entropy, and key sensitivity [44].
- (ii) Hyperchaotic memristive ring neural network and application in medical image encryption [45] which shows a medical image encryption scheme constructed based on the MRNN from a perspective of practical engineering application. Performance evaluations demonstrate that the proposed medical image cryptosystem has several advantages in terms of key space, information entropy, and key sensitivity, compared with cryptosystems based on other chaotic systems.
- (iii) Complex dynamics, hardware implementation, and image encryption application of multiscroll memristive Hopfield neural network (MHNN) with a novel local active memristor [46] perform well in image encryption applications for the significant complexity of multiscroll.

Memristive circuits from chaotic signals have a very complex topology, which is very similar to those of high-dimensional chaotic systems [11, 47–53].

Among them, a genetic algorithm was used [54, 55] while others used DNA schemes [47, 56, 57]. The latter consisted in some biological and algebra operations on DNA sequences. Refs [58, 59] combined DNA and bit level permutation to strengthen the encryption algorithm.

Other refs [60–62] mixed many chaotic systems to improve randomness of the chaos. They are used in the aim to increase chaoticity of the seldom map and therefore reinforce randomness of the key produced. Another good-standing contribution performed frequency domain coding approach [63]. This technique provides good security and robustness against noise and distortion attacks. The key space obtained is large enough standard to standard, and the NPCR/UACI are close to ideal values. But the computation times are not shown in this contribution. While the author of references contributes with genetic algorithm [54, 55] resulting in good cryptography

metrics, the proposed contribution is robust with huge key space, short time computation, and could have better metrics with good chaotic maps. Some papers with many citations like ref. [64] built a new image encryption scheme, in which shuffling the positions and changing the gray values of image pixels are combined to confuse the relationship between the cipher image and the plain image. The experimental results demonstrate that the key space is large enough to resist the brute-force attack, and the distribution of gray values of the encrypted image has a random-like behavior.

Ref. [65] suggested a new, fast, simple, and robust chaos-based cryptosystem structure. The cryptosystem uses a diffusion layer followed by a bit-permutation layer, instead of byte-permutation, to shuffle the positions of the image pixels. The security analysis and the obtained simulation results show that the proposed cryptosystem is resistant to various types of attacks and it is efficient for hardware and software implementation.

Ref. [20] proposed an encryption scheme for the medical image encryption based on a combination of scrambling and confusion. The novelty of this paper is that they make use of chaos in both image diffusion and confusion parts. It is worth noting that the resistance of the scheme against differential and linear cryptanalysis is at least as of S-AES.

Ref. [26] shows a medical image encryption method based on a hybrid model of the modified genetic algorithm (MGA) and coupled map lattices. Experimental results and computer simulations both indicate that the proposed method that includes a hybrid algorithm not only performs excellent encryption but also is able to resist various typical attacks.

Despite this cloud of cryptosystems designed with great attention described above, we focused in this work on a medical image encryption algorithm built with Chua's new memristive chaotic oscillator that uses an encryption technique built around a permutation-diffusion architecture. First, the raw images are subdivided into small blocks (4×4). These blocks are mixed using a rotation of the image pixels. This is followed by a permutation of the pixels, making chaotic iterations along the rows and then along the columns of the mixed image using the pseudorandom number sequences of the Chua memristive chaotic oscillator. The computation of the substituted position index leads to a scrambled image. The diffusion simply consists in performing a XOR operation between the previously obtained image and a stream of pseudorandom numbers in order to obtain the encrypted image at the output of the cryptosystem. The main strengths of the new memristive Chua oscillator and the developed cryptosystem can be summarized in the following points:

- (a) The new memristive Chua oscillator displays some complex behaviors:
 - (a) Period doubling and intermittency route to chaos
 - (b) The coexisting of multiple attractors in the chaotic regime
 - (c) Bursting and spiking oscillations for a set of its parameters.
- (b) The novel Chua oscillator is used as a pseudorandom number generator for cryptography application with interesting properties:
 - (a) Simplicity of cryptosystem and fast encryption using new, simple, and famous chaotic map
 - (b) The encryption key used contained image parameters resulting in the improvement of the security of our system
 - (c) Robustness against attacks and therefore reinforced security, thanks to the trick of transformation of secret key to get the initial conditions and control parameters
 - (d) Enhanced sensitivity to key change and key space enlargement, thanks to the used technique.
- (c) The microcontroller embedded of the oscillator experiment shows consistent results with numerical ones; therefore, it is a candidate for a critical component of the healthcare system.

The rest of this paper is as follows. The novel memristive Chua oscillator is described and mathematically modeled in Sect. 2, and some basic properties are shown in Sect. 3. It is then followed by the numerical analyses in Sect. 4 where some dynamics are investigated. The microcontroller verification is performed in Sect. 5 thereafter, and the image encryption is the object of Sect. 6. The paper ends with some concluding remarks.

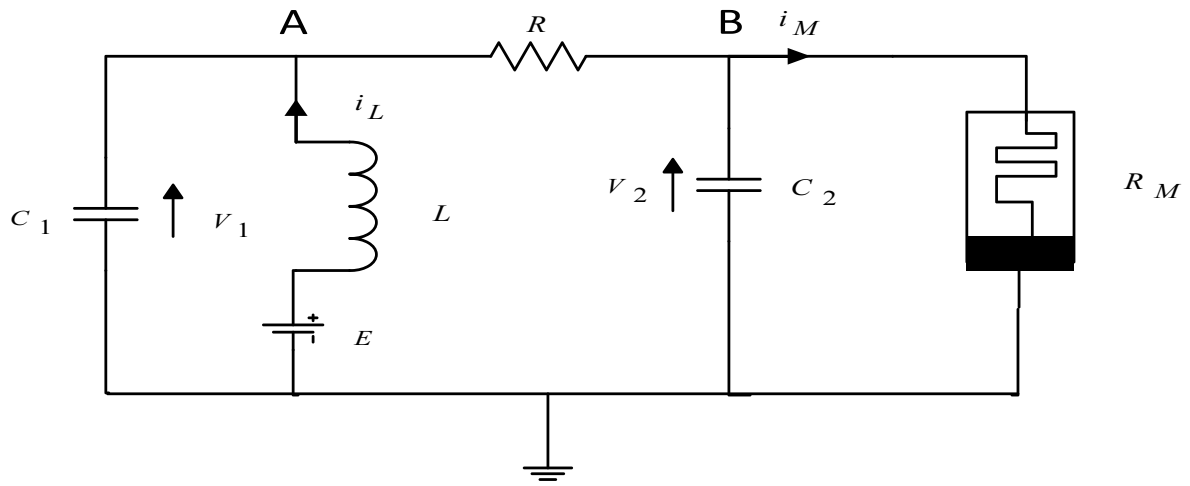
2 Circuit Description and Mathematical Modeling of the Novel Memristive Chua Oscillator

The novel memristive Chua oscillator is derived from the circuit presented in ref. [66] where we replace the tunnel diode 1N3858 by the voltage-controlled memristor proposed by ref. [67]. The resulting novel circuit is described in the next section.

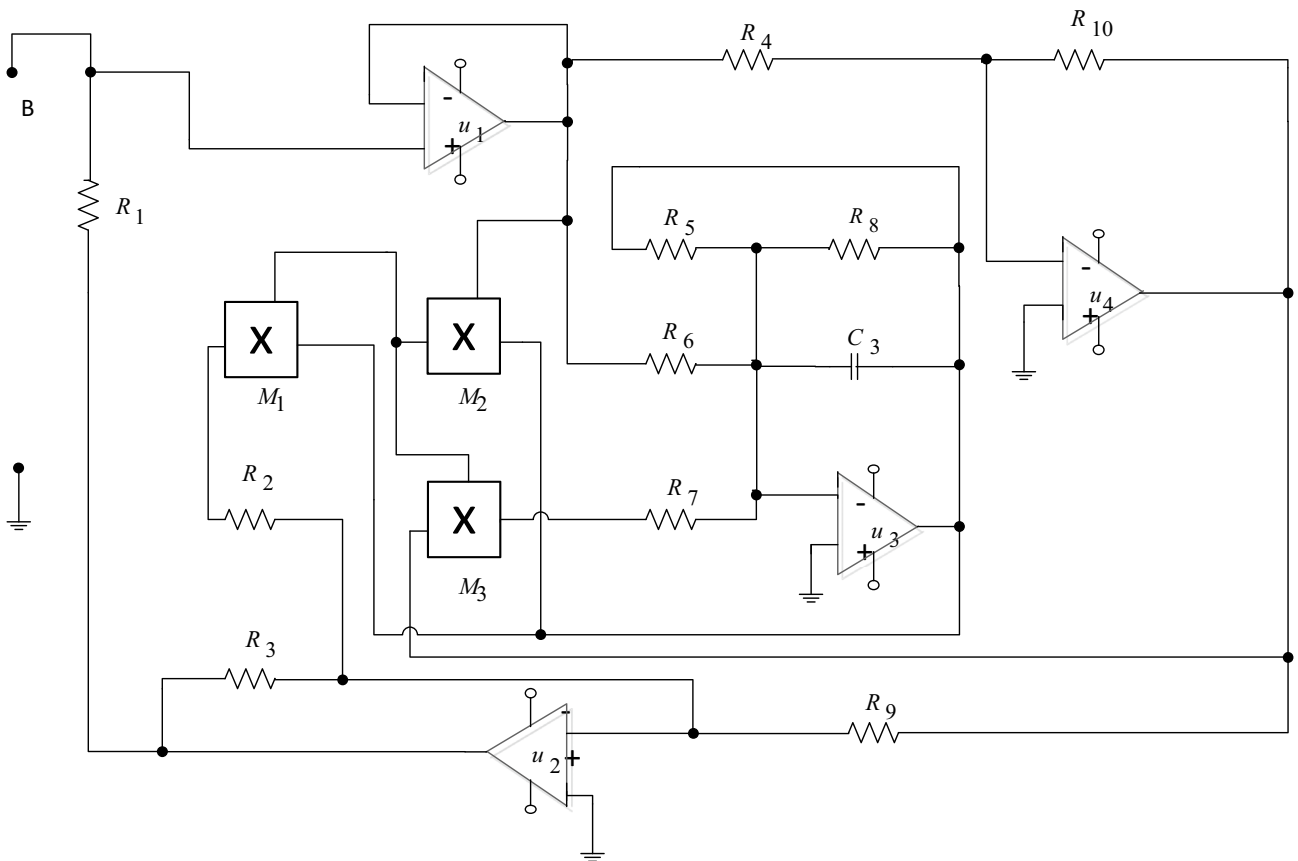
2.1 Circuit Description

The new memristor-based oscillator circuit introduced above is shown in Fig. 1.

The circuit of Fig. 1 consists of three nodes and five branches. On the first node, A connected three branches:



(a)



(b)

Fig. 1 **a** Electronic diagram of the novel memristor oscillator and **b** equivalent electronic diagram of the voltage-controlled memristor R_M replacing the tunnel diode proposed in ref. [66]

first one with capacitor C_1 , the second branch with inductor in series with a DC voltage source, and third branch with resistor R . The second node B connects three branches of capacitor C_2 , the memristor R_M and the common resistor R connecting the two nodes. The memristor part (b) is a voltage-controlled memristor proposed by Xu et al. [67]. It is connected between node B and the ground. The memristor is noted R_M in this manuscript. Its internal components are displayed in Fig. 1b, and it is composed of four operational amplifier TL084-A type (u_1, u_2, u_3, u_4), three analog multiplier AD633/JN (M_1, M_2, M_3), 10 resistors, and one capacitor C_3 . The summary of these electronics' components with their values are listed in the Table 1.

In order to study this novel circuit, it is recommended to find its mathematical model that facilitates the following studies.

2.2 Mathematical Model of the Novel Memristive Chua

This model is obtained by first defining state variables of the circuits related to the energy storage elements. For these purposes, the voltage across capacitors C_1, C_2 , and C_3 are defined as V_{C1}, V_{C2} , and V_{C3} , respectively. The current flowing across the inductor is named I_L . By applying the Kirchhoff's voltage laws (KVL) to the R_M [66], the following equations are obtained from Fig. 1b:

Table 1 Electronic component parameter of the circuits in Fig. 1

Parameters	Signification	Values
Main circuit (a)		
C_1, C_2	Capacitor	10 nF
R	Resistor	2.5 kΩ
L	Inductor	0.66 mH
E	DC voltage source	0.001 V
Memristor circuit R_M (b)		
R_1	Resistor	1 kΩ
C_3	Capacitor	10 nF
R_2	Resistor	300 kΩ
R_3	Resistor	20 kΩ
R_4, R_9	Resistor	10 kΩ
R_5	Resistor	466 kΩ
R_6	Resistor	80 kΩ
R_7	Resistor	625 kΩ
R_8	Resistor	100 MΩ
R_{10}	Resistor	466 kΩ
L	Inductor	5.66 mH
M_1 to M_3	Analog multiplier chip	AD633JN multiplier of gain 1
u_1 to u_4	Operational amplifier chip	TL-084A low-power operational amplifier

$$\begin{cases} i_m = \frac{1}{R_1} \left(1 - \frac{R_3}{R_9} + \frac{R_3}{R_2} V_{C3}^2 \right) V_{A0} \\ \frac{dV_{C3}}{dt} = -\frac{1}{R_6 C_1} V_{A0} - \frac{1}{R_5 C_1} V_{A0} + \frac{1}{R_7 C_1} V_{A0}^2 V_{C3} \end{cases} \quad (1)$$

By posing $a = R_3/R_2, b = (1/R_1)(R_3/R_9 - 1), c = 1/R_6 C_1, d = 1/R_5 C_1, e = 1/R_7 C_1$, the set of Eq. (1) becomes

$$\begin{cases} \dot{i}_m = (ay^2 - b)V_M \\ \dot{y} = -cV_M - dy + eV_M^2 y \end{cases} \quad (2)$$

where a, b, c, d , and e represent the intrinsic parameters of the memristor. To verify the properties of the memory effect of the memristor, a sinusoidal voltage is to be applied to the input of the memristor $v(t) = V_{max} \sin(2\pi ft)$, with V_{max} as its signal amplitude and f as its frequency [67]. Table 2 display the numeric values of the memristor parameters used.

For the given specific parameters, the memristor behavior should be bistable, mining that the orbits from two flanks of the initial critical point move along different pinched hysteresis loops in the state space. With a periodic voltage signal $v(t)$ applied at the input of the circuit $V_{max} = 0.6$ V, we varied the frequency to $f = 45$ Hz, 50 Hz, and 75 Hz and we plot in Fig. 2a the current flowing inside R_M versus the stimulus voltage. On the other figure, Fig. 2b, we maintain the frequency constant to $f = 45$ Hz and varied the maximum voltage of the stimulus source to $V_{max} = 0.6$ V, $V_{max} = 0.7$ V, and $V_{max} = 0.8$ V and we plot the curves of current $i(A)$ flowing inside R_M versus the stimulus voltage $v(V)$ in Fig. 2b.

In the light of the Fig. 2a, we observed that when V_{max} is constant, the area of the hysteresis loop decreases with the increase of the frequency, while for constant frequency, this area increases with the value of the V_{max} , see Fig. 2b. Thus, the characteristic fingerprints are confirmed by applying periodic signals with zero mean, showing the hysteresis behavior of the memristor. We also note the symmetric pinched loop.

