scientific reports

Check for updates

OPEN

A comprehensive study of the novel 4D hyperchaotic system with self-exited multistability and application in the voice encryption

Khaled Benkouider[1], Aceng Sambas[2,3], Talal Bonny[4], Wafaa Al Nassan[4], Issam A. R. Moghrabi[5,6]✉, Ibrahim Mohammed Sulaiman[7,8], Basim A. Hassan[9] & Mustafa Mamat[10]

This paper describes a novel 4-D hyperchaotic system with a high level of complexity. It can produce chaotic, hyperchaotic, periodic, and quasi-periodic behaviors by adjusting its parameters. The study showed that the new system experienced the famous dynamical property of multistability. It can exhibit different coexisting attractors for the same parameter values. Furthermore, by using Lyapunov exponents, bifurcation diagram, equilibrium points' stability, dissipativity, and phase plots, the study was able to investigate the dynamical features of the proposed system. The mathematical model's feasibility is proved by applying the corresponding electronic circuit using Multisim software. The study also reveals an interesting and special feature of the system's offset boosting control. Therefore, the new 4D system is very desirable to use in Chaos-based applications due to its hyperchaotic behavior, multistability, offset boosting property, and easily implementable electronic circuit. Then, the study presents a voice encryption scheme that employs the characteristics of the proposed hyperchaotic system to encrypt a voice signal. The new encryption system is implemented on MATLAB (R2023) to simulate the research findings. Numerous tests are used to measure the efficiency of the developed encryption system against attacks, such as histogram analysis, percent residual deviation (PRD), signal-to-noise ratio (SNR), correlation coefficient (cc), key sensitivity, and NIST randomness test. The simulation findings show how effective our proposed encryption system is and how resilient it is to different cryptographic assaults.

Keywords Chaos, Bifurcation, Hyperchaos, Electronic circuit and voice encryption

After the seminal work of Lorenz, the construction of models and implementation of circuits for chaotic systems have emerged as an intriguing area of research, driven by the significant potential of chaotic systems in various engineering applications, particularly in secure communications. In terms of Lyapunov exponents, high-dimensional 4D hyperchaos dynamical systems with two positive Lyapunov exponents can produce more unpredictable and complex random signals than 3D chaotic systems, which improves the security of chaos-based communication systems. Consequently, the literature has reported numerous 4-D hyperchaos systems with two positive Lyapunov exponents[1,2].

[1]Department of Electronics, Faculty of Technology, Badji-Mokhtar University, B.P. 12, Sidi Ammar, Annaba, Algeria. [2]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin (UniSZA), Besut Campus, 22200 Besut, Malaysia. [3]Department of Mechanical Engineering, Universitas Muhammadiyah Tasikmalaya, Tasikmalaya 46196, Indonesia. [4]Department of Computer Engineering, University of Sharjah, Sharjah, United Arab Emirates. [5]Computer Science Department, School of Arts and Sciences, University of Central Asia, Naryn, Kyrgyz Republic. [6]Department of Information Systems and Technology, Kuwait Technical College, Kuwait city, Kuwait. [7]Institute of Strategic Industrial Decision Modelling (ISIDM), School of Quantitative Sciences, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia. [8]Faculty of Education and Arts, Sohar University, Sohar 311, Oman. [9]College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq. [10]University College Bestari Putera Jaya, Setiu, 22100 Permaisuri, Terengganu, Malaysia. ✉email: issam.moughrabi@ucentralasia.org

In addition, the existence of multistability phenomenon in certain chaotic systems is very interesting. Multistability or the presence of different coexisting attractors for a given set of system parameters allows the system to behave with a high degree of flexibility and this has recently become a fundamental research topic explored by various researchers. For instance, studies by[3,4] recently investigated some chaotic systems with multistability. Furthermore, a chaotic system that allows for free offset boosting control is attractive for engineering and industrial applications. A prospective chaotic system's offset boosting control is a crucial component that makes converting a bipolar signal to a unipolar signal or vice versa very helpful. Many studies have been conducted recently on chaotic systems with offset boosting control[5,6]. Therefore, developing a new system with multiple positive Lyapunov exponents, multistability and offset boosting is a challenging, interesting, and very demanding task. Chaotic systems are known for their intricate and unpredictable behavior, making them suitable for generating cryptographic keys and enhancing encryption algorithms[7,8]. Therefore, chaotic systems have been used intensively to improve the security of different information formations, images, voices, and videos. Integrating a chaotic system with encryption systems increases the complexity and makes it more difficult for attackers to decrypt data[9–13].