By applying the KVL to the circuit diagram of Fig. 1a, the following set of equations is obtained and presented in Sect. 2.

$$\begin{cases} \frac{C_1 dV_1}{dt} = i_L - \frac{V_1 - V_2}{R} \\ \frac{C_2 dV_2}{dt} = \frac{V_1 - V_2}{R} - \left(\frac{R_3}{R_1 R_2} y^2 - \frac{1}{R_1} \left(\frac{R_3}{R_9} - 1 \right) \right) V_2 \\ \frac{L di_L}{dt} = E - V_1 \\ \frac{dy}{dt} = -\frac{1}{R_6 C_3} V_2 - \frac{1}{R_5 C_3} y + \frac{1}{R_7 C_3} V_2^2 y \end{cases} \quad (3)$$

Table 2 Parameters of the memristor R_M

Parameters	a	b	c	d	e
Values	0.006	0.00006	1250	625	1250

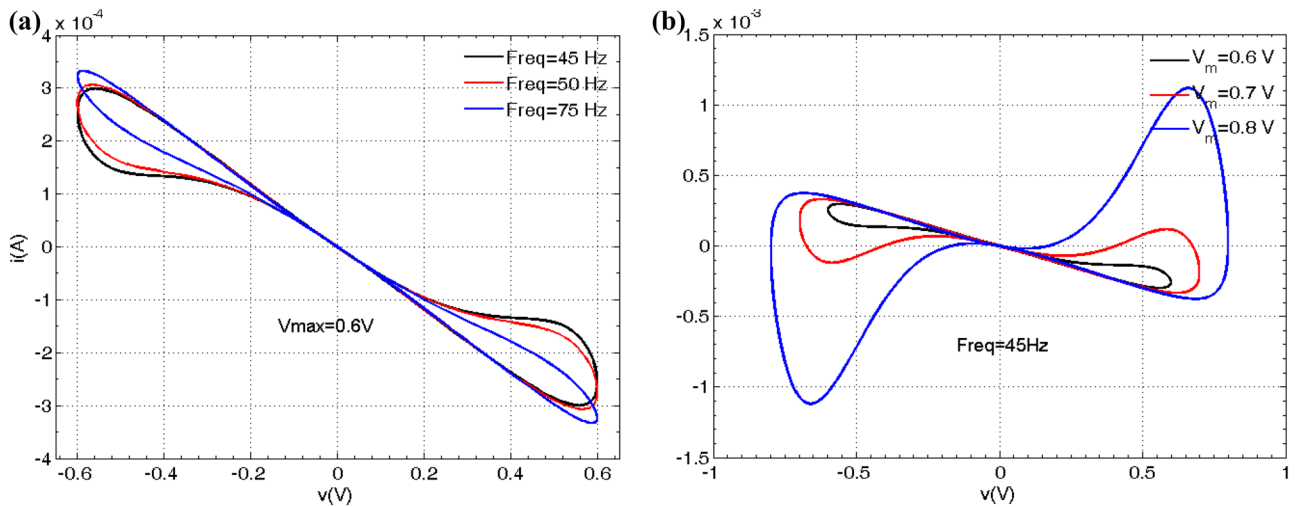


Fig. 2 The current–voltage characteristic of the memristor emulator: **a** $V_{\max}=0.6$ V, we varied the frequency to $f=45$ Hz, $f=50$ Hz, and $f=75$ Hz; **b** we maintain the frequency constant to $f=45$ Hz and

varied the maximum voltage of the stimulus source to $V_{\max}=0.6$ V, $V_{\max}=0.7$ V, and $V_{\max}=0.8$ V. The initial state of the internal voltage is 0.149 V

By introducing the following dimensionless variables and normalized circuit parameters,

$$\begin{cases} x = \frac{V_1}{1000V}; z = \frac{V_2}{1000V}; \tilde{z} = \frac{i_i}{100A}; \tau = RC_1 t; \alpha = R; \alpha_1 = \frac{RC_1}{R_6 C_3} \\ \alpha_2 = \frac{RC_1}{R_5 C_3}; \alpha_3 = \frac{RC_1}{R_7 C_3}; \alpha_4 = \frac{C_1}{C_2}; \alpha_5 = \frac{RC_1}{L} \\ \beta_1 = \frac{R_3 R}{R_1 R_2}; \beta_2 = \frac{R}{R_1} \left(\frac{R_3}{R_9} - 1 \right); u = E; a = 1000 \end{cases} \quad (4)$$

The state Eq. (3) can be written in dimensionless form as

$$\begin{cases} \dot{x} = \alpha w - x + z \\ \dot{y} = -\alpha_1 z - \alpha_2 y + \alpha_3 z^2 y \\ \dot{z} = \alpha_4 (x - z - (\beta_1 y^2 - \beta_2) z) \\ \dot{w} = \alpha_5 (u - ax) \end{cases} \quad (5)$$

3 Basic Properties of the Novel Memristive Chua Oscillator

In this section, some analytical properties of the system (5) are presented such as symmetry, dissipativity, and equilibrium point study.

3.1 Symmetry

Based on the symmetry of the above memristor, it is crucial to check if the novel circuit conserved this property. Indeed, it gives information about the number of

solutions of the system. Thus, for an asymmetric system, the solutions are unique. On the other hand, for symmetrical systems, the solutions are in pairs; otherwise, they are symmetric around the origin of the state space. Starting from the equation system of the proposed model, we see that it is not variant to the transformation $(x_1, x_2, x_3, x_4) \Rightarrow (-x_1, -x_2, -x_3, -x_4)$. Therefore, our system is not symmetric, and therefore, we do not expect symmetric solutions of Eq. (5).

3.2 Dissipation and Existence of Attractor

The study of the dissipation and the existence of attractors are the first research step of the dynamical behavior of a dynamic system [68, 69]; it aims to verifying the existence of solutions in state space. Note that if the dissipation is greater than zero, then there is no solution in state space, and if, on the other hand, it is less than zero, the solutions exist in the state space. The attractor dissipation formula is given by Eq. (6).

$$\Lambda = V^{-1} \frac{dV}{dt} = \frac{\partial \dot{x}_1}{\partial x_1} + \frac{\partial \dot{x}_2}{\partial x_2} + \frac{\partial \dot{x}_3}{\partial x_3} + \dots + \frac{\partial \dot{x}_n}{\partial x_n} < 0 \quad (6)$$

By applying Eq. (6) to the system (5), we obtained the Eq. (7)

$$\Lambda = \alpha_3 z^2 + \alpha_4 (\beta_2 - 1 - \beta_1 y^2) - 1 - \alpha_2 \quad (7)$$

We choose the parameters α_3 , α_4 and β_1 , β_2 such that Eq. (7) is negative. Therefore, the novel oscillator is dissipative and can develop attractors in the state space.

3.3 Equilibrium Point Study

The equilibrium point of a dynamical system is defined as the set of starting points for which the system does not evolve in space time [70]. Thus, the equilibrium points of the system are obtained by solving the equation $\dot{x} = \dot{y} = \dot{z} = \dot{w} = 0$. By setting $\alpha_1 = 45 \times 10^{-7}$, $\alpha_2 = 0.054$, $\alpha_3 = 0.036$, $\alpha_4 = 1.41$, $\alpha_5 = 0.007558$, $\beta_1 = 1.5$, $\beta_2 = 7.5$, $\alpha = 1.5$, and $a = 1000$, we get only one equilibrium point E_0 as $E_0 (10^{-3}, 1.282 \times 10^{-8}, -1.538 \times 10^{-4}, 1.153 \times 10^{-3})$.

The Jacobian matrix of system (5) evaluated at the equilibrium point E_0 is computed as in Eq. (8).

$$J = \begin{bmatrix} -1 & 0 & 1 & \alpha \\ 0 & \alpha_3 z^2 - \alpha_2 & 2\alpha_3 yz - \alpha_1 & 0 \\ \alpha_4 & -2\alpha_4 \beta_1 yz & \alpha_4(\beta_2 - 1 - \beta_1 y^2) & 0 \\ -\alpha_5 a & 0 & 0 & 0 \end{bmatrix} \quad (8)$$

with $\det(J - \lambda I_4) = 0$; where I_4 is the 4X4 identity matrix. The characteristic equation is written as follows:

$$-\lambda^4 + (N + 1 - M)\lambda^3 + (N - MN + M + L - \alpha_4 - \alpha\alpha_5 a)\lambda^2 + (-MN + L + G + \alpha P\alpha_5 a + \alpha T)\lambda + F - \alpha PT = 0 \quad (9)$$

with $N = \alpha_4(\beta_2 - 1 - \beta_1 y^2)$; $M = -\alpha_3 z - \alpha_2$; $L = 2\alpha_4 \beta_1 yz(2\alpha_3 yz - \alpha_1)$; $G = \alpha_4(-\alpha_3 z + \alpha_2)$; $P = \alpha_3 z - \alpha_2$; $T = \alpha_5 \alpha_4(\beta_2 a - a - \beta_1 y^2)$; and $F = 2\alpha_5 \alpha_4 \beta_1 a yz$.

Considering the value used to get the equilibrium point E_0 , we computed in Table 2 the corresponding eigenvalues. In this regard, we have chosen for some discrete values of β and display the eigenvalues of the Eq. (9) in Table 3.

We have computed the eigenvalues from Eq. (9) in Table 3 by setting the parameter $\alpha = \alpha_{\text{constant}}$ and by varying β_2 in around the value of stability and instability regimes.

We realize that the stability nature of the equilibrium point E_0 changes from stable to unstable by well-known Hof bifurcation phenomenon (not demonstrated here for simplicity reason of the paper) when the parameter β_2 passes the critical value $\beta_{2\text{Critical}} = 1$.

In global view, to share the dynamic behaviors of the system (5) versus the parameters α and β_2 , we plot in the space (α, β_2) , the sign of real part of the eigenvalue in the

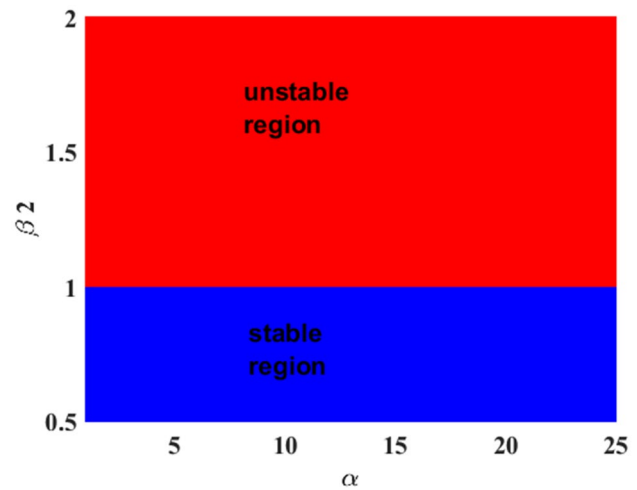


Fig.3 Stability diagram of the novel Chua oscillator in the plane (α, β_2) highlighting the stable regions (color blue) and unstable regions (color red) of system (5)

Fig. 3 (negative sign in color blue and positive sign in color red of system (5)).

3.4 Stability Diagram

The stability diagram of the only equilibrium point E_0 versus the parameters α and β_2 is presented in Fig. 3.

We observed in the light of Fig. 3 that the stable region is separate from the unstable region by the critical line of equation $\beta_{2\text{Critical}} = 1$. The parameter α does not influence the stability of the system (5). Another remark is that the unstable surface is greater that the stable surface. For the rest of this paper, we will choose the $\beta_2 > 1$.

4 Numerical Study

This section deals with the numerical analyses of the system (5) using the fourth order Runge Kutta algorithm (RK4). The numerical computation environment is Pascal

Table 3 Eigenvalues of the characteristic equation and the stability nature of the trivial equilibrium point E_0

Control parameter β_2	Eigenvalues	Stability behavior of E_0
$\beta_2 = 0.5$ to $\beta_2 = 0.9$		Stable
$\beta_{2\text{Critical}}$		Hopf bifurcation
$\beta_2 = 1$	$\lambda_1 = 9.2919$; $\lambda_{2,3} = -0.5634 \pm 2.6715i$; $\lambda_4 = -0.0539$	Instable
$\beta_2 = 1.1$	$\lambda_1 = 9.2910$; $\lambda_{2,3} = -0.5630 \pm 2.8078i$; $\lambda_4 = -0.0539$	Instable
$\beta_2 = 1.3$	$\lambda_1 = 9.2892$; $\lambda_{2,3} = -0.5621 \pm 3.0623i$; $\lambda_4 = -0.0539$	Instable
$\beta_2 = 1.4$	$\lambda_1 = 9.2883$; $\lambda_{2,3} = -5616 \pm 3.1820i$; $\lambda_4 = -0.0539$	Instable
$\beta_2 = 1.5$	$\lambda_1 = 9.2875$; $\lambda_{2,3} = -0.5612 \pm 3.2973i$; $\lambda_4 = -0.0539$	Instable

compiler with variable in extended precision running on an Intel core i5 processor computer with 4 GB of RAM. The well-known methods for dynamical systems analysis such as 2D bifurcation diagram, phase portraits, largest Lyapunov exponent plot, times series, and basin of attraction diagram are used.

4.1 2D Bifurcation Diagrams

The 2D bifurcation diagrams play a very important role in engineering applications because they provide a wider view on the system dynamics under investigation [71]. The following diagrams in Fig. 4 are obtained by varying at the same time two important parameters of the system (5) in order to have a global view on the evolution of the system: firstly, $1 < \beta_1 < 1.5$, $1 < u < 4.5$ in Fig. 4a, and secondly, $3 < u < 7$ in Fig. 4b; $1 < \alpha < 1.5$.

The colors on these diagrams described the behavior of the novel Chua memristive oscillator according to the value of the MLE (maximum Lyapunov exponent), computed using the well-known method described by Wolf et al. in ref. [72]. In the light of these figures, the light green, cyan, dark red, and magenta characterize a chaotic motion while the blue, dark-blue, and light green represent periodic or quasi-periodic motion. It is therefore visible that parameters u , β_1 , and α induced many diverse and interesting dynamics. For these reasons, we chose them in their interesting interval to study the scenario toward chaos.

4.2 Transition to Chaos

In this subsection, we study the transition into chaos toward different parameters of the system namely α and u chosen from Fig. 4. The transition to chaos is illustrated by plotting the bifurcation diagram which represents the local maximums when a parameter of the system is varied [73]. In the following diagrams, we can easily study and predict the long-term behavior of a dynamic system as show in the following subsections.

4.3 Transition to Chaos with the Parameter α

A system is sensitive toward a parameter when, by plotting the bifurcation diagram versus that parameter, we observe a qualitative and quantitative change in the dynamics. This behavior is generally observed in chaotic oscillators as Wien bridge oscillator [74], jerk circuit [75], and more others.

Figure 5a represents the bifurcation diagram by varying the α parameter: $1 < \alpha < 1.5$. The system exhibits period-2 oscillations in the range $1 < \alpha < 1.18$ followed by chaotic oscillations up to $\alpha = 1.28$. Then, a periodic dynamic of period-7 appears followed by a chaotic dynamics in an explanatory way: This is the intermittency route to chaos phenomenon [74]. Figure 5b is the plot of the maximum exponent of Lyapunov for increasing and decreasing value of the control parameter α : $1 < \alpha < 1.5$. The purpose of plotting this figure is to confirm the dynamics observed in the bifurcation diagram [69].

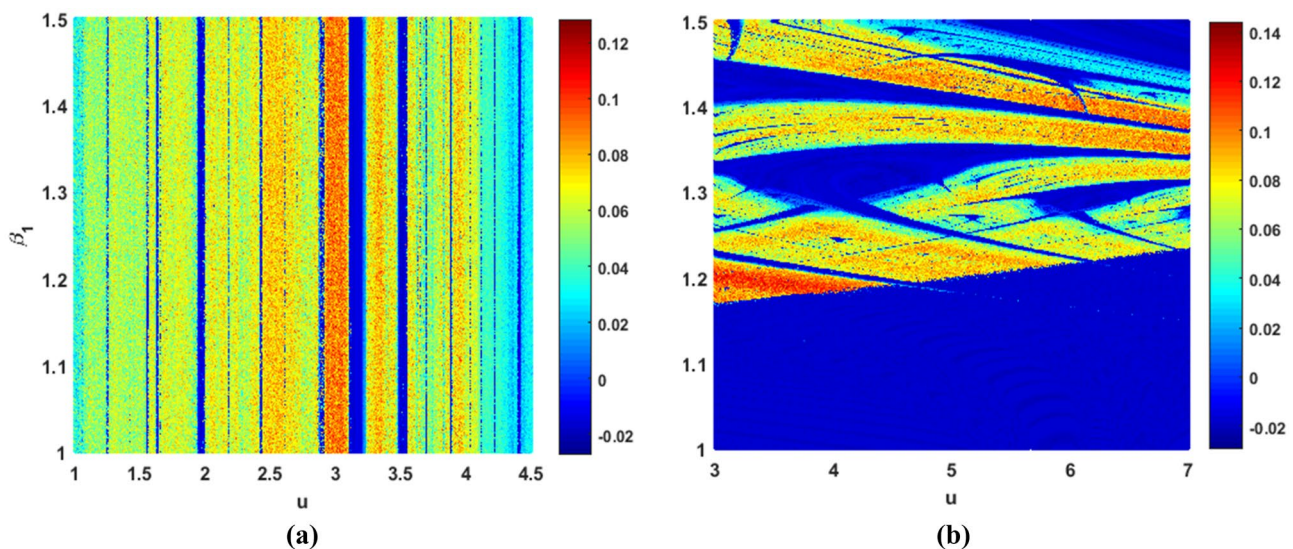


Fig. 4 2D bifurcation diagrams in the plane: **a** (u , β_1) and **b** (u , α) depicting the region of complex dynamics of the system (4) with respect to the maximum Lyapunov exponent (MLE) (right column bar); System (5) parameters are $\alpha_1 = 45 \times 10^{-7}$, $\alpha_2 = 0.054$,

$\alpha_3 = 0.036$, $\alpha_4 = 1.41$, $\alpha_5 = 0.007558$, $\beta_1 = 1.5$, $\beta_2 = 7.5$, $u = 1$, $a = 1000$. Initial conditions are $(x_0; y_0; z_0; w_0) = (0.025; 0.27; 0.001; 0)$ (Color figure online)

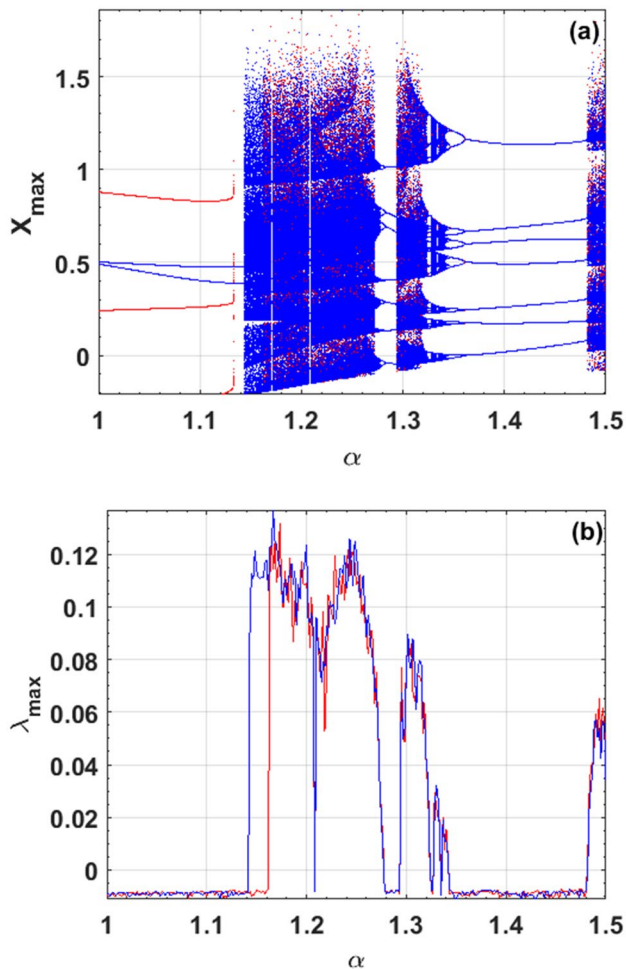


Fig. 5 **a** Bifurcation diagrams of local maxima of state variable x and **b** MLE (λ_{\max}) plotted in the range $1 < \alpha < 1.5$ while keeping $\alpha_1 = 45 \times 10^{-7}$, $\alpha_2 = 0.054$, $\alpha_3 = 0.036$, $\alpha_4 = 1.41$, $\alpha_5 = 0.007558$, $\beta_1 = 1.5$, $\beta_2 = 7.5$, $u = 1$, and $a = 1000$ constants. Blue curve is for increasing value α , while red curve is for decreasing value. Initial computing state $(0.025, 0.27, 0.001, 0)$

We also notice that the increasing path (blue curve) is different from the decreasing path (red curve) of the control parameter: This is known as the hysteresis phenomenon [76]. The hysteresis behaviors are observed in many dynamic systems as in ref. [77]; this behavior is sometimes at the origin of multistability dynamics [78].