Numerous studies delve into hyperchaotic systems, such as the work by Xu et al.[14], who by featuring torus attractors was able to introduce a novel 4D hyperchaotic system and further demonstrated the presence of the maximum of two positive Lyapunov exponents. In a related vein, Hui et al.[15] proposed an intricate four-dimensional hyperchaotic system exhibiting a larger key space and more complex dynamic behaviors. Their application extended to image encryption via the hyperchaotic sequence and Secure Hash Algorithm-512 (SHA-512) functions. Fu et al.[16] developed a 4D hyperchaotic system derived from a 3D Lü chaotic system's foundation. This system found application in audio encryption employing a cross-XOR algorithm, implemented on the platform of STM32 embedded hardware. Li et al.[17] introduced a 4D hyperchaotic system incorporating certain exponential term. They explored synchronization issues using an adaptive control law having two inputs. Yang et al.[18] presented a sequential architecture that converts 3D quadratic system into a basic 6D hyperchaotic system with complex dynamics using linear control. Notably, when the system had a single equilibrium line, they found that at least seven distinct attractors coexisted. Jiang et al.[19] put forth a brand-new TDCS that exhibits hyperchaotic behavior over the whole parameter range. Their method involved fusing SVD, BP, and the recently created TDCS to create an image cryptosystem with aesthetic significance. Meanwhile, Gu et al.[20] introduced a novel conservative hyperchaotic system that is non-Hamiltonian in four dimensions. They compared the time sequences produced by the system with previously published works using a complexity analysis of the study. Kong et al.[21] introduced a novel 5D FOD memristive HNN (FOMHNN) framework aimed at simulating a neuron's autapse and clarifying electromagnetic induction resulting from electromagnetic radiation. Additionally, they developed a secure image encryption scheme that reduces memory overhead and simplifies hardware implementation significantly. On the other hand, Yu et al.[22] designed three distinct memristive HNNs, including a 4D memristive synapse weight HNN, and designed an image encryption circuit to allow FPGA to directly encrypt images and transmit them to the IO device.

The main contribution and novelty of this paper is proposing a new 4D dynamical system with two positive Lyapunov exponents, multistability and offset boosting. Dynamical properties of the proposed scheme are studied using LEs, bifurcation diagrams, phase plots, and stability analysis. Different coexisting attractors are displayed. An equivalent electrical circuit is designed using Multisim to validate the proposed system's feasibility. Finally, offset boosting control is achieved and shown using numerical plots. Moreover, it demonstrates the effectiveness of the properties of the proposed system, which is helpful for chaos-based applications. The paper introduces a novel voice encryption system using the new hyperchaotic system for encrypting voice signals. Then, various tests were applied to determine how effectively the encryption system responded against attacks, including histogram analysis, percent residual deviation (PRD), signal-to-noise ratio (SNR), correlation coefficient (CC), key sensitivity, and NIST randomness test.

A new 4D hyperchaotic system

The new 4D hyperchaotic system is defined by the algebraic equations that follows:

$$\begin{cases} \dot{x} = ax - yz + w \\ \dot{y} = xz - by \\ \dot{z} = xy - cz \\ \dot{w} = -y + d \end{cases} \tag{1}$$

where the parameters *a, b, c, d* denotes positive constant and *x, y, z, w,* define the state variables. This study aim to establish that system (1) is hyperchaotic by taking the initial state as $[10,1,10,1]^{T}$ and parameters as $a = 8$, $b = 40$, $c = 15$, $d = -0.1$. In Fig. 1, we generate the hyperchaotic attractors of system (1) using the MATLAB ode45 function.

By choosing system (1)'s previous parameter values, the corresponding Lyapunov exponents are calculated using Wolf's algorithm[23] incorporated in MATLAB as:

$$\begin{cases} LE_1 = 3.036 \\ LE_2 = 0.010 \\ LE_3 = 0 \\ LE_4 = -50.032 \end{cases} \tag{2}$$