4.3.1 Dynamic 1 Revealed: Intermittency Route to Chaos on Parameter α

In dynamical systems, intermittency is the irregular alternation of phases of apparently periodic and chaotic dynamics (Pomeau–Manneville dynamics), or different forms of chaotic dynamics (crisis-induced intermittency) [79]. They described three routes to intermittency where a nearly periodic system shows irregularly spaced bursts of chaos [80]. The following

Fig. 6 shows some phase portraits alongside with a time traces of the system (5) for some discrete values of α .

Figure 6 shows the phase portraits of different transitions observed in our bifurcation diagram with their corresponding temporal traces. Firstly, we obtained an attractor of period-2 with $\alpha = 1.1$ and after tiny changes of control parameter α , the dynamic changes directly to chaotic with $\alpha = 1.2$, which confirms the comments above.

4.4 Transition to Chaos with DC Voltage u

We remarked that the parameter u presents rich dynamics that can be exploited for the study of the global dynamics of the novel memristive Chua oscillator. In addition, the parameter u has a physical meaning which represents for the studied system, the direct voltage connected in series with the inductance L . We plotted in Fig. 7 the bifurcation diagram of the system (5) with respect to parameter u and its corresponding MLE.

Figure 7 represent the outward and inward bifurcation diagrams while varying the parameter u as well as the corresponding MLE spectrum. The interval of this parameter is $3 < u < 7$. As in the previous subsection, we also record the phenomenon of hysteresis marked by the non-superposition of the blue curve and the red curve.

Some sample-phased portraits Fig. 8(i) with the corresponding time traces Fig. 8(ii) are drawn in the following line to illustrate the sensitivity of the system (5) toward u .

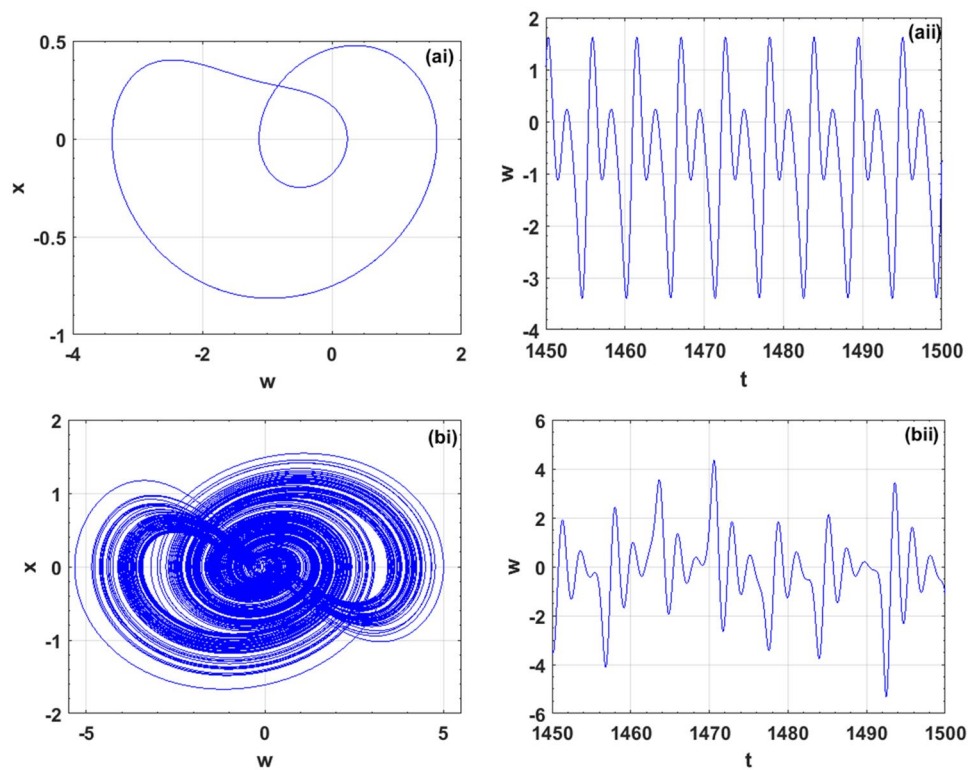
Figure 8 shows phase portraits of the different transitions observed in the bifurcation diagram on Fig. 7 for varying u , with their corresponding temporal traces. We obtained an attractor of period-2 with $u = 7$; period-4 attractor with $u = 6.3$; period-8 attractor with $u = 5.3$; and chaotic attractor with $u = 3$. We can conclude that the system enters chaos by well-known period doubling route [73].

4.4.1 Dynamics 2 Revealed: Coexistence of Multiple Attractors

The multistability is the ability of a system to present different a long-term dynamic with the same set of system parameters and with only changing initial conditions. In chaotic systems, it is defined by the coexistence of multiple attractors in phase space [74, 81]. Note that these solutions are found by fixing the system parameters and by just varying only the initial conditions [82]. This phenomenon is very interesting because it has encountered many engineering systems like electronics circuits [73, 83], Josephson junction [84], biological systems [85], and chemical reaction [86], just to name a few. They are, for some other engineering applications, avoided.

The diagrams in Fig. 9 are obtained by fixing $\alpha = 1.16$ and by changing only the initial conditions from $(x_0; y_0; z_0; w_0) = (2; 2; 0.001; 0)$ to $(x_0; y_0; z_0; w_0) = (0.025;$

Fig. 6 Intermittency route to chaos of system (5) by varying parameter α : **a** period-2 attractor with $\alpha = 1.1$; **b** chaotic attractor with $\alpha = 1.2$. Other parameters: $\alpha_1 = 45 \times 10^{-7}$, $\alpha_2 = 0.054$, $\alpha_3 = 0.036$, $\alpha_4 = 1.41$, $\alpha_5 = 0.007558$, $\beta_1 = 1.5$, $\beta_2 = 7.5$, $u = 1$, and $a = 1000$. (i) are the phased portraits while (ii) are the corresponding time traces. Initial conditions $(x_0; y_0; z_0; w_0) = (0.025; 0.27; 0.001; 0)$



0.27; 0.001; 0). We obtained two different dynamics: a limit cycle of period-2 and a chaotic attractor. This phenomenon is characterized by sensitivity to initial conditions. It is caused by the presence of hysteresis branches observed in the bifurcation diagrams (see Figs. 5 and 7). We therefore drawn the basin of attraction for each found coexisting attractor in Fig. 10 in order to highlight all the initials conditions resulting to each attractor.

The basin of attraction of an attractor is defined as the set of points in the phase space which give an evolving trajectory toward the attractor considered. Pools can extend into infinity, but we stay between $[-3, 3]$ for simplicity of the figure. Some good-standing papers describe the evidence of this behaviors in electronic chaotic oscillators [87, 88], electrical machines [89], chaotic systems [73], and many others.

In the light of Fig. 10, we can see that the blue area that represents initial conditions evolving to the period-2 attractor is larger than the magenta zone that evolve to the chaotic attractor in the plane $(X(0), Y(0))$. The other planes are not shown for simplicity of the paper.

4.4.2 Dynamics 3 Revealed: Spiking and Chaos Bursting

Another interesting dynamic found in this contribution is the spiking and dynamic bursting oscillations. Bursting behavior is an extremely diverse [90] and is found during the activation patterns of neurons in the central

nervous system and spinal cord where periods of rapid action potential spiking are followed by quiescent periods much longer than typical inter-spike intervals [91]. We choose the set of parameters $\alpha = \alpha_1 = 45 \times 10^{-7}$, $\alpha_2 = 0.054$, $\alpha_3 = 0.036$, $\alpha_4 = 1.41$, $\alpha_5 = 0.007558$, $\beta_1 = 1.5$, $\beta_2 = 7.5$, $\alpha = 1.5$ and record the phase portraits and the time traces of the state variable z and x .

The bursting and the spiking displayed in Fig. 11 are interesting phenomena found in the study of the dynamics of our novel memristive Chua oscillator. This phenomenon shows the slow variables Fig. 11a and the fast variables Fig. 11b of the system (5) during its evolution over time. These phenomena are found in many engineering systems [92] and are used in telecommunications [93].

This section end with some interesting dynamics revealed. The next section is focused on the microcontroller experiment to confirm their existence in the novel Chua memristive oscillator.

5 Experimental Study: Microcontroller Implementation

In this section, we proposed an embedded system of the Chua memristive circuit based on the Arduino MEGA microcontroller to confirm the revealed dynamics. This is one of the best methods of implementing dynamic systems because the implementation errors are very low [74].

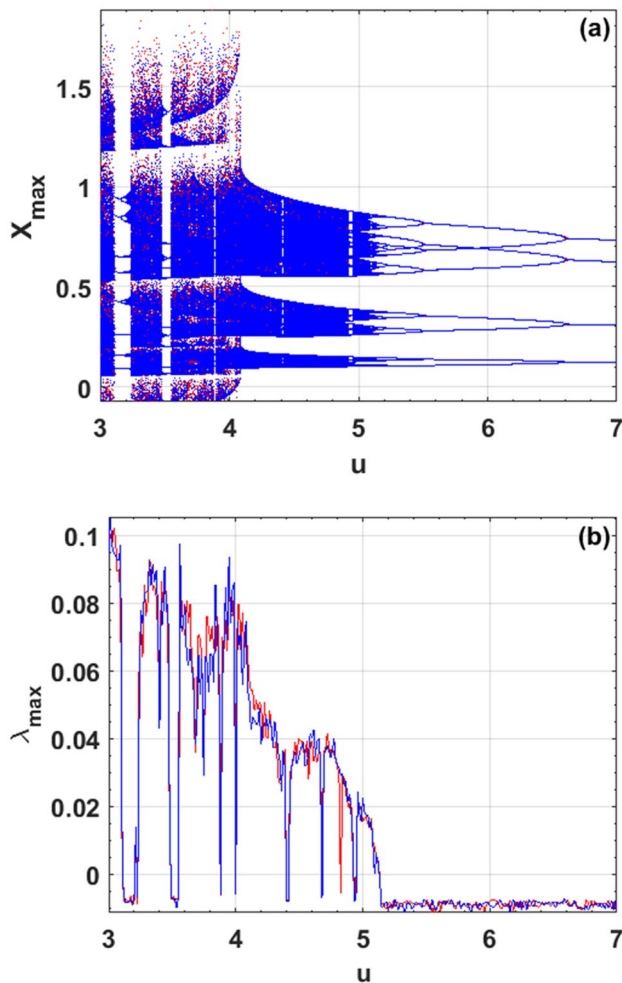


Fig. 7 Bifurcation diagram showing local maxima of state variable x (a) and the MLEs (λ_{max}) (b), plotted in the range $3 < u < 7$ taking $\alpha_1 = 45 \times 10^{-7}$, $\alpha_2 = 0.054$, $\alpha_3 = 0.036$, $\alpha_4 = 1.41$, $\alpha_5 = 0.007558$, $\beta_1 = 1.5$, $\beta_2 = 7.5$, $\alpha = 1.5$, and $a = 1000$. Blue curve is for increasing value α , while red curve is for decreasing value. Initial conditions $(x_0; y_0; z_0; w_0) = (0.025; 0.27; 0.001; 0)$

Note that there are also other digital implementations using FPGA, FPAA, or PIC microcontrollers. Using the RK4 integration method, we solve the discrete version of system (5) using the microcontroller. We are able to retrieve the information in the card from the serial port of the card. The complete setup of the implementation of the novel memristive Chua oscillator is displayed in Fig. 12.

In Fig. 12, the computer is connected to the USB port of an Arduino card built on a simple ATmega2560 microprocessor. The novel memristive Chua oscillator described by system (5) is transformed in its numerical form by means of the 4th order Runge Kutta numerical method with tiny a step time of 0.005 in Arduino software and downloaded in the Arduino card. The resulting real state variables are sent to the serial monitor of the software from the analog signal. Figures 13, 14 and 15 show the

phase planes obtained from the microcontroller of embedded novel memristive Chua oscillator.

The well-known period doubling route to chaos versus voltage u is confirmed experimentally.

As the reader can notice, the intermittence route to chaos revealed in Fig. 6 is confirmed experimentally.

In the light of Fig. 15, the coexisting of 2 different kinds of attractor revealed in Fig. 9 is confirmed experimentally.

From Figs. 13, 14 and 15, we notice that the results obtained experimentally are in agreement with the numerical results obtained in Sect. 4, which shows that our system can be used in engineering applications such as image encryption [94], telemedicine [95], and more others.

These interesting dynamics summarizes a contribution in the research community regarding the idea of founding novel oscillators that have interesting dynamics and that can be helpful in some engineering application [96]. Therefore, in the following Sect. 6, the engineering application (biomedical image encryption) of the novel Chua memristive oscillation is presented.

6 Image Encryption Using the Novel Chua Oscillator

In this section, we are going to use the novel Chua circuit as a random number generation for image encryption as an engineering application.

6.1 Pseudorandom Number Generation

A pseudorandom number generator (PRNG), is an algorithm that generates a sequence of numbers with certain properties of chance [36]. For example, numbers are assumed to be sufficiently independent of each other, and it is potentially difficult to spot groups of numbers that follow a certain rule (group behaviors). Pseudorandom numbers are usually generated from chaotic systems [36], chaotic maps [97], and more others. In addition, note that pseudorandom numbers generated are applied in the encryption of medical information [98]. Our scheme of producing pseudorandom numbers is as follows (Fig. 16).

The bits generated from the previous flowchart must be subjected to NIST test 800–22 Rev. 1a [99] if they are intended for cryptography application. The NIST test allows you to check if the generated bits are random enough to guarantee their use in key for image encryption [100]. The following Table 4 shows the NIST test 800–22 Rev. 1a test carried out.

Table 4 shows the NIST tests performed on our system (5), each time keeping the last eight bits of the three

Fig. 8 Route to chaos by varying the parameter u : **a** period-3 attractor with $u = 7$; **b** period-6 attractor with $u = 6.3$; **c** period-12 attractor with $u = 5.3$; and **d** chaotic attractor with $u = 3$. The others parameter are $\alpha_1 = 45 \times 10^{-7}$, $\alpha_2 = 0.054$, $\alpha_3 = 0.036$, $\alpha_4 = 1.41$, $\alpha_5 = 0.007558$, $\beta_1 = 1.5$, $\beta_2 = 7.5$, $\alpha = 1.5$, and $a = 1000$. Initial condition $(x_0; y_0; z_0; w_0) = (0.025; 0.27; 0.001; 0)$

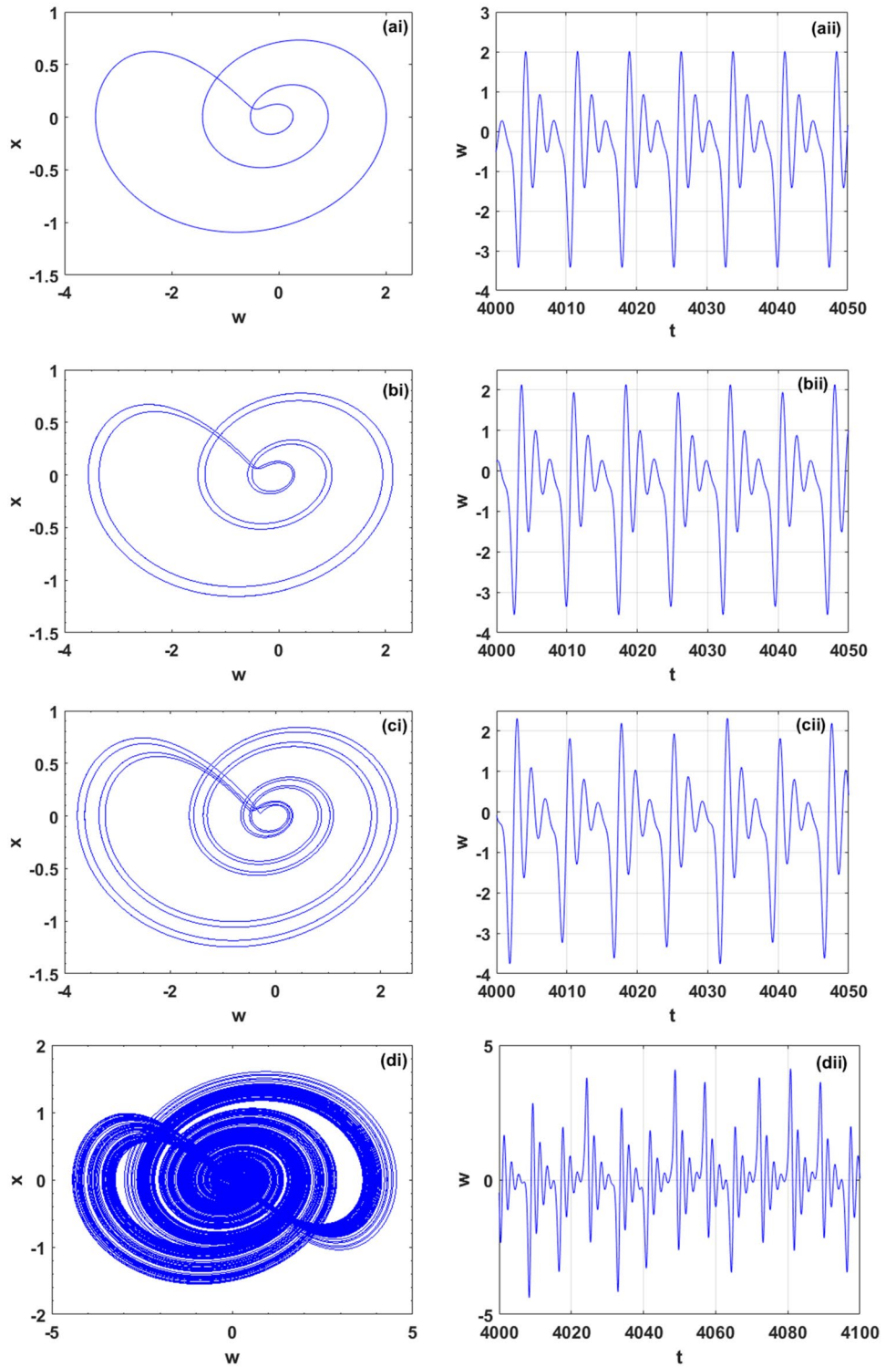
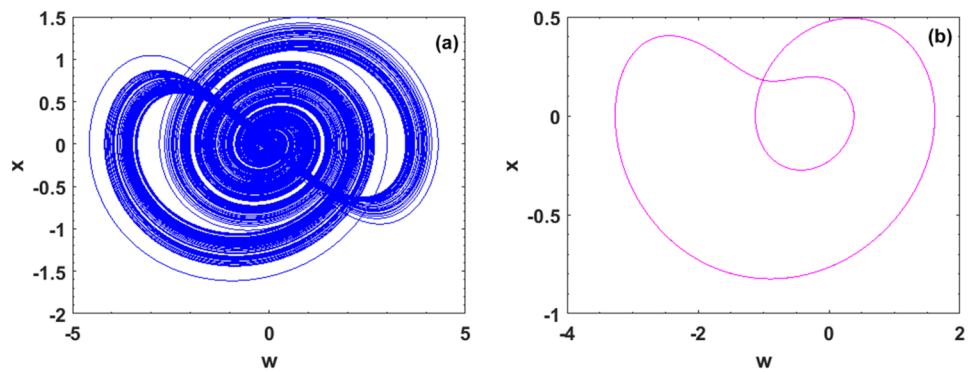


Fig. 9 Phase portraits showing the coexistence of two kinds of attractors for $\alpha = 1.16$; **a** chaotic attractor taking initial conditions: $(x0; y0; z0; w0) = (2; 2; 0.001; 0)$ and **b** period-2 attractor taking $(x0; y0; z0; w0) = (0.025; 0.27; 0.001; 0)$. The system parameters are $\alpha_1 = 45 \times 10^{-7}$, $\alpha_2 = 0.054$, $\alpha_3 = 0.036$, $\alpha_4 = 1.41$, $\alpha_5 = 0.007558$, $\beta_1 = 1.5$, $\beta_2 = 7.5$, and $a = 1000$



different state variables. We can see for different tests, the $P - value \geq 0.01$: This is the necessary condition for the success of a statistical test [101]. Hence, our 4D system is authorized to be used in a cryptosystem application [102].

6.2 Description of the Encryption/Decryption Scheme

In this subsection, the data produced by the Chua’s new chaotic map are used in a permutation-diffusion structure for encryption and decryption of some images and a set of combined images. The main steps of the encryption algorithm are shown in Sect. 6.2.1 and those of the decryption algorithm are shown in Sect. 6.2.2.

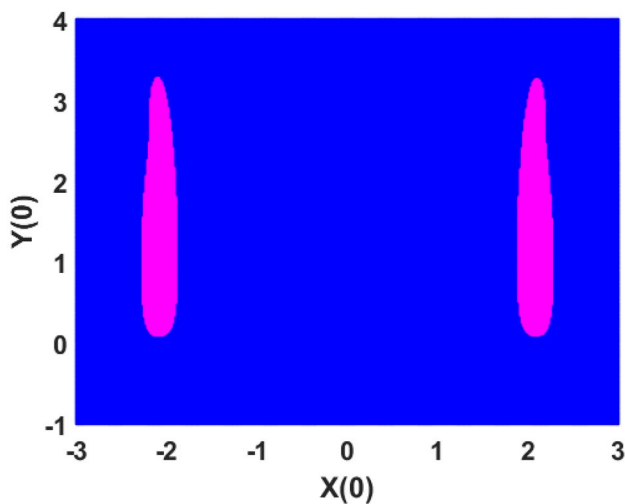


Fig. 10 Basin of attraction plotted in the plane $(X(0), Y(0))$ showing initial conditions that lead to each coexisting steady states: magenta area is for chaotic attractor while blue area is for a period-2 attractor. System (5) parameters are $\alpha_1 = 45 \times 10^{-7}$, $\alpha_2 = 0.054$, $\alpha_3 = 0.036$, $\alpha_4 = 1.41$, $\alpha_5 = 0.007558$, $\beta_1 = 1.5$, $\beta_2 = 7.5$, $\alpha = 1.5$, $a = 1000$, and $u = 1$ (color online)

6.2.1 Encryption Scheme

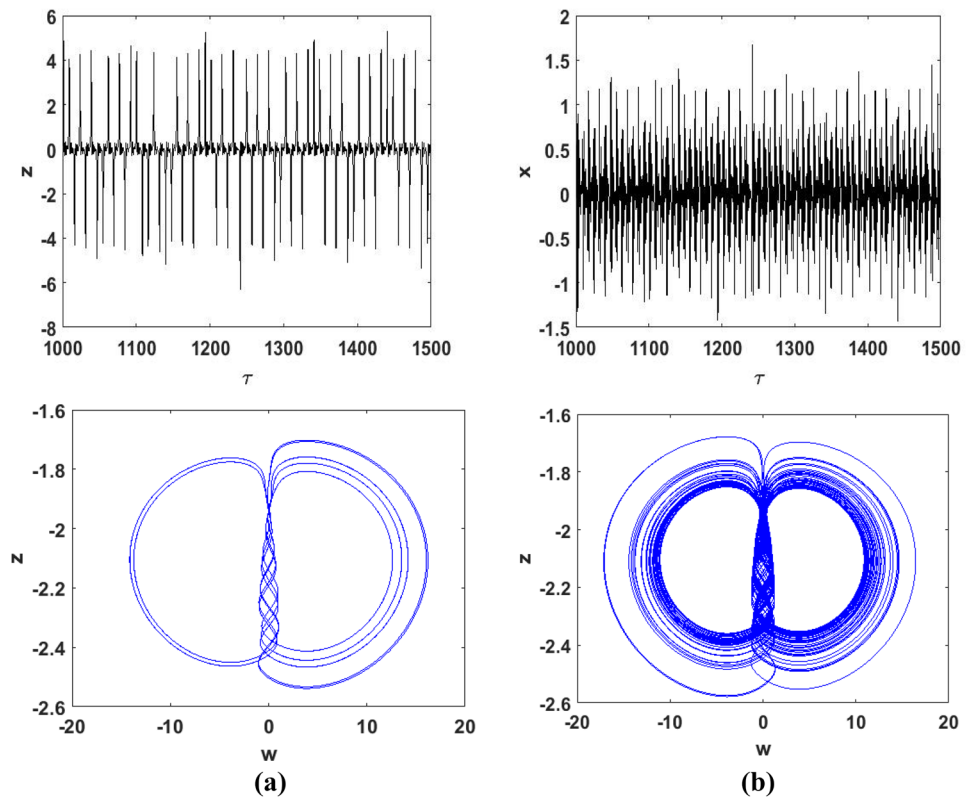
The flowchart of the proposed algorithm consists of three parts, namely, a preprocessing part, a permutation part, and a diffusion part shown in Fig. 17.

The proposed scheme is designed to encrypt one or more images. When a plain image consists of a single source of information, the permutation operation at the pixel level is sufficient to perform the diffusion of it. On the other hand, when the plain image contains several sources of information (a medical image, different medical images in a combined image), it becomes necessary to carry out a first preprocessing operation. It consists of an image pixel rotation (or circular transformation) of blocks of pixels that allows in addition to the rotations to interchange the positions of the blocks in the split image while maintaining parallelism. For this, we used the procedure described in Algorithm 1 because it increases the randomness in the image and reduces the correlation of the image to process. This circular transformation phase results in a mixed image which is then used in the permutation phase at the pixel’s level. In this phase of permutation, the chaotic sequence is generated and used to modify the position of the pixels of the mixed image, in order to obtain the permuted image. Then, a diffusion phase is performed by applying a bit-by-bit XOR operation between another chaotic sequence generated by our chaotic Chua system and the permuted image to obtain the encrypted image. The encryption process is detailed below.

Step 1:

- (a) Split the original image (or combined images) into main image elements (or sub-blocks of small images);
- (b) A pixel block rotation (or circular transformation) is performed between the different image sub-blocks of the main image elements as described by Algorithm 1. The resulting image is a mixed element image.

Fig. 11 Temporal traces of the variables z and x (top) and phase portraits (bottom) marked respectively by the phenomenon of spiking and bursting for the initial conditions $(x_0; y_0; z_0; w_0) = (1; -0.27; -0.2; 1)$. The system (5) parameters are $\alpha = \alpha_1 = 45 \times 10^{-7}$, $\alpha_2 = 0.054$, $\alpha_3 = 0.036$, $\alpha_4 = 1.41$, $\alpha_5 = 0.007558$, $\beta_1 = 1.5$, $\beta_2 = 7.5$, $a = 1000$ for bursting and $\alpha_3 = 0.0036$ for the spiking



Step 2:

Introducing the original image (of size $[M \ N]$ where M is the number of rows and N is the number of columns) is fed into the SHA-256 hash function to produce the keys x_0, y_0, z_0, w_0 for the proposed new Chua chaotic oscillator. More precisely, we obtained a 256-bit hash key that can be denoted by $k = k_1, k_2, \dots, k_{32}$; then, the 256-bit secret key is divided into 8-bit blocks ($k_i = \{k_1, k_2, \dots, k_8\}$). The keys of our new proposed Chua chaotic map here are obtained as follows:

$$\begin{cases} x_0 = \frac{1}{2^8}(k_1 \oplus k_8 \oplus k_2 \oplus k_7 \oplus k_3 \oplus k_6 \oplus k_4 \oplus k_5) \\ y_0 = \frac{1}{2^8}(k_9 \oplus k_{16} \oplus k_{10} \oplus k_{15} \oplus k_{11} \oplus k_{14} \oplus k_{12} \oplus k_{13}) \\ z_0 = \frac{1}{2^8}(k_{17} \oplus k_{24} \oplus k_{18} \oplus k_{23} \oplus k_{19} \oplus k_{22} \oplus k_{20} \oplus k_{21}) \\ w_0 = \frac{1}{2^8}(k_{25} \oplus k_{32} \oplus k_{26} \oplus k_{31} \oplus k_{27} \oplus k_{30} \oplus k_{28} \oplus k_{29}) \end{cases} \quad (10)$$

where \oplus is the bitwise or exclusive operation. Due to the high sensitivity of the raw image for SHA-256, the slightest change in the original image will result in completely different secret keys. Considering the original images of thorax, phalanges, and combined images, the initial conditions are chosen as follows: (x_0, y_0, z_0, w_0) , $(x_0, y_0 + d_2, z_0 + d_3, w_0)$, and $(x_0, y_0 + d_1, z_0 + d_1, w_0)$, with $d_1 = 0.1$, $d_2 = 0.2$, and $d_3 = 0.5$ depending on whether we have the thorax

image (256×256), phalanges (512×512), and combined images (512×512), respectively.

Step 3:

- (a) Use the previously obtained initial conditions (x_0, y_0, z_0, w_0) and the control parameters $\alpha, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \beta_1, \beta_2, u, a$ of our Chua chaotic system as the key parameters of our cryptosystem.
- (b) After specifying the key parameters, use the fourth order Runge–Kutta discretization algorithm to iterate Eq. (5) n times and generate two sequences of values $X_1 = \{x_1, x_2, \dots, x_n\}, Y_1 = \{y_1, y_2, \dots, y_n\}$, or $n = M$

The first sequence of values X_1 is intended to scramble the image of mixed elements along the rows and the second Y_1 along the columns. The first 10,000 iterations are dropped.

Step 4:

- (a) Arrange the values of the chaotic sequences obtained previously in ascending order;
- (b) For each position of couple row-column (x_i, y_i) of pixels of the image, look for the previous position of the corresponding couple row-column (X_{i-1}, Y_{i-1}) of the ordered and substituted pseudorandom values.

Algorithm 1. Image pixel rotation (or Circular transformation)

input: Im0 (image divided into blocks)

output: Im1 (mixed image)

```

1  Load divided image Im0 of size  $M \times N$  ;
2  Store all of the  $k$  small sub-blocks of images obtained previously in matrix  $A$  size  $M \times N$  ;
3  Determine  $m$  et  $n$  as the number of row and column of  $A$  ;
4   $B \leftarrow reshape(A', 1, m \times n)$ ; where  $B$  is the transpose of  $A$  into a column matrix
5   $A1 \leftarrow B$  ;
6   $A1 \leftarrow circshift(A1, 1)$ ;
7   $N \leftarrow length(A1)$ ; where  $N$  is the number of blocks of  $A1$  size  $p \times q$ 
8  for  $j$  from 1 to  $N$  do
9       $Y \leftarrow A1(j+1:end, 1)$ ;
10      $Y \leftarrow circshift(Y, 1)$ ;
11      $A1(j+1:end, 1) \leftarrow Y$ ;
12 End
13  $Im1 \leftarrow reshape(A1', [m, n])$ ;
    
```

$$(x_i, y_i) \leftarrow (X_{i-1}, Y_{i-1}) \tag{11}$$

- (c) Permute the position of the last pixel of the image with a real.

Step 5:

Convert the permuted image as a column vector.

Step 6:

- (a) Do the same as in **Step 3** (a);
- (b) Use the fourth order Runge–Kutta discretization algorithm to iterate Eq. (5) and generate a sequence of values $Z_2 = \{z_1, z_2, \dots, z_{M \times N}\}$, where M and N are, respectively, the number of rows and columns of the original image.
- (c) Load the values of the chaotic sequence Z_2 into an array W of the same size with the permuted (or encrypted) image.

Step 7:

Reshape the values W of as a column vector.

Step 8:

Calculate the pixel value $C(i)$ of the encrypted image using the pixel of the permuted (or scrambled) image $P(i)$ and the column vector of the chaotic sequence values $W(i)$ according to the following relationship:

$$C(i) = P(i) \oplus floor[\text{mod}(W(i) \times 10^{15}), 256] \tag{12}$$

Or $i = 1, 2, \dots, M \times N$.

Thus, the cipher image is obtained.