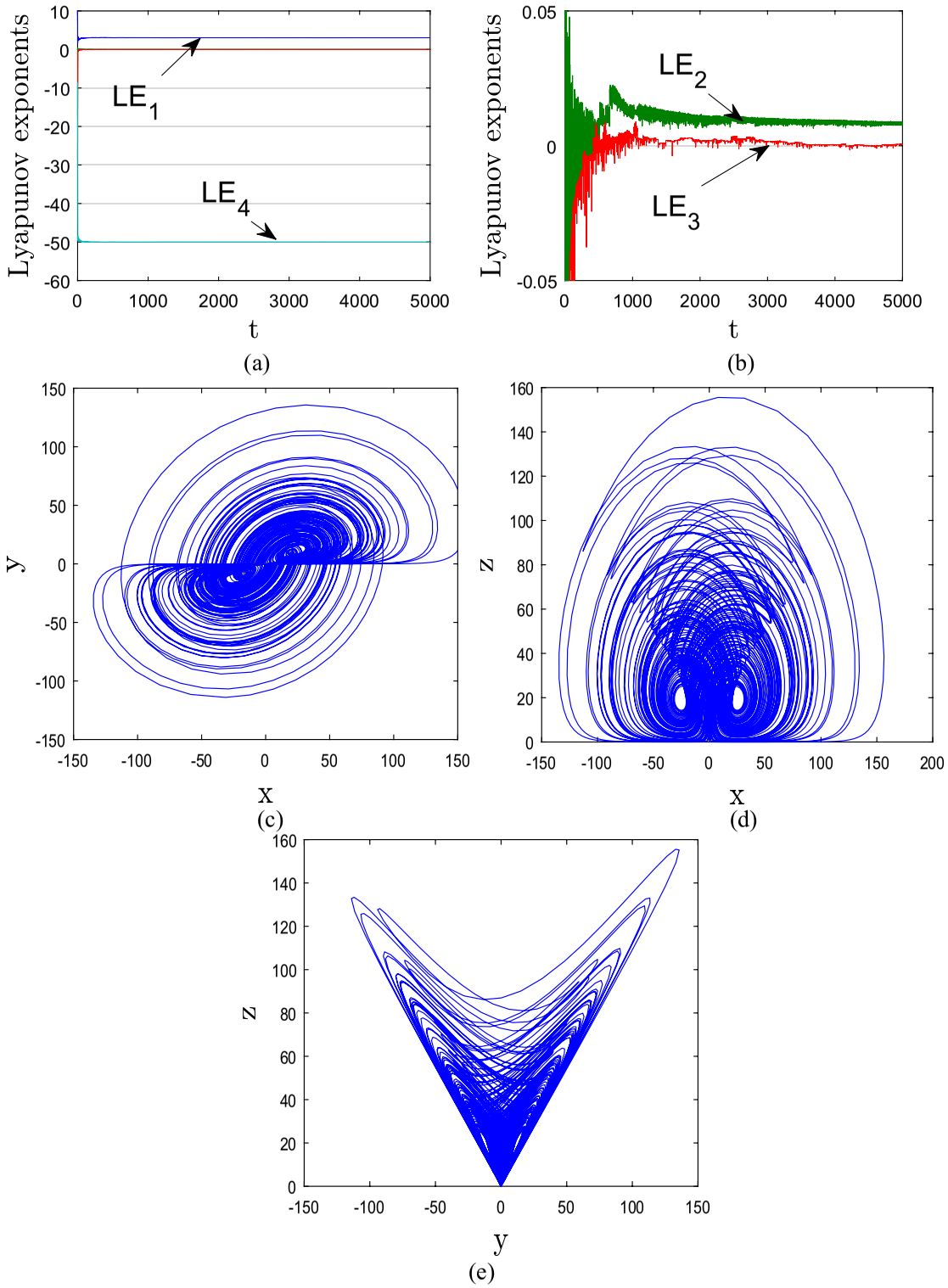


Figure 1. Lyapunov exponents and hyperchaotic attractors of the proposed system (1) for a = 8, b = 40, c = 15, and d = − 0.1

From (2), System (1) has: $LE_{1,2} > 0$, $LE_3 = 0$, $LE_4 < 0$ as depicted in Fig. 1 implying that the system exhibits a hyperchaotic behaviour with two positive Lyapunov exponents, one zero Lyapunov exponents, and one negative Lyapunov exponent. Also, we note that the sum of the Lyapunov exponents is negative, confirming that the proposed 4D system (1) is dissipative.

According to the chaos theory, a high value of Kaplan–Yorke dimension directly corresponds to high complexity of system dynamics. The corresponding Kaplan-Yorke dimension for the suggested system (1) is computed as follows:

$$D_{KY} = 3 + \frac{LE_1 + LE_2 + LE_3}{|LE_4|} = 3.061 \tag{3}$$

The fractional nature of the Kaplan-Yorke dimension is seen from Eq. (3). Thus, the new 4D system (1) produces intricate hyperchaotic attractors. This section will examine the effects of the parameters and initial conditions on the complexity and features of system (1).

System (1) has two equilibrium points; they are obtained as the following:

$$\begin{aligned} E_1 &= \left[\frac{c}{d}\sqrt{\frac{bd^2}{c}},\ d,\ \sqrt{\frac{bd^2}{c}},\ \left(1-\frac{ac}{d}\right)\sqrt{\frac{bd^2}{c}}\right] \\ E_2 &= \left[-\frac{c}{d}\sqrt{\frac{bd^2}{c}},\ d,\ -\sqrt{\frac{bd^2}{c}},\ \left(\frac{ac}{d}-1\right)\sqrt{\frac{bd^2}{c}}\right] \end{aligned} \tag{4}$$

By examining the eigenvalues of the Jacobian matrix J_{E_i}, the study was able to investigate the stability of the new system (1) at the two equilibrium positions. All equilibrium points are unstable, as Table 1 demonstrates. Therefore, it follows that the 4D system is a member of the self-excited family.

Dynamical analysis of the new 4D hyperchaotic system

Bifurcation analysis

This section examines the dynamic characteristics of the 4D hyperchaotic system (1) versus the control parameter c using phase graphs, bifurcation diagrams, and Lyapunov exponents spectra. Figures 2a and b show the Lyapunov exponents spectrum and the bifurcation diagram of the new system, respectively, when the parameters a, b, and d are fixed at $a = 8$, $b = 40$, and $d = -0.1$, while the control parameter c is adjusted in the range[7,15].

When $7 < c < 8$, system (1) has no positive Lyapunov exponent implying that the system exhibits periodic behaviour as shown in Fig. 3a for $c = 7$. The corresponding *LEs* are: $LE_1 = 0$, $LE_2 = -0.078$, $LE_3 = -2.202$, $LE_4 = -36.719$.

When $8 < c < 9$, system (1) has exhibits quasi-periodic behaviour as demonstrated in Fig. 3b for $c = 8.4$. The corresponding *LEs* are: $LE_1 = 0$, $LE_2 = 0$, $LE_3 = -0.484$, $LE_4 = -39.916$.

When $9 < c < 10$, system (1) exhibits chaotic behaviour with one positive LE as depicted in Fig. 3c for $c = 9.4$. The corresponding *LEs* are: $LE_1 = 0.847$, $LE_2 = 0$, $LE_3 = -0.073$, $LE_4 = -42.171$.

When $10 < c < 15$, system (1) has two positive Lyapunov exponents implying that the system exhibits hyperchaotic behavior as presented in Fig. 3d for $c = 14$. The corresponding *LEs* are: $LE_1 = 2.818$, $LE_2 = 0.012$, $LE_3 = 0$, $LE_4 = -48.810$.

Coexisting attractors

For varying parameter values, the 4D system (1) exhibits the coexistence of one periodic attractor and one chaotic attractor, the coexistence of two hyperchaotic attractors, or the coexistence of two chaotic attractors, as demonstrated by the coexisting bifurcation diagram, basin of attraction, and phase plots. Assume that $Y_{01} = (1, 1, 1, 1)$ and $Y_{02} = (10, 1, 10, 1)$ are two distinct starting points for the new 4D system (1). We will use blue for the state orbit associated with Y_{01} and red for the state orbit associated with Y_{02}. Figure 4a illustrates the bifurcation diagram of system (1) versus parameters c, calculated and plotted starting from Y_{01} and Y_{02}, showing that the new system can generate coexisting attractors. Additionally, Fig. 4b illustrates the basin of attraction for system (1) plotted in the $x(0)$-$z(0)$ plane, highlighting regions associated with distinct behaviors. The blue region represents the basin of attraction for periodic behavior, where trajectories converge to periodic orbits, while the red regions denote areas where chaotic dynamics emerge.

Adjusting the values of $a = 8$, $b = 40$, $c = 7$, and $d = -0.1$, as seen in Fig. 4c, the 4D system (1) exhibits the coexistence of one chaotic attractor and one periodic attractor. Setting $a = 8$, $b = 40$, $c = 9.4$, and $d = -0.1$ as the parameters, as shown in Fig. 4d, the 4D system (1) exhibits two coexisting chaotic attractors. Further adjusting the values to $a = 8$, $b = 40$, $c = 10$, and $d = -0.1$, as depicted in Fig. 4e, the 4D system (1) exhibits two coexisting hyperchaotic attractors.

Offset boosting control

Since the fourth variable of system (1), w appears just in the first equation, the proposed 4-D scheme is a variable-boosting hyperchaotic system with controlled w. As a result, w can be boosted by replacing w with $(w + k)$. System (1)'s first differential equation can be rewritten as follows:

$$\dot{x} = ax - yz + (w + k) \tag{5}$$

E_i	J_{Ei} eigenvalues	Stability
E_1	$\lambda_1 = -54.995$, $\lambda_2 = 7.995$, $\lambda_3 = 0.105$, $\lambda_4 = -0.105$	Unstable
E_2	$\lambda_1 = -54.995$, $\lambda_2 = 7.995$, $\lambda_{3,4} = 0.001 + -0.105i$	Unstable

Table 1. Eigen value of the new 4d hyperchaotic system.

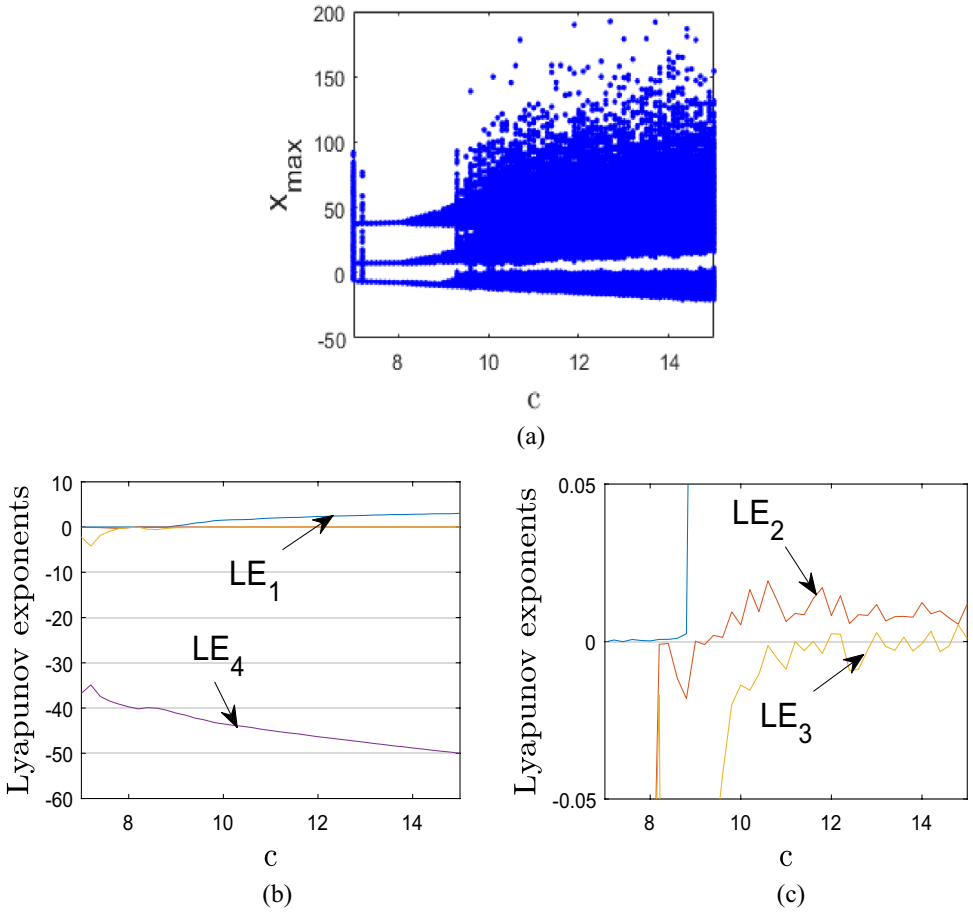


Figure 2. Graphical presentation of bifurcation and LEs spectrum of system (1) for specific interval of the control parameter c.

where k is a controller for offset boosting. Figure 5 depicts several positions of hyperchaotic attractors boosted on different k in the x–y plane. For a positive value of k, the attractors are boosted in the negative direction while for a negative value of k, the attractors are boosted in the positive direction. This special property has a numerous application in chaos-based cryptography and other engineering domains[24–27]

Circuit design

Multisim software is used to implement the analog circuit of the proposed 4D hyperchaotic system (1). Figure 6 displays the circuit schematic of the 4D hyperchaotic system. The circuit used in this study includes linear resistors, capacitors, an operational amplifier (TL082CD), and a multiplier (AD633). A power supply of ± 15 V is used. Circuit functions including addition, subtraction, and integration are performed by the operational amplifier. In the meantime, the multiplier unifies the four state variables into a coherent whole while capturing the nonlinearity of the system.