6.2.2 Decryption Scheme

To recover the permuted (or scrambled) image during decryption, it is sufficient to perform the inverse form of Eq. (12) as follows:

$$P(i) = C(i) \oplus floor[\text{mod}(W(i) \times 10^{15}), 256] \tag{13}$$

Or $i = 1, 2, \dots, M \times N$.

Thus, the scrambled (or permuted) image is obtained.

The raw image is obtained by decrypting the permuted image following the decryption flowchart in Fig. 18.

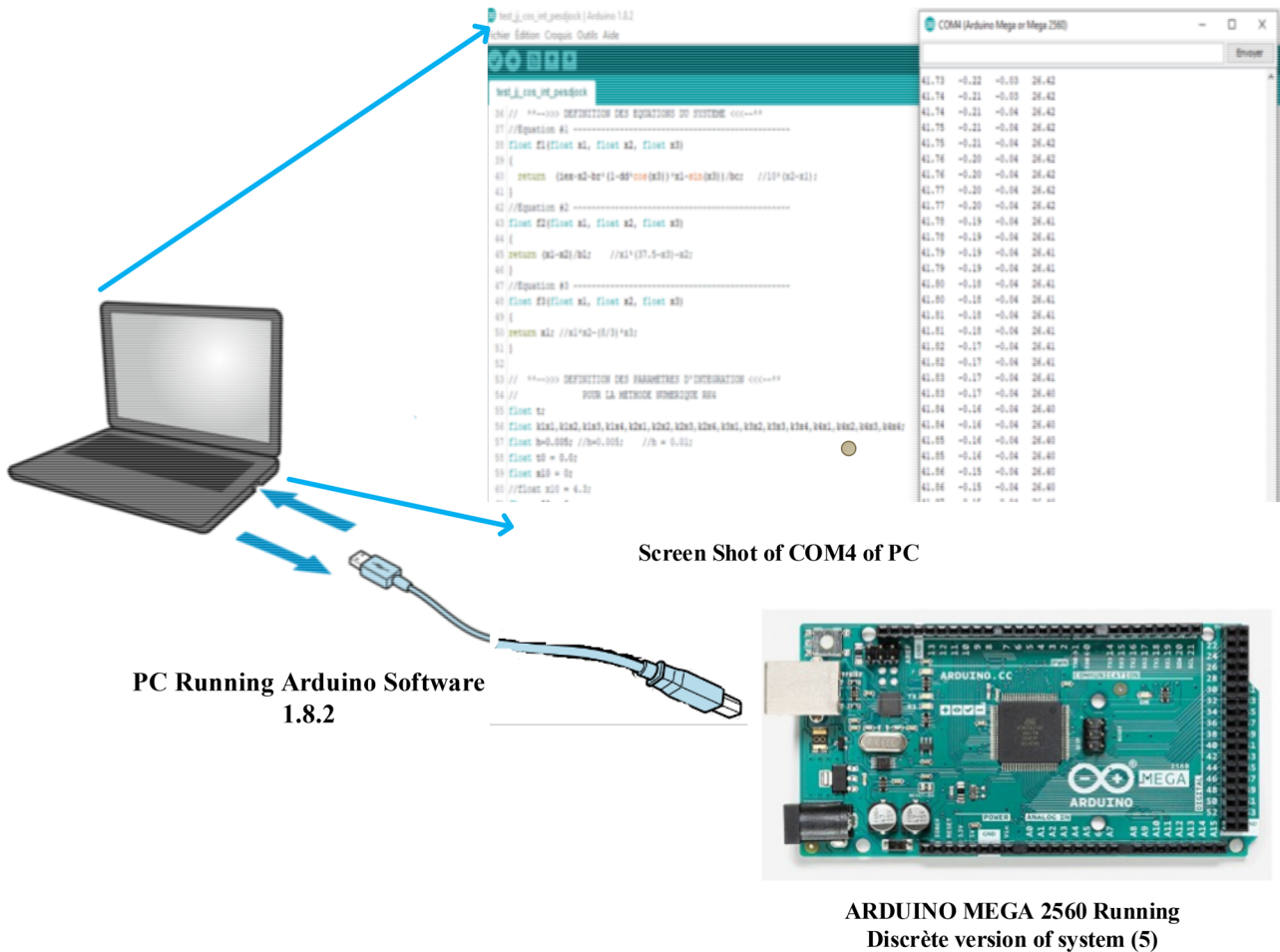


Fig. 12 Microcontroller design circuit embedded the novel memristive Chua oscillator

6.3 Experimental Results

The encryption/decryption process is applied on 3 biomedical images: Thorax (256 × 256), phalanges (512 × 512), and combined image (512 × 512) as shown in the first line of Fig. 19.

Then, the mixed and ciphered images of the latter are shown in the second and third line of Fig. 19. Thereafter, the recovered images are shown in the fourth line of Fig. 19. Simulations are carried out on a computer using the MATLAB 2012b platform, Windows 10 operating system, Intel(R) Core (TM) i5-4030 M CPU @ 1.9 GHz, and 4 GB RAM. In order to appreciate the efficiency of the proposed cryptosystem against the mains attacked, many tests and analyses are performed in the upcoming subsection.

6.4 Performance Analyses

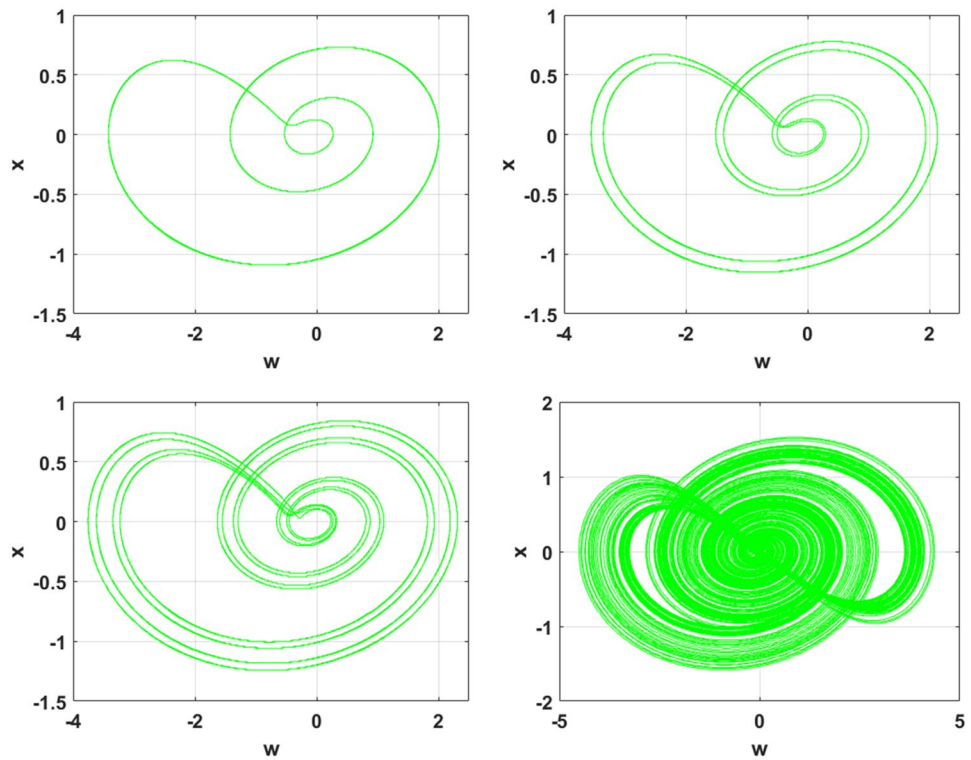
This subsection is devoted to show some indicators and results to access the performances of our cryptosystem. They

are key space, key sensitivity, differential attack, statistical analyses, histogram, speed analysis, and noise attack just to mention some critical ones.

6.4.1 Key Space

For a good cryptosystem, the key space should be large enough to invalidate violent attack [103, 104]. It is built from available key used in the cryptosystem. For our cryptosystem, the initial conditions (x_0, y_0, z_0, w_0) and the parameters $(\alpha, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \beta_1, \beta_2, u, a)$ of the chaotic oscillator constitute the key space parameters. Therefore, the key space is around $(10^{15})^4 \times (10^{15})^{10} = 10^{210} \approx 2^{630}$. The suggested accuracy is 10^{-15} , for 64 bits' double precision number, which depends on the IEEE floating point rule. The resulting key space is 2^6 times greater than the value of key space to be safe 2^{100} . Therefore, the key space is not the means by which this encryption algorithm will fail.

Fig. 13 Route to chaos using Arduino: The first figure obtained with $u = 7$, the second with $u = 6.3$, the third with $u = 5.3$, and the fourth with $u = 3$. Initial conditions $(x_0; y_0; z_0; w_0) = (0.025; 0.27; 0.001; 0)$. These figures resemble the one in Fig. 8, Sect. 4



6.4.2 Key Sensitivity

For a good cryptosystem, a tiny change in the secret key should result in a completely different cipher image for the same input image. In this way, one cannot decrypt the cryptogram of the other cryptosystem. It then becomes very difficult to carry out a plain image or chosen cipher image attack. To verify this property, we performed a slight change in the key of order of 10^{-5} , resulting in difficulty to decrypt the cipher image. We tested this property by modifying of 14 parameters of the key and results in image difficulty to decrypt as shown in Fig. 20.

6.4.3 Differential Attack Analysis

There are two main parameters to analyze the differential attacks: the number of pixels change rate (NPCR) and the unified average

changing intensity (UACI). These parameters test the sensitivity algorithm toward slightest changes in plain image [48].

NPCR The NPCR is defined as the percentage of different pixel numbers between two encrypted images, whose plain images have only one-pixel difference. It can be computed as follows.

$$NPCR = \frac{\sum_{i=1}^m \sum_{j=1}^n f(i, j)}{m \times n} \times 100\% \tag{14}$$

$$\text{With } f(i, j) = \begin{cases} 0 & \text{if } I_{mo}(i, j) = I_{mc}(i, j) \\ 1 & \text{if } I_{mo}(i, j) \neq I_{mc}(i, j) \end{cases}$$

where m and n represent, respectively, the high and the width of the image. $f(i, j)$ denotes the difference between

Fig. 14 Intermittency route to chaos confirmed: The first figure obtained with $\alpha = 1.1$ and alpha second with $\alpha = 1.2$. Initial condition $(x_0; y_0; z_0; w_0) = (0.025; 0.27; 0.001; 0)$. These figures resemble the ones in Fig. 6

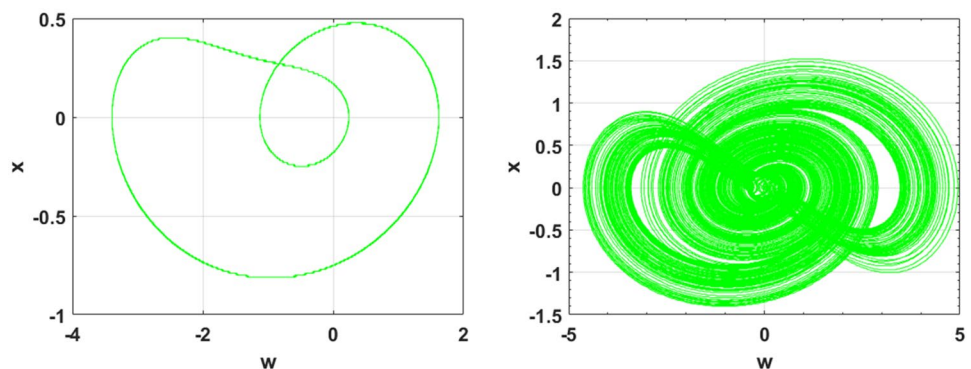
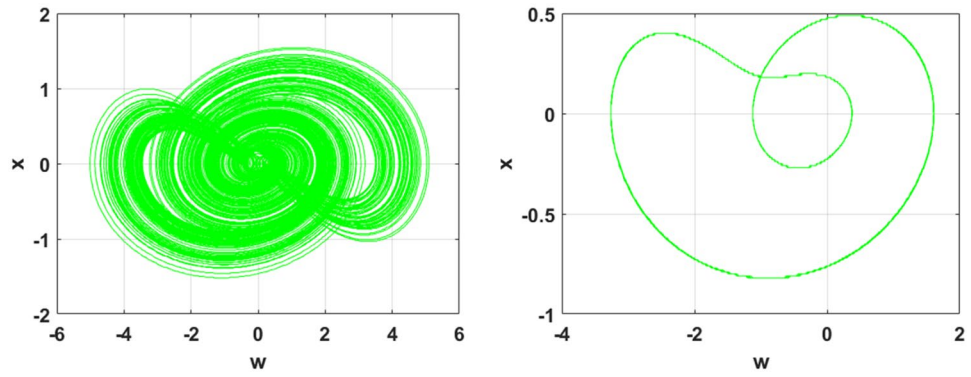


Fig. 15 Multistability behavior experiment using Arduino: The first figure obtained with $\alpha = 1.16$. Initial condition $(x_0; y_0; z_0; w_0) = (2; 2; 0.001; 0)$, and the second with initial condition $(x_0; y_0; z_0; w_0) = (0.025; 0.27; 0.001; 0)$. These curves resemble the ones in Fig. 9



corresponding pixels of encrypted image $I_{mc}(i, j)$ from the original image $I_{mo}(i, j)$. The ideal value of NPCR is 100. In the light of Eq. (14), we displayed in Table 5 this metric for the 3 analyzed images.

It is easy to see from Table 5 that the average NPCR value for the thorax, phalanges, and combined images is at least 99.6044%; therefore, our encryption method having NPCR value is close to ideal metrics.

UACI The average intensity of the pixel value modified in the same location of the two images is determined by UACI defined as

$$UACI = \frac{\sum_{i=1}^m \sum_{j=1}^n |I_{mo}(i, j) - I_{mc}(i, j)|}{255 \times m \times n} \times 100\% \tag{15}$$

The UACI values computed for the analyzed images are displayed in Table 6.

It is evident from Table 6 that the UACI values computed are close to those standard values, and these results indicate that the proposed image encryption algorithm may effectively spread slight change of original images to the complete cipher images. That is because our algorithm is highly sensitive to the plain image, so that the different cipher images may be gotten by varying plain image a little.

6.4.4 Statistical Analysis

Histogram Analysis This analysis reflects the distribution of gray scale of digital image [52]. The variance computation is an analysis to measure the randomness in histogram of images as in the Eq. (16).

Fig. 16 Flow chart of the PRNG

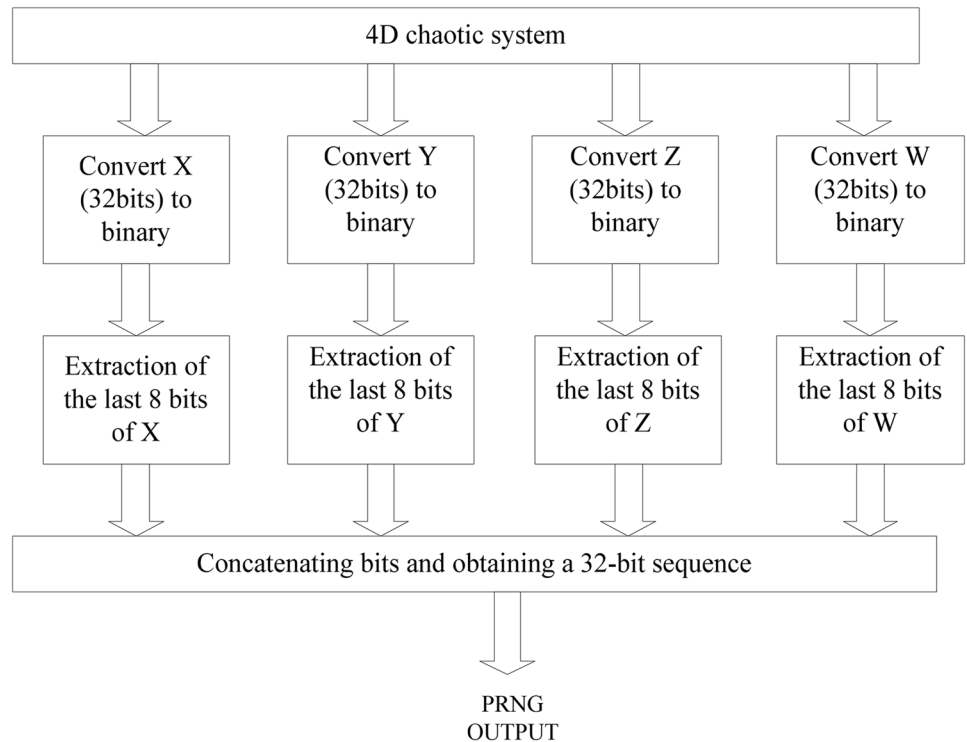


Table 4 NIST test 800–22 Rev. 1a performed on data coming from the system (5)

Name of test	P-value	Results
Frequency test	0.2324	Success
Block frequency test	0.0474	Success
Runs test	0.3296	Success
Longest runs of one’s test	0.8912	Success
Rank test	0.0788	Success
Discrete Fourier transform test	0.8760	Success
Overlapping template of all one test	0.3144	Success
Non-overlapping template of all one test	0.0194	Success
Maurer’s «universal statistical» test	0.8404	Success
Linear complexity test	0.3722	Success
Serial test	0.8213	Success
Approximate entropy test	0.0934	Success
Cumulative sum test	0.04157	Success
Random excursion test	0.4443	Success
Random excursion test variant test	0.5387	Success

$$\text{var}(z) = \frac{1}{n^2} \sum_1^n \sum_1^n \frac{1}{2} (z_i - z_j)^2 \tag{16}$$

where z is the vector of the histogram values in an array and the quantity of pixels having gray levels z_i equivalent to i ; the quantity of pixels having gray levels z_j equivalent to j individually; the total number of pixels is represented by n .