The following corresponding circuital equations of proposed scheme (1) is derived by applying Kirchhoff's laws to the circuit in Fig. 6, where:

$$\begin{cases} \dot{x} = \frac{1}{R_1C_1}x - \frac{1}{R_2C_1}yz + \frac{1}{R_3C_1}w \\ \dot{y} = \frac{1}{R_4C_2}xz - \frac{1}{R_5C_2}y \\ \dot{z} = \frac{1}{R_6C_3}xy - \frac{1}{R_7C_3}z \\ \dot{w} = -\frac{1}{R_8C_4}y - \frac{1}{R_7C_4}V_1 \end{cases} \tag{6}$$

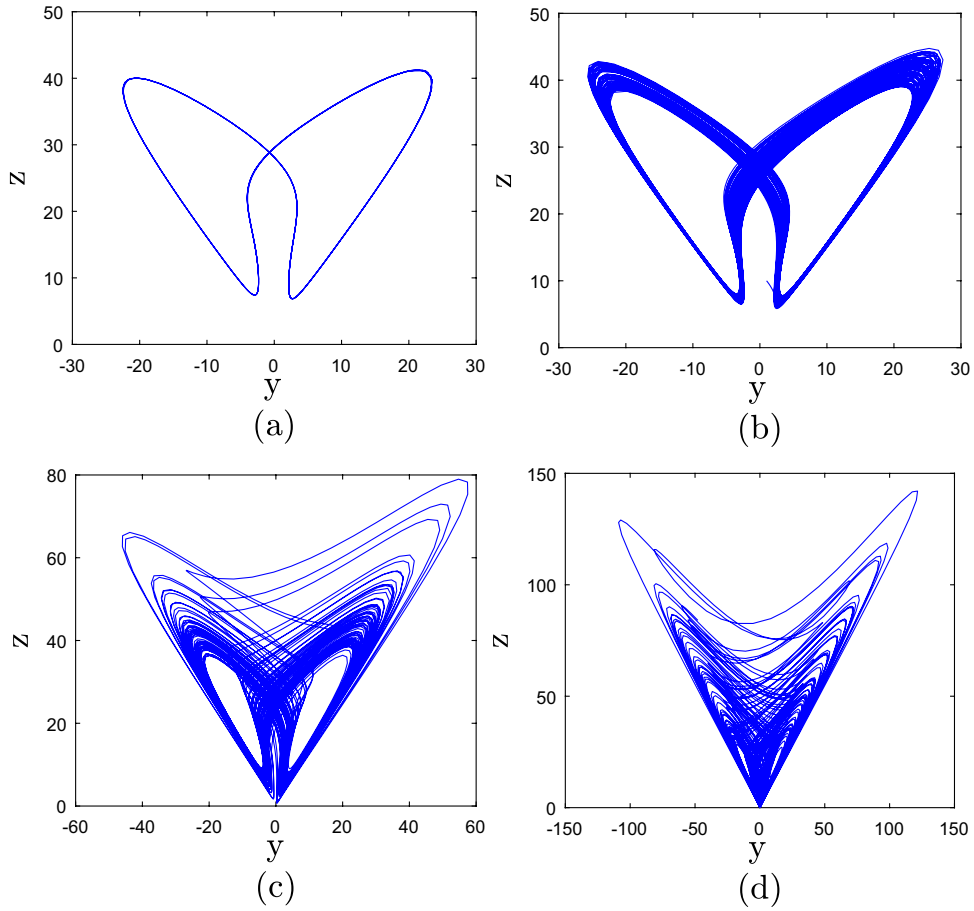


Figure 3. Phase plots of system (1) for specific values of the control parameter c.

$$\begin{cases} C_1 = C_2 = C_3 = C_4 = 1nF \\ R_1 = 50k\Omega \\ R_2 = R_3 = R_4 = R_6 = R_8 = 400k\Omega \\ R_5 = 10k\Omega, \;\; R_7 = 26.67k\Omega \\ R_9 = 4M\Omega \\ R_i = 100k\Omega, \;\; i = 10, \ldots\ldots, 15 \end{cases} \tag{7}$$

The agreement between the outcomes derived from numerical simulation software Matlab (See Fig. 1) and the electronic circuit simulation software Multisim (See Fig. 7) establishes strong validation for both hyperchaotic attractors of the novel hyperchaotic systems.

Voice encryption algorithm

The block diagrams of voice encryption\decryption using the new hyperchaotic process are demonstrated in Fig. 8 and Fig. 9 respectively.

As displayed in Fig. 8, the encryption process contains two levels: scrambling level and masking level, where both levels depend on the sequence generated by the proposed scheme. Chaotic scrambling is the process of transforming the original voice signal based on a particular algorithm[28–30]. This transformation can be achieved through various techniques, including mathematical transformations, encryption algorithms, or chaotic systems. In our system, the voice signal is scrambled using the *x, y, z,* and *w* sequences generated by the new hyperchaotic system according to the following equation:

$$V_s = v(t) + scramblingStrength * (s_1 * x(t).^{p} + s_2 * y(t).^{p2} + s_3 * z(t).^{p3} + s_4 * w(t).^{p4}) \tag{8}$$

The scrambling equation introduces a more sophisticated algorithm by integrating chaos and nonlinearity into the scrambling process. Where V_s is the scrambled voice signal, $v(t)$ is the original voice signal s_1, s_2, s_3, and s_4 represent coefficients, and p_1, p_2, p_3, and p_4, represent the power terms associated with each state variable $w(t)$, $z(t)$, $y(t)$, and $x(t)$. The power terms add an element of nonlinearity to the scrambling process, making it more complex and potentially enhancing the algorithm's security. Adjusting the power terms allows for fine-tuning the scrambling strength and the degree of nonlinearity introduced into the signal. Where the scrambling

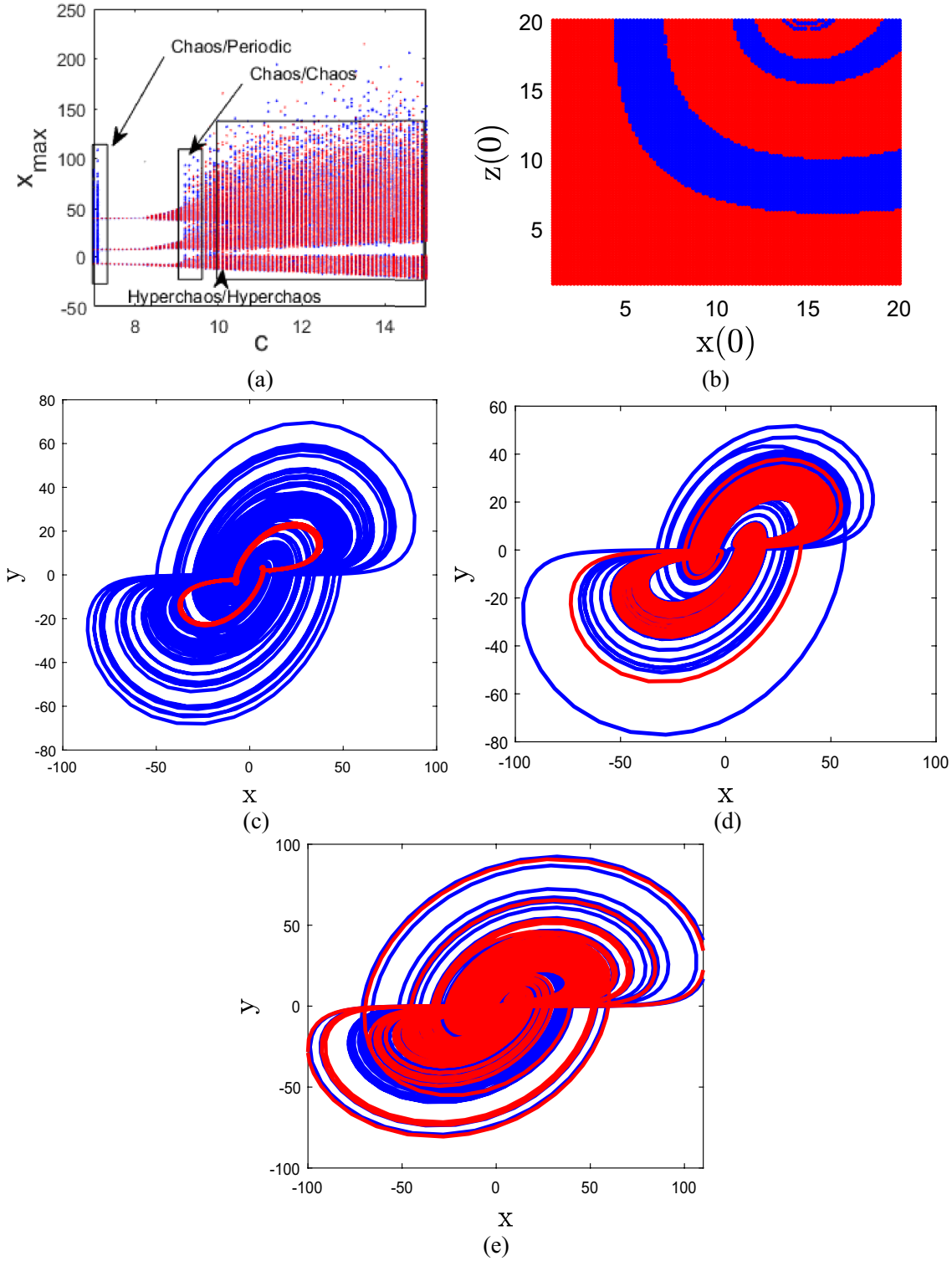


Figure 4. Graphical presentation of system (1): (**a**) coexisting bifurcation diagram for $7 < c < 15$, (**b**) basin of attraction in x(0)—z(0) plane with $y(0) = w(0) = 1$ and $c = 7$, (**c**) coexistence of one chaotic attractor and one periodic attractor, (**d**) coexisting of two chaotic attractors, (**e**) coexisting of two hyperchaotic attractors.

strength is set to 0.9, and the values of $p^1 = p^2 = p^3 = p^4 = 1$. The secret keys used in the encryption process are $s^1 = s^2 = s^3 = s^4 = 1$.