We computed the histogram of original image of thorax and phalanges in Fig. 21 as well as the scramble image at Fig. 22. It can be seen that Fig. 22 hides the statistic behavior of the image.

To demonstrate the degree of distribution in each image, Table 7 shows the cipher images variance computed of phalange, thorax, and combined images.

In the light of Table 7, the variance of cipher image is not far from the ideal value of 5000 showing that our encryption method is secure enough to overcome the statistical attacks.

Correlation Analysis An important statistical key point to evaluate an image encryption algorithm in the adjacent pixel correlation [105]. If neighboring pixels are highly correlated, the image is exposed to statistical attack. To avoid this type of attack, 5000-pixel pairs are randomly selected from plain images and their respective cipher. Then, the correlation index between two adjacent pixels in vertical, horizontal, and diagonal directions is calculated using Eq. (17).

Fig. 17 Flowchart of the proposed encryption scheme

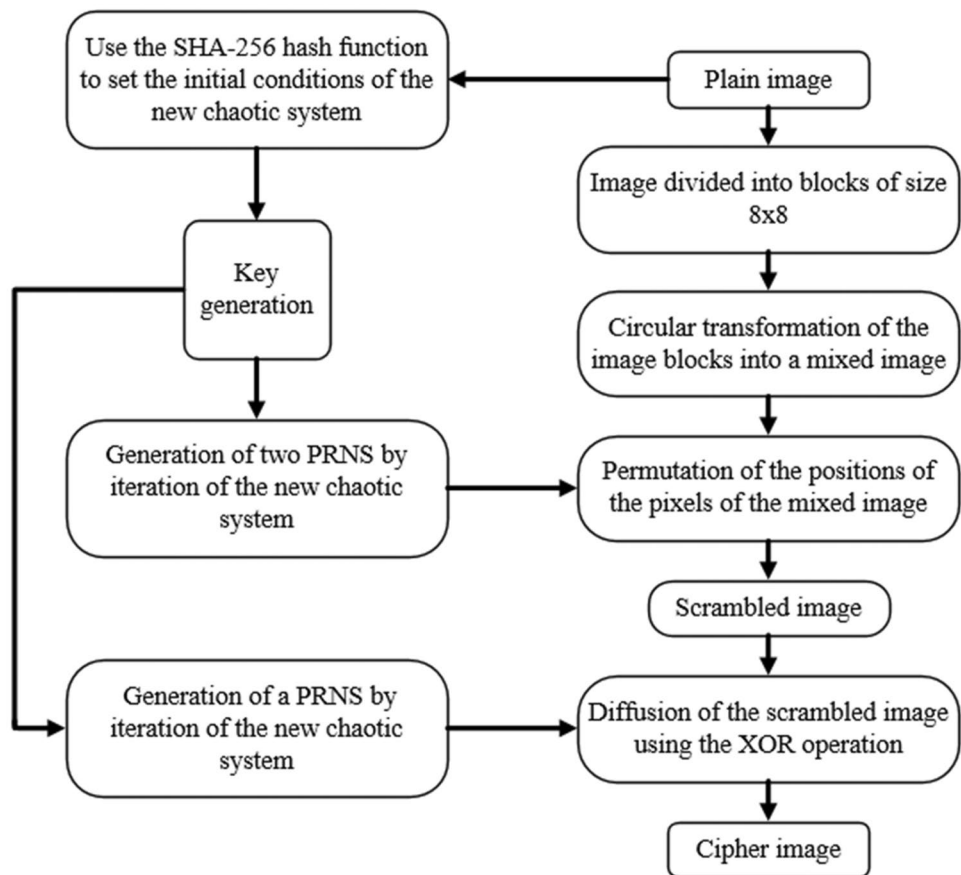
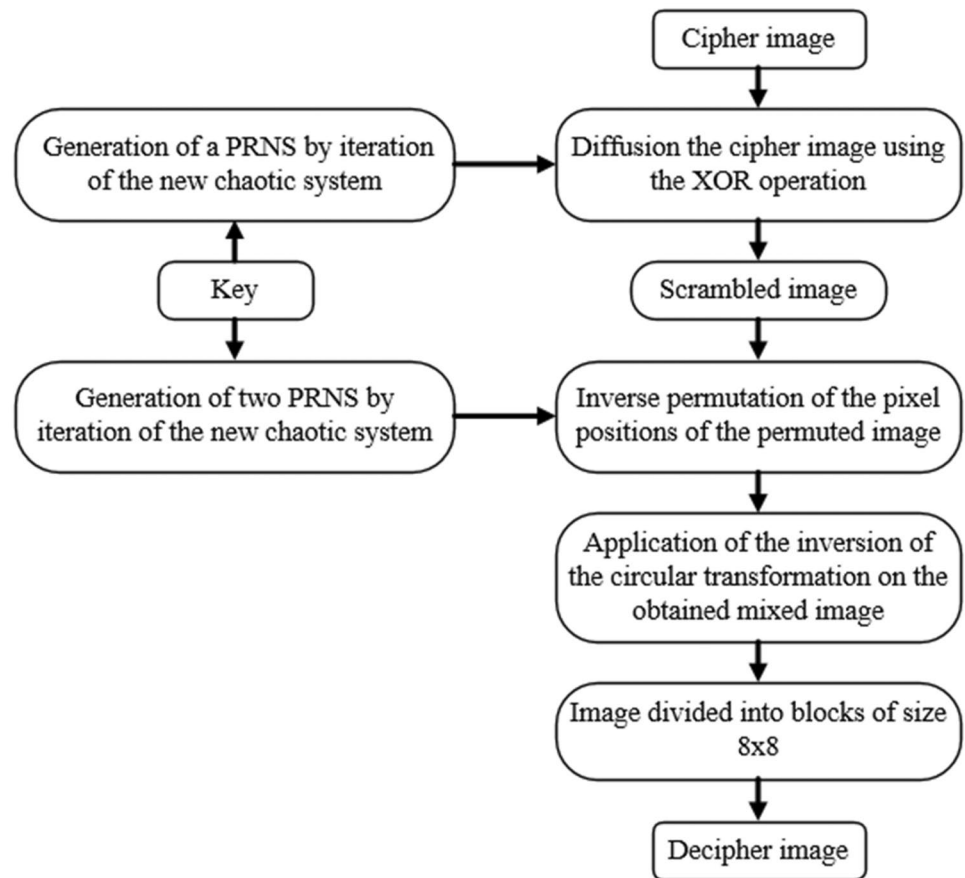


Fig. 18 Flowchart of the proposed decryption scheme



$$r_{xy} = \frac{N \times \sum_{i=1}^N x_i y_i - \sum_{i=1}^N x_i^2 \times \sum_{i=1}^N y_i^2}{\sqrt{\left(N \times \sum_{i=1}^N (x_i)^2 - \left(\sum_{i=1}^N x_i \right)^2 \right) \times \left(N \times \sum_{i=1}^N (y_i)^2 - \left(\sum_{i=1}^N y_i \right)^2 \right)}} \quad (17)$$

where x and y are the values of the selected adjacent pixels, N is the total number of randomly selected pixel pairs, and r_{xy} is the correlation coefficient of x and y . The pixel distributions of the raw images and the encrypted images are shown in Figs. 23 and 24.

As can be seen in Fig. 23, for the phalanx image, the adjacent pixels in the plain image are densely concentrated in all directions, while the adjacent pixels in its encrypted image in Fig. 24 are uniformly distributed. This shows that the plain image has strong correlation in all directions (horizontal, vertical, and diagonal), but the correlation in the encrypted image is weak.

Furthermore, the values of the correlation coefficients of the images are recorded in Table 8 for the correlation coefficients of the plain images and their encrypted equivalents in Fig. 19. These results show that the correlation coefficients

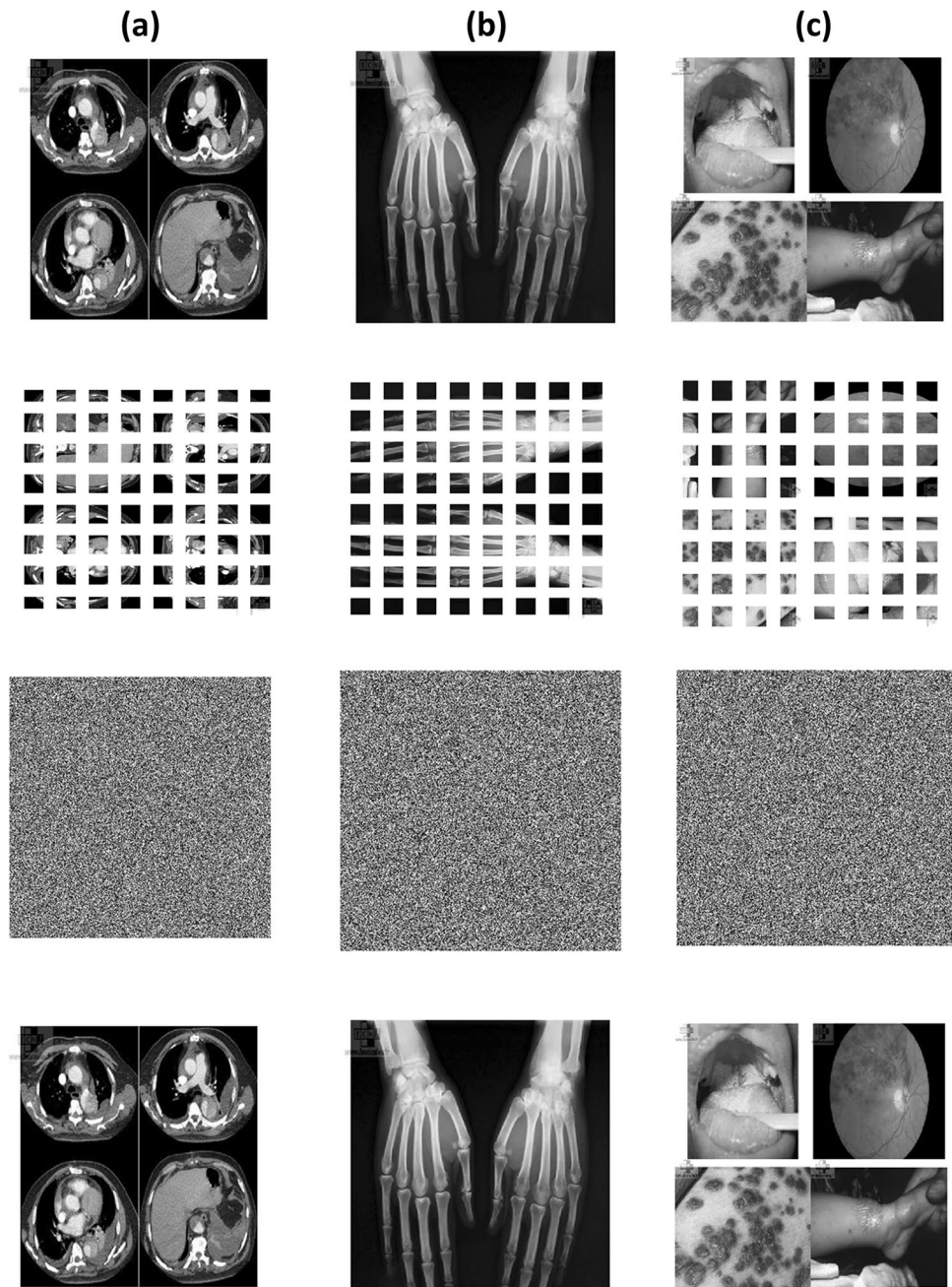
of the plain images are close to 1. While for the encrypted images, the correlation coefficients are close to 0. Thus, the proposed algorithm is highly resistant to statistical attacks.

As it can be seen from Table 8, correlation coefficients of adjacent pixels of plain images are greater than 0.9, indicating that there is a strong relationship between adjacent pixels of plain images in different directions, and correlation coefficients of adjacent pixels of cipher images are less than 0.015; the correlation between pixels is small and can be ignored. The above results prove that our image encryption has good pixel de-correlation feature.

Entropy Analysis This key point measures the disorder or the randomness of the encrypted image. A high value of entropy determines a better distribution of the gray levels of the image [106]. It is measured using the Shannon entropy formula as follows.

$$H(m) = \sum_{i=0}^{255} p(m_i) \log_2 \left(\frac{1}{p(m_i)} \right) \quad (18)$$

Fig. 19 Medical images of **a** thorax, **b** phalanges, and **c** combined: from top to bottom: plain, circular transformation, cipher, and decipher. **a** Thorax, **b** phalanges, **c** and combined image



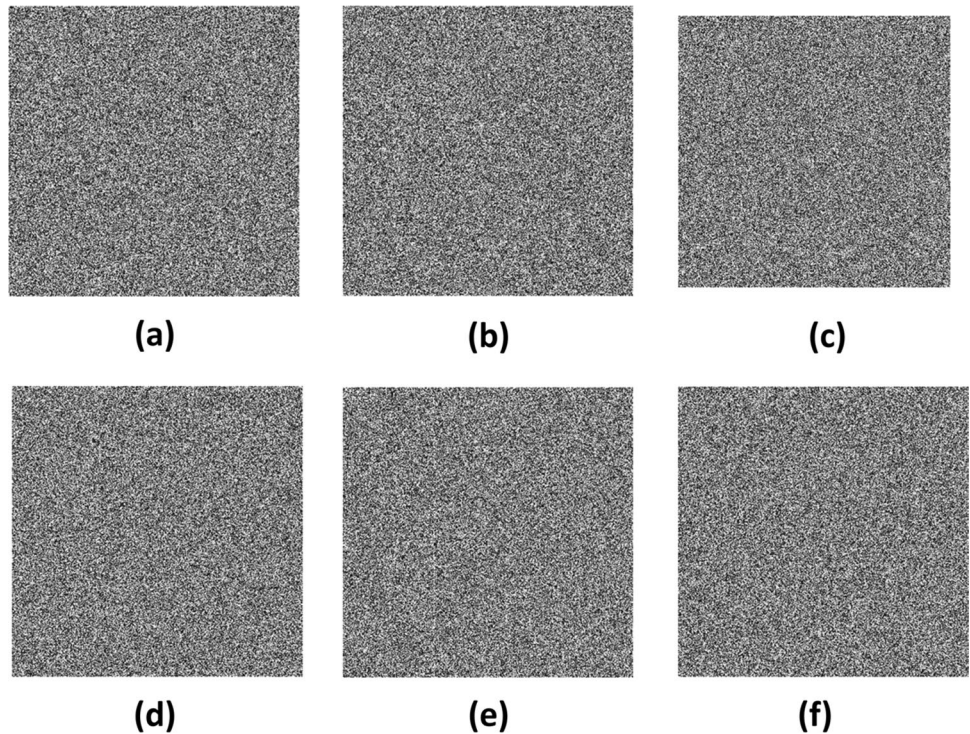
where $p(m_i)$ is the probability of the symbol m_i and $H(m)$ is the entropy of the data image. For an image of 256 Gy level, the pixel has 28 possible values and the ideal entropy for a perfect encrypted image is 8. Then, the security of the encryption algorithm against entropy attack is highlighted when the entropy value is close to 8.

In the light of Table 9, the information entropy computed for cipher images is all at least greater than 7.99 indicating that cipher images gotten from the proposed algorithm have good randomness.

6.4.5 Speed Analysis

The processing time is the time required to encrypt and decrypt an image. The smaller value the processing time has, the better the encryption efficiency will be. Time consumption was carried under Windows 10 operating system, Intel(R) Core (TM) i5-4030 M CPU @ 1.9 GHz, and 4 GB RAM. The MATLAB 2018(a) platform was used for our encryption algorithm. For a 512×512 image, it takes 2.465685 s for encryption. This time is very small to give time for some attacks.

Fig. 20 Key sensitivity analysis when decrypting the encrypted image of thorax by slightly changing the secret key: **a** y_0 modified to $y'_0 = y_0 + 10^{-15}$, **b** α modified to $\alpha' = \alpha + 10^{-15}$, **c** α_5 modified to $\alpha'_5 = \alpha_5 + 10^{-15}$, **d** β_1 modified to $\beta'_1 = \beta_1 + 10^{-15}$, **e** z_0 modified to $z'_0 = z_0 + 10^{-15}$, and **f** α_1 modified to $\alpha'_1 = \alpha_1 + 10^{-15}$



6.4.6 Noise Attack Analysis

This type of attack is designed to prevent the receiver from successfully recovering the encrypted image by introducing Gaussian or Poisson noise into the encrypted image. To test the encryption scheme, Gaussian noise of zero mean and different variance is added to the image as follows.

$$Img = immnoise(Ie, 'Guassian', 0, var) \tag{19}$$

where Ie represents the original image; Img represents the contaminated image; and var represents the variance number $0.01 < var < 1$. Figure 12 displays the analyzed image thorax, of 256×256 bits added to Gaussian noise with variance of 0.1; 0.5; and 0.9.