Then, to add a complexity to the encrypted signal, the resulted scrambled signal $V_s(t)$ is further masked using the state variables generated from the new scheme producing the encrypted voice signal $V_e(t)$ as follows:

$$V_e(t) = V_s(t) + (x(t) + y(t) + z(t) + w(t)) \tag{9}$$

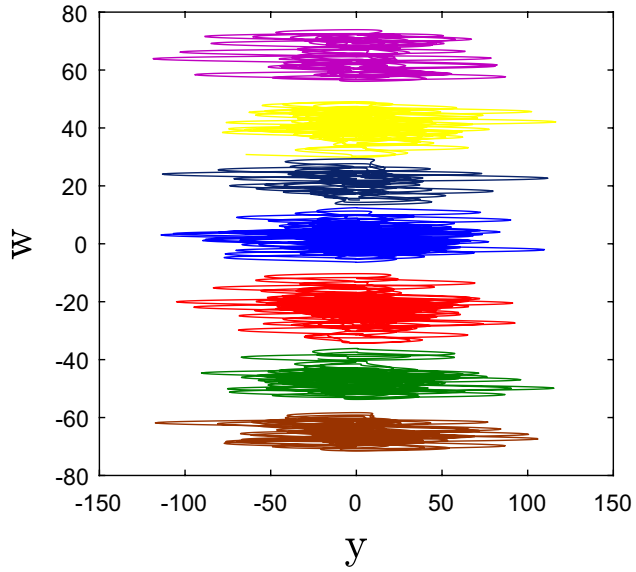


Figure 5. The plot of y-w hyperchaotic attractor of system (1) boosted with various values of offset boosting parameter k = 0 (blue), 10 (red), − 10 (black) 20 (green), − 20 (yellow), 30 (brown), and − 30 (magenta).

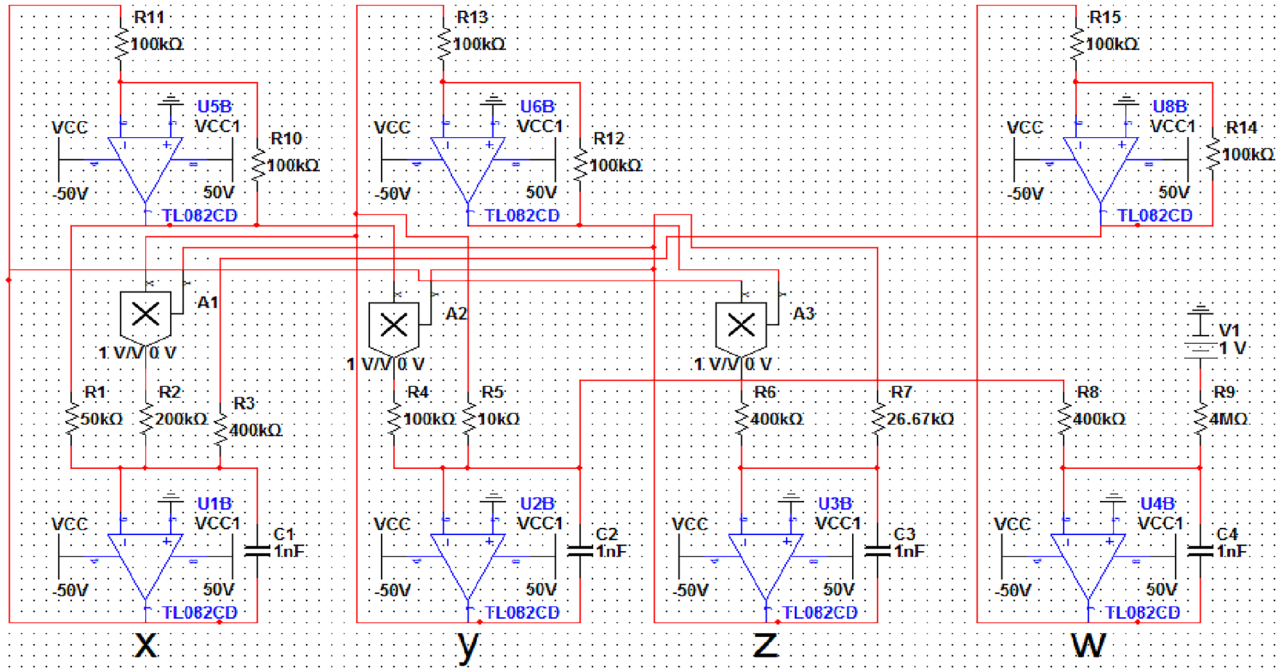


Figure 6. The schematic of the circuit.

In masking level, the complete state variables are used for masking the signal to increase the security level of the proposed system.