In the light of Fig. 25, the decrypted image of thorax (256×256) affected by Gaussian noise is presented

for three different values of the variance. In this figure, we observed that even for a high value of the variance ($var = 0.9$), the decrypted image is still recognizable.

6.5 Comparison with Other Cryptosystems

In this last subsection, the security comparisons with the latest published article in terms of security testing are shown in Table 10.

The performance of our system has been compared (Table 10) with some recent and good quality papers in the literature. We can see in Table 10 that the key space of our cryptosystem is larger than those of refs. [44, 45, 50, 52, 53]. It should be noted that compared to ref. [53], the proposed encryption scheme has a lower information entropy. Nevertheless, the difference between them is so small that it does not affect the security of the cryptosystem. We can

Table 5 NPCR computation after differential attacks of thorax, phalanges, and combined images

Image name	Thorax (256 × 256)	Phalanges (512 × 512)	Combined images (512 × 512)
NPCR	99.6261	99.6044	99.6051

Table 6 UACI computation after differential attacks of thorax, phalanges, and combined images

Image name	Thorax (256 × 256)	Phalanges (512 × 512)	Combined images (512 × 512)
UACI	33.4688	33.4259	33.3518

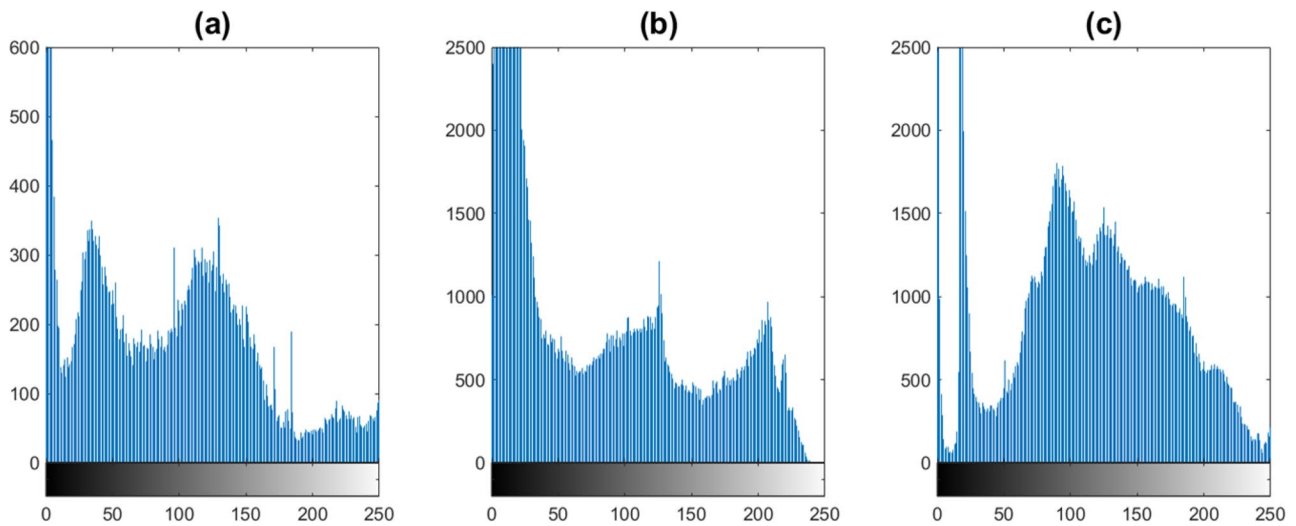


Fig. 21 Histogram diagram of original images: **a** Thorax (256×256), **b** phalanges (512×512), and **c** combined images (512×512)

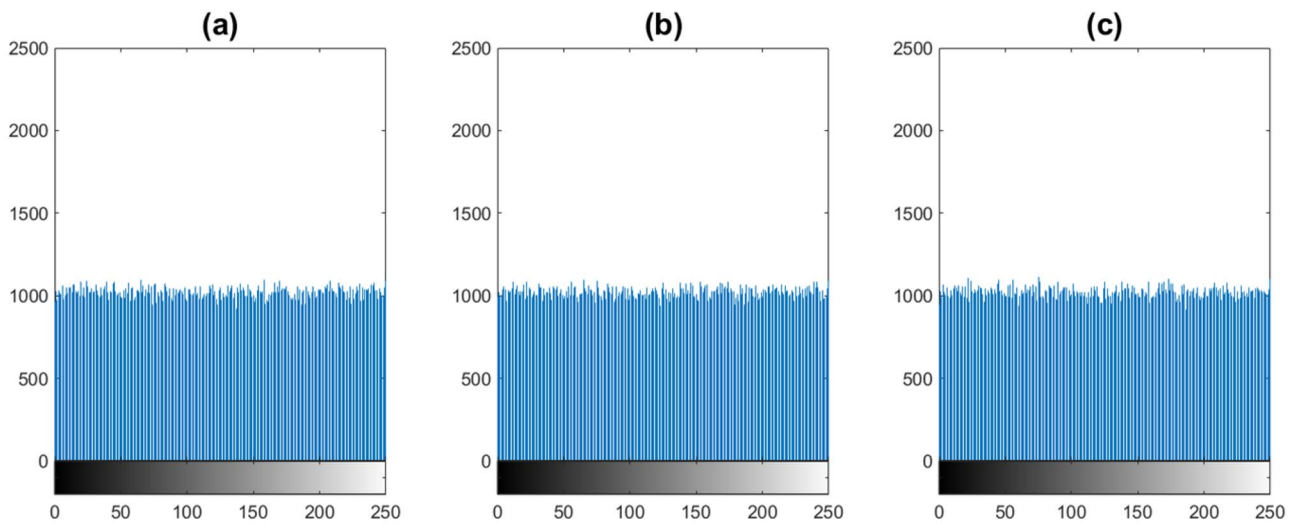


Fig. 22 Histogram diagram of cipher images: **a** Thorax (256×256), **b** phalanges (512×512), **c** combined images (512×512)

Table 7 Histogram variances for original and scrambles images of the proposed cryptosystem

	Dimension	Original image	Scramble image
Thorax	256×256	7116.7	5468
Phalanges	512×512	6026.6	5473.4
Combined image	512×512	5610.5	5479.4

also notice in Table 10 that the average NPCR and UACI values obtained by the proposed scheme are among the best in the literature. Therefore, these results suggest that the medical image encryption scheme based on Chua’s chaotic memristive oscillator system can resist entropy and statistical and differential attacks more effectively and can be applied to protect image data in real-time information communication systems.

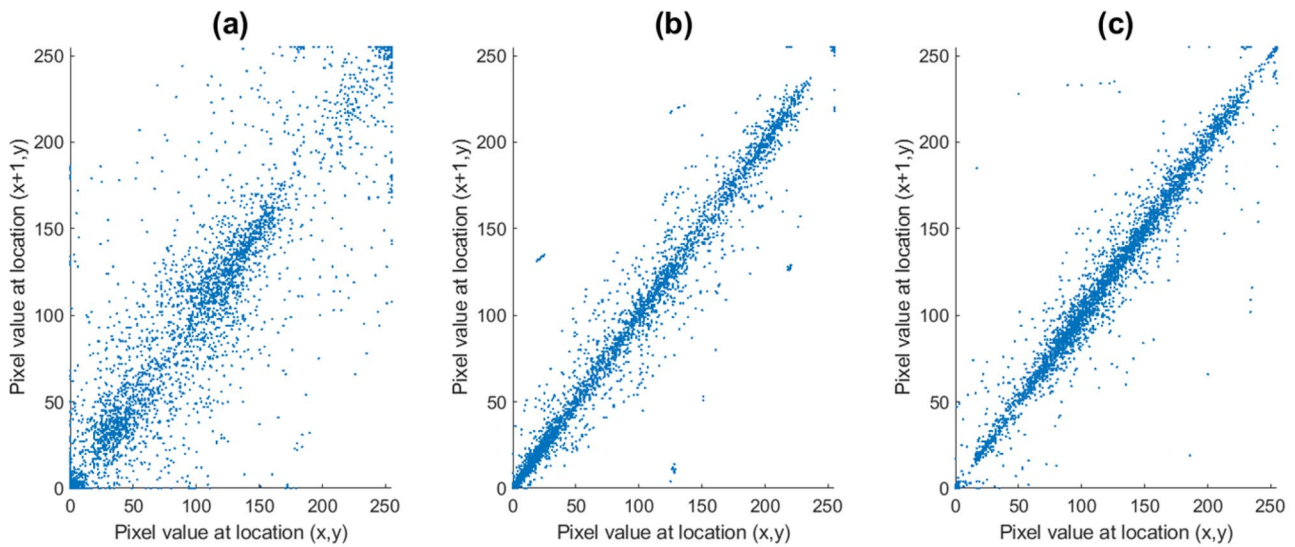


Fig. 23 Pixel value distribution of the plain images of **a** thorax, **b** phalanges, and **c** combined images

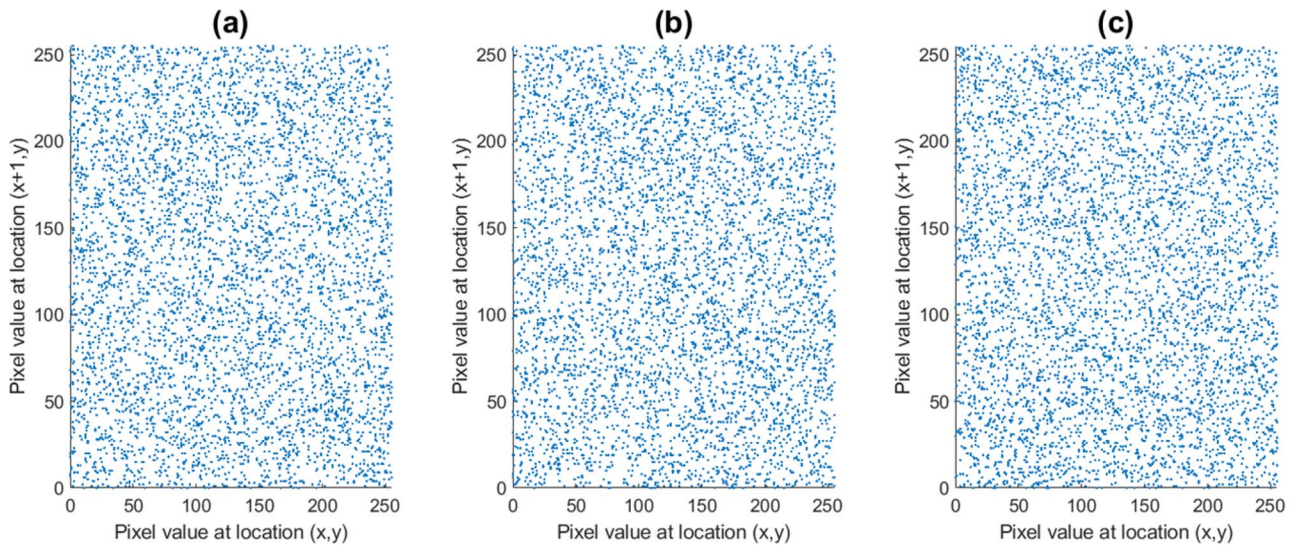


Fig. 24 Distribution of the adjacent pixels of cipher images in the horizontal direction: **a** thorax, **b** phalanges, and **c** combined images

Table 8 Correlation coefficients of two adjacent pixels of plain image and cipher images

	Dimension	Test direction	Original Image	Cipher image
Thorax	(256 × 256)	HC	0.9174	0.0051
		VC	0.9757	-0.0056
		DC	0.9030	0.0012
Phalanges	(512 × 512)	HC	0.9688	0.0084
		VC	0.9968	0.0160
		DC	0.9707	-0.0023
Combined images	(512 × 512)	HC	0.9843	-0.0078
		VC	0.9844	0.0122
		DC	0.9749	0.0153

Table 9 Information entropy values (*H*) of encrypted image

	Thorax (256 × 256)	Phalanges (512 × 512)	Combined images (512 × 512)
Information entropy (<i>H</i>)	7.9992	7.9992	7.9993

Fig. 25 Decipher images with Gaussian noise. **a** var = 0.4, **b** var = 0.7, **c** var = 0.9

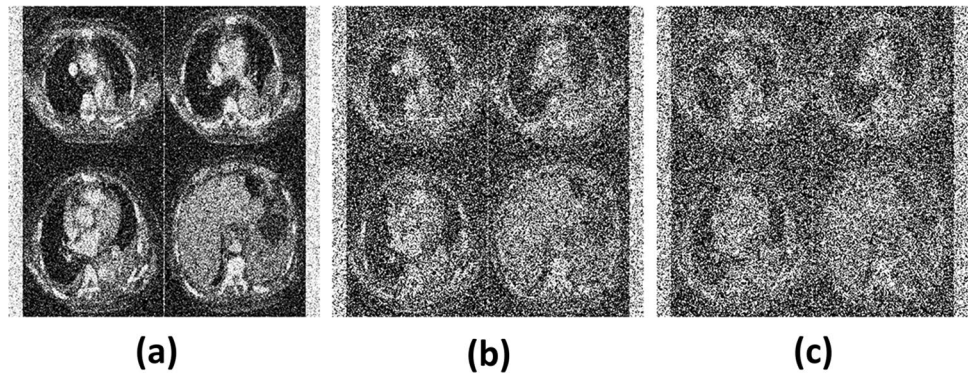


Table 10 Comparison of the proposed algorithm metrics with recent contribution in the literature

(Year) refs	Image type	System type	Key space	Entropy	NPCR (%)	UACI (%)
This work	Medical image Thorax (256 × 256)	4D Chua oscillator system	2^{630}	7.9992	99.6261	33.4688
(2020) [50]	Normal image Lena (256 × 256)	2D Lorenz and logistic map	2^{336}	7.9894	99.66	33.42
(2020) [51]	Medical image DICOM (256 × 256)	3D Lorenz and logistic map	2^{714}	7.998	99.68	33.47
(2021) [52]	Normal image Lena (256 × 256)	Chen hyperchaotic system	2^{512}	7.9939	99.54	34.25
(2021) [53]	Normal image Lena (256 × 256)	4D Lorenz hyperchaotic system	4.4607×2^{153}	7.9993	99.6142	33.4536
(2022) [44]	Medical image Chest (256 × 256)	Initial-boosted hyperchaotic HNN	2^{480}	7.9979	99.6104	33.4662
(2022) [45]	Medical image Lung (256 × 256)	5D MRNN	2^{336}	7.9978	99.6299	33.6548

7 Conclusion

In this paper, a novel memristive Chua circuit is proposed and used as a chaos-based encryption scheme for biomedical image security. It is demonstrated that the novel memristive oscillator can develop complex behaviors like: (i) period doubling and intermittency routes to chaos; (ii) multistability or coexisting of different attractors for the same set of oscillator parameters; and (iii) spiking and bursting oscillations. An Arduino-based embedding of the oscillator confirms these dynamics. We used the chaotic attractor data along with system parameters to generate a secret key for the encryption scheme. The chaotic data passed the NIST test SP 800–22 Rev. 1a proved that they are pseudorandom enough to be used for cryptography application. Security tests of brute force attack and differential attack are demonstrated to be inefficient to our proposed cryptosystem. Other tests like variance of histogram, correlation analysis, and entropy results attested that those statistical attacks failed since the algorithm exhibits excellent

statistical properties of the designed maps. Moreover, the encryption/decryption average NPCR and UACI values obtained by the proposed scheme are compared with recent and good-standing contributions: They are among the best in the literature. Therefore, these results suggest that the medical image encryption scheme based on Chua's chaotic memristive oscillator system can resist entropy and statistical and differential attacks more effectively. Therefore, it can be applied to protect biomedical images in real-time information communication systems.

Funding SIDA (the Swedish International Development Cooperation Agency) through ISP (the International Science Programme, Uppsala University) is acknowledged by Mr. Alain Djomo Fanda for financial support in the form of a PhD scholarship scheme.

Data Availability Statement The data generated during the current study will be made available at reasonable request.

Declarations

Conflicts of Interest The authors declare no competing interests.

References

1. B. Blasius, A. Huppert, L. Stone, Complex dynamics and phase synchronization in spatially extended ecological systems. *Nature* **399**(6734), 354–359 (1999)
2. D.W. Graham et al., Experimental demonstration of chaotic instability in biological nitrification. *ISME J.* **1**(5), 385–393 (2007)
3. R. Matthews, On the derivation of a “chaotic” encryption algorithm. *Cryptologia* **13**(1), 29–42 (1989)
4. T. Yang, C.W. Wu, L.O. Chua, Cryptography based on chaotic systems. *IEEE Trans. Circuits Syst. I Fundam. Theory Appl.* **44**(5), 469–472 (1997)
5. R. He, P. Vaidya, Implementation of chaotic cryptography with chaotic synchronization. *Phys. Rev. E* **57**(2), 1532 (1998)
6. L. Kocarev, S. Lian, *Chaos-based cryptography: theory, algorithms and applications*. Vol. 354. (2011) Springer Science & Business Media.
7. G. Makris, I. Antoniou, Cryptography with chaos. In *Proceedings of the 5th Chaotic Modeling and Simulation International Conference*, Athens, Greece. (2012)
8. R. Ebrahimzadeh, M. Jampour, Chaotic genetic algorithm based on Lorenz chaotic system for optimization problems. *Int. J. Intell. Syst. Appl.* **5**(5), 19 (2013)
9. K. Rajagopal et al., Analysis and electronic implementation of an absolute memristor autonomous Van der Pol-Duffing circuit. *Eur. Phys. J. Spec. Top.* **228**(10), 2287–2299 (2019)
10. G.F. Kuiate et al., Autonomous Van der Pol-Duffing snap oscillator: analysis, synchronization and applications to real-time image encryption. *Int. J. Dyn. Control* **6**(3), 1008–1022 (2018)
11. S. Vaidyanathan et al., A new 4-D chaotic hyperjerk system, its synchronization, circuit design and applications in RNG, image encryption and chaos-based steganography. *Eur. Phys. J. Plus* **133**(2), 1–18 (2018)
12. Z. Lin, H. Wang, Efficient image encryption using a chaos-based PWL memristor. *IETE Tech. Rev.* **27**(4), 318–325 (2010)
13. B.-C. Bao et al., Chaotic memristive circuit: equivalent circuit realization and dynamical analysis. *Chin. Phys. B* **20**(12), 120502 (2011)
14. B. Muthuswamy, Implementing memristor based chaotic circuits. *Int. J. Bifurcat. Chaos* **20**(05), 1335–1350 (2010)
15. B. Bao et al., Coexistence of multiple bifurcation modes in memristive diode-bridge-based canonical Chua’s circuit. *Int. J. Electron.* **105**(7), 1159–1169 (2018)
16. P. Liu, H. Chu, B.-C. Zheng, Robust sliding mode controller design of memristive Chua’s circuit systems. *AIP Adv.* **12**(2), 025207 (2022)
17. L.O. Chua, Chua circuit. *Scholarpedia* **2**(10), 1488 (2007)
18. M. Ghebleh, A. Kanso, H. Noura, An image encryption scheme based on irregularly decimated chaotic maps. *Signal Process. Image Commun.* **29**(5), 618–627 (2014)
19. P. Sarosh, S.A. Parah, G.M. Bhat, An efficient image encryption scheme for healthcare applications. *Multimed. Tools Appl.* **81**(5), 7253–7270 (2022)
20. M. Ashtiyani, P.M. Birgani, H.M. Hosseini, Chaos-based medical image encryption using symmetric cryptography. *Int. Conf. Inf. Commun. Technol. Theory Appl.* IEEE (2008)
21. Jebril, N., World Health Organization declared a pandemic public health menace: a systematic review of the coronavirus disease, COVID-19. Available at SSRN **3566298**, 2020 (2019)
22. H. Liu et al., Clinical and CT imaging features of the COVID-19 pneumonia: focus on pregnant women and children. *J. Infect.* **80**(5), e7–e13 (2020)
23. X. Wang, L. Teng, X. Qin, A novel colour image encryption algorithm based on chaos. *Signal Process.* **92**(4), 1101–1108 (2012)
24. Y. Luo et al., An efficient and self-adapting colour-image encryption algorithm based on chaos and interactions among multiple layers. *Multimed. Tools Appl.* **77**(20), 26191–26217 (2018)
25. M. Roy et al., A study on the applications of the biomedical image encryption methods for secured computer aided diagnostics. *Amity Int. Conf. Artif. Intell. (AICAI)*. IEEE (2019)
26. H. Nematzadeh et al., Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. *Opt. Lasers Eng.* **110**, 24–32 (2018)
27. K. Mali, S. Chakraborty, M. Roy, A study on statistical analysis and security evaluation parameters in image encryption. *Entropy* **34**, 36 (2015)
28. P. Kavitha, P.V. Saraswathi, A survey on medical image encryption. *Int. Conf. Appl. Soft Comput. Tech. Int. J. Sci. Res. Sci. Technol.* (2019)
29. A. Umamageswari, M.F. Ukrit, G. Suresh, A survey on security in medical image communication. *Int. J. Comput. Appl.* **30**(3), 41–45 (2011)
30. X. Zhang, X. Wang, Multiple-image encryption algorithm based on DNA encoding and chaotic system. *Multimed. Tools Appl.* **78**(6), 7841–7869 (2019)
31. S. Pan, J. Wei, S. Hu, A novel image encryption algorithm based on hybrid chaotic mapping and intelligent learning in financial security system. *Multimed. Tools Appl.* **79**(13), 9163–9176 (2020)
32. B. Bouteghrine, C. Tanougast, S. Sadoudi, Novel image encryption algorithm based on new 3-d chaos map. *Multimed. Tools Appl.* **80**(17), 25583–25605 (2021)
33. J. Tian et al., A novel image encryption algorithm using PWLCM map-based CML chaotic system and dynamic DNA encryption. *Multimed. Tools Appl.* **80**(21), 32841–32861 (2021)
34. Y. Shi et al., Multiple-image double-encryption via 2D rotations of a random phase mask with spatially incoherent illumination. *Opt. Express* **27**(18), 26050–26059 (2019)
35. W.-H. Chen, S. Luo, W.X. Zheng, Impulsive synchronization of reaction–diffusion neural networks with mixed delays and its application to image encryption. *IEEE Trans. Neural Netw. Learn. Syst.* **27**(12), 2696–2710 (2016)
36. L. Kamdjeu Kengne et al., Image encryption using a novel quintic jerk circuit with adjustable symmetry. *Int. J. Circuit Theory Appl.* **49**(5), 1470–1501 (2021)
37. C. Wu et al., Asymmetric encryption of multiple-image based on compressed sensing and phase-truncation in cylindrical diffraction domain. *Opt. Commun.* **431**, 203–209 (2019)
38. R. Hamza et al., Hash based encryption for keyframes of diagnostic hysteroscopy. *IEEE Access* **6**, 60160–60170 (2017)
39. M. Jridi, A. Alfalou, Real-time and encryption efficiency improvements of simultaneous fusion, compression and encryption method based on chaotic generators. *Opt. Lasers Eng.* **102**, 59–69 (2018)
40. Y. Mao, G. Chen, Chaos-based image encryption. In *Handbook of geometric computing*. (Springer, 2005), pp.231–265
41. Z.T. Njitacke et al., Window of multistability and its control in a simple 3D Hopfield neural network: application to biomedical image encryption. *Neural Comput. Appl.* **33**(12), 6733–6752 (2021)
42. I.S. Doubla et al., Multistability and circuit implementation of tabu learning two-neuron model: application to secure biomedical images in IoMT. *Neural Comput. Appl.* **33**(21), 14945–14973 (2021)
43. C. Zhou et al., Observer-based synchronization of memristive neural networks under DoS attacks and actuator saturation and its application to image encryption. *Appl. Math. Comput.* **425**, 127080 (2022)
44. H. Lin et al., Brain-like initial-boosted hyperchaos and application in biomedical image encryption. *IEEE Transact. Industr. Inform.* (2022)

45. H. Lin et al., Hyperchaotic memristive ring neural network and application in medical image encryption. *Nonlinear Dyn.* **110**(1), 841–855 (2022)
46. F. Yu et al., Complex dynamics, hardware implementation and image encryption application of multiscroll memristive hopfield neural network with a novel local active memristor. *IEEE Trans. Circuits Syst. II Express Briefs* **70**(1), 326–330 (2022)
47. S. Stalin et al., Fast and secure medical image encryption based on non linear 4D logistic map and DNA sequences (NL4DLM_DNA). *J. Med. Syst.* **43**(8), 1–17 (2019)
48. H. Liu, X. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Opt. Commun.* **284**(16–17), 3895–3903 (2011)
49. H. Lin et al., An extremely simple multiwing chaotic system: dynamics analysis, encryption application, and hardware implementation. *IEEE Trans. Industr. Electron.* **68**(12), 12708–12719 (2020)
50. T. Li, B. Du, X. Liang, Image encryption algorithm based on logistic and two-dimensional lorenz. *IEEE Access* **8**, 13792–13805 (2020)
51. A. Banu S, R. Amirtharajan, A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach. *Med. Biol. Eng. Comput.* **58**(7), 1445–1458 (2020)
52. X. Wang, M. Zhao, An image encryption algorithm based on hyperchaotic system and DNA coding. *Opt. Laser Technol.* **143**, 107316 (2021)
53. R. Lin, S. Li, An image encryption scheme based on Lorenz hyperchaotic system and RSA algorithm. *Secur. Commun. Netw.* (2021)
54. M. Kaur et al., Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map. *Futur. Gener. Comput. Syst.* **107**, 333–350 (2020)
55. X. Zhang et al., An image encryption algorithm based on hyperchaotic system and genetic algorithm. *Int. Conf. Bio-Inspir. Comput. Theories Appl.* (2018). Springer
56. Y. Niu, X. Zhang, F. Han, Image encryption algorithm based on hyperchaotic maps and nucleotide sequences database. *Comput. Intell. Neurosci.* (2017)
57. M. Xu, Z. Tian, Security analysis of a novel fusion encryption algorithm based on dna sequence operation and hyper-chaotic system. *Optik* **134**, 45–52 (2017)
58. T. Wang, M.-H. Wang, Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding. *Opt. Laser Technol.* **132**, 106355 (2020)
59. S. Sun, A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling. *IEEE Photonics J.* **10**(2), 1–14 (2018)
60. Y.-Q. Zhang, X.-Y. Wang, A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. *Inf. Sci.* **273**, 329–351 (2014)
61. Y. Abanda, A. Tiedeu, Image encryption by chaos mixing. *IET Image Proc.* **10**(10), 742–750 (2016)
62. L.M. Heucheun Yepdia, A. Tiedeu, G. Kom, A robust and fast image encryption scheme based on a mixing technique. *Secur. Commun. Netw.* (2021)
63. S.-S. Yu et al., Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system. *Opt. Lasers Eng.* **124**, 105816 (2020)
64. Z.-H. Guan, F. Huang, W. Guan, Chaos-based image encryption algorithm. *Phys. Lett. A* **346**(1–3), 153–157 (2005)
65. S. El Assad, M. Farajallah, A new chaos-based image encryption system. *Signal Process. Image Commun.* **41**, 144–157 (2016)
66. P. Louodop et al., Finite-time synchronization of tunnel-diode-based chaotic oscillators. *Phys. Rev. E* **89**(3), 032921 (2014)
67. B. Xu et al., A memristor–meminductor-based chaotic system with abundant dynamical behaviors. *Nonlinear Dyn.* **96**(1), 765–788 (2019)
68. S.H. Strogatz, *Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering*. 2015: Second edition. Boulder, CO: Westview Press, a member of the Perseus Books Group (2015).
69. R.C. Hilborn, *Chaos and nonlinear dynamics: an introduction for scientists and engineers*. Oxford University Press on Demand (2000)
70. J. Awrejcewicz, *Bifurcation and chaos: theory and applications*. Springer Science & Business Media (2012)
71. W. Marszalek, H. Podhaisky, J. Sadecki, Computing two-parameter bifurcation diagrams for oscillating circuits and systems. *IEEE Access* **7**, 115829–115835 (2019)
72. A. Wolf et al., Determining Lyapunov exponents from a time series. *Physica D* **16**(3), 285–317 (1985)
73. L.K. Kengne et al., Dynamics, control and symmetry breaking aspects of a single opamp-based autonomous LC oscillator. *AEU-Int. J. Electron. Commun.* **118**, 153146 (2020)
74. G.J. Kitio et al., Four-scroll hyperchaotic attractor in a five-dimensional memristive Wien bridge oscillator: analysis and digital electronic implementation. *Math. Probl. Eng.* (2021)
75. J. Kengne, A.N. Negou, D. Tchiotso, Antimonotonicity, chaos and multiple attractors in a novel autonomous memristor-based jerk circuit. *Nonlinear Dyn.* **88**(4), 2589–2608 (2017)
76. A.N. Pisarchik, U. Feudel, Control of multistability. *Phys. Rep.* **540**(4), 167–218 (2014)
77. P.-H. Shen, S.-W. Lin, Mathematic modeling and characteristic analysis for dynamic system with asymmetrical hysteresis in vibratory compaction. *Meccanica* **43**(5), 505–515 (2008)
78. D. Angeli, J.E. Ferrell, E.D. Sontag, Detection of multistability, bifurcations, and hysteresis in a large class of biological positive-feedback systems. *Proc. Natl. Acad. Sci.* **101**(7), 1822–1827 (2004)
79. E. Ott, *Chaos in dynamical systems*. Cambridge university press (2002)
80. Y. Pomeau, P. Manneville, Intermittent transition to turbulence in dissipative dynamical systems. *Commun. Math. Phys.* **74**(2), 189–197 (1980)
81. A. Taher Azar et al., Multistability analysis and function projective synchronization in relay coupled oscillators. *Complexity* (2018)
82. B. Bao et al., Multistability in Chua's circuit with two stable node-foci. *Chaos Interdiscip. J. Nonlinear Sci.* **26**(4), 043111 (2016)
83. F.F. Kemwoue et al., Bifurcation, multistability in the dynamics of tumor growth and electronic simulations by the use of Pspice. *Chaos Solitons Fractals* **134**, 109689 (2020)
84. B. Ramakrishnan et al., Image encryption with a Josephson junction model embedded in FPGA. *Multimed. Tools Appl.* 1–25 (2022)
85. J.S. Kelso, Multistability and metastability: understanding dynamic coordination in the brain. *Philos. Trans. R. Soc. B Biol. Sci.* **367**(1591), 906–918 (2012)
86. P.Y. Yu, G. Craciun, Mathematical analysis of chemical reaction systems. *Isr. J. Chem.* **58**(6–7), 733–741 (2018)
87. A. Namajunas, A. Tamasevicius, Modified Wien-bridge oscillator for chaos. *Electron. Lett.* **31**(5), 335–336 (1995)
88. M.P. Kennedy, Chaos in the Colpitts oscillator. *IEEE Trans. Circuits Syst. I Fundam. Theory Appl.* **41**(11), 771–774 (1994)
89. D.G. Taylor, Nonlinear control of electric machines: an overview. *IEEE Control Syst. Mag.* **14**(6), 41–51 (1994)
90. G.B. Ermentrout, N. Kopell, Parabolic bursting in an excitable system coupled with a slow oscillation. *SIAM J. Appl. Math.* **46**(2), 233–253 (1986)
91. G.E. Ha, E. Cheong, Spike frequency adaptation in neurons of the central nervous system. *Exp. Neurobiol.* **26**(4), 179 (2017)
92. A.S. Kemnang Tsafack et al., Coexisting attractors and bursting oscillations in IFOC of 3-phase induction motor. *Eur. Phys. J. Spec. Top.* **229**(6), 989–1006 (2020)
93. E.M. Izhikevich, *Bursting*. Scholarpedia **1**(3), 1300 (2006)
94. W. Diffie, M. Hellman, New directions in cryptography. *IEEE Trans. Inf. Theory* **22**(6), 644–654 (1976)

95. A. Bakshi, A.K. Patel, Secure telemedicine using RONI half-toned visual cryptography without pixel expansion. *Journal of Information Security and Applications* **46**, 281–295 (2019)
96. J.C. Sprott, A proposed standard for the publication of new chaotic systems. *Int. J. Bifurcat. Chaos* **21**(09), 2391–2394 (2011)
97. L.M.H. Yepdia, A. Tiedeu, Secure transmission of medical image for telemedicine. *Sens. Imaging* **22**(1), 1–31 (2021)
98. M. Madani, Y. Bentoutou, Cryptage d'images médicales à la base des cartes chaotiques. *Int. Conf. Colloque Tassili SCCIBOV* (2015)
99. A. Rukhin et al., A statistical test suite for random and pseudorandom number generators for cryptographic applications. *Booz-allen and hamilton inc mclean va.* (2001)
100. P. Peris-Lopez et al., LAMED—a PRNG for EPC class-1 generation-2 RFID specification. *Comput. Stand. Interfaces* **31**(1), 88–97 (2009)
101. Q. Zhang et al., Image encryption method based on discrete Lorenz chaotic sequences. *J. Inf. Hiding Multim. Signal Process.* **7**(3), 576–586 (2016)
102. T. Tuncer et al., Implementation of non-periodic sampling true random number generator on FPGA. *Informacije Midem* **44**(4), 296–302 (2014)
103. M. Xu, Z. Tian, A novel image encryption algorithm based on self-orthogonal Latin squares. *Optik* **171**, 891–903 (2018)
104. K. Zhan et al., Cross-utilizing hyperchaotic and DNA sequences for image encryption. *J. Electron. Imaging* **26**(1), 013021 (2017)
105. Y. Zhang, D. Xiao, An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. *Commun. Nonlinear Sci. Numer. Simul.* **19**(1), 74–82 (2014)
106. F.E. Abd El-Samie, *Image encryption: a communication perspective.* CRC Press. (2019)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.