Decryption process

The decryption procedure is the vice versa of the encryption procedure, it involves generating an unmask signal by subtracting the same state variables from the encrypted signal producing the signal $V_d(t)$ as follows:

$$V_d(t) = V_e(t) - (x(t) + y(t) + z(t) + w(t) \tag{10}$$

The produced signal is then unscrambled according to the following equation:

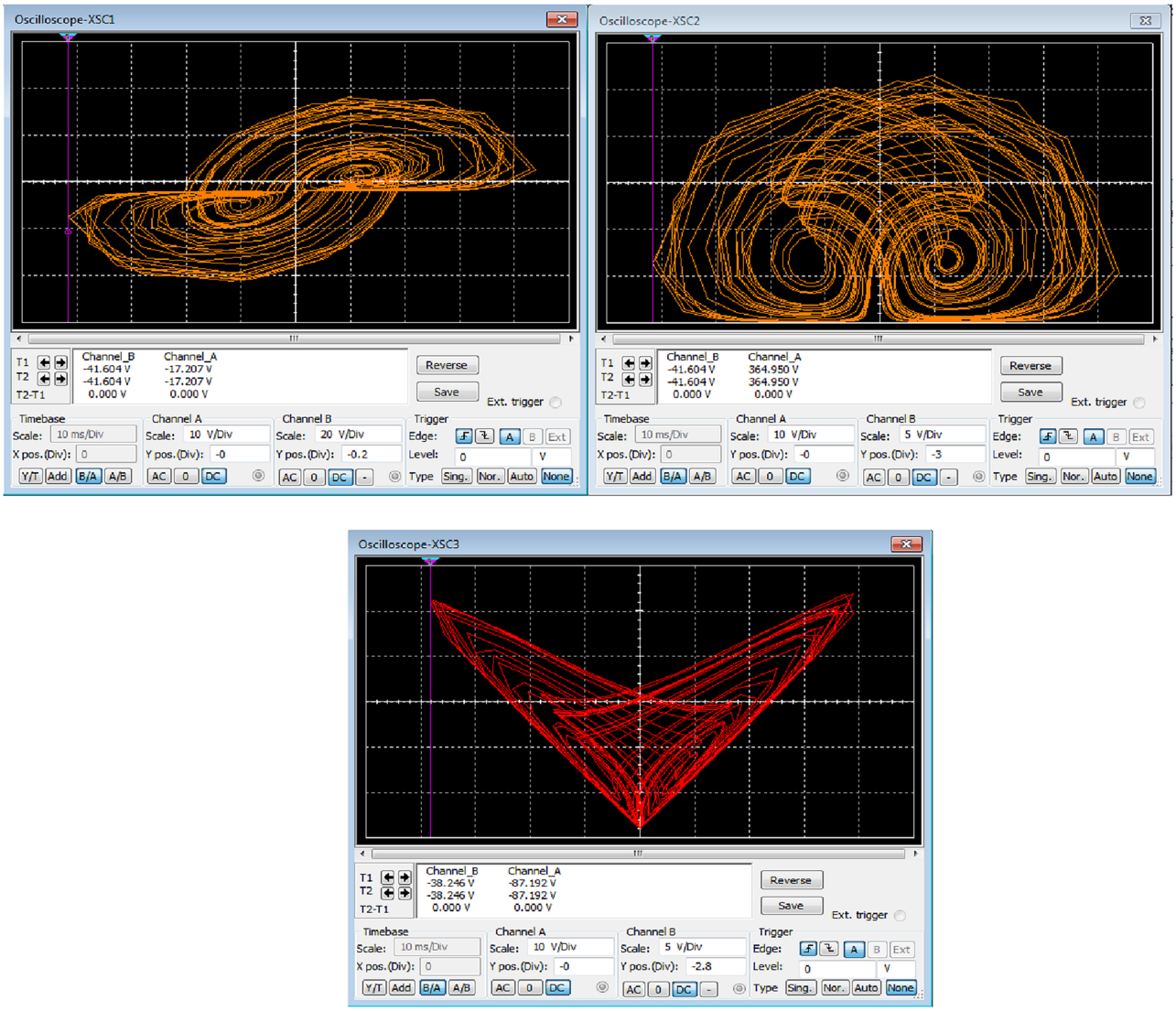


Figure 7. Experimental phase plots of the new hyperchaotic system.

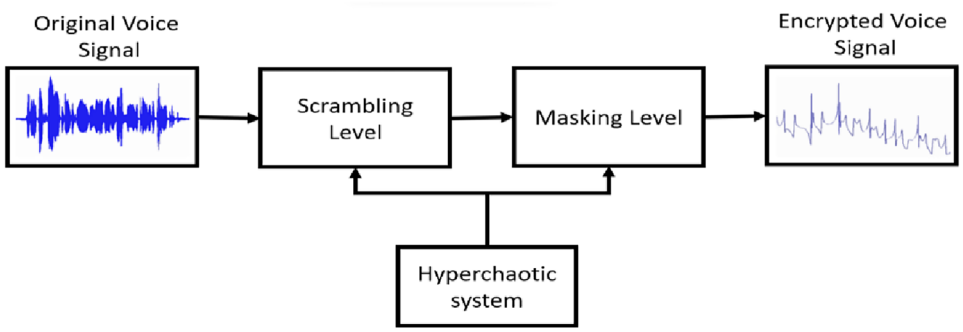


Figure 8. The voice encryption scheme using the new hyperchaotic system.

$$V_r = V_d(t) - scramblingStrength * (s_1 * x(t).^{p} + s_2 * y(t).^{p2} + s_3 * z(t).^{p3} + s_4 * w(t).^{p4}) \quad (11)$$

The resulting signal $V_r(t)$, represents the recovered voice signal. Assuming that the hyperchaotic systems in both the encryption and decryption systems are identical, have the same initial condition, and synchronized. The recovered signal $V_r(t)$ is like the original voice signal $v(t)$. In our system the values of coefficients terms are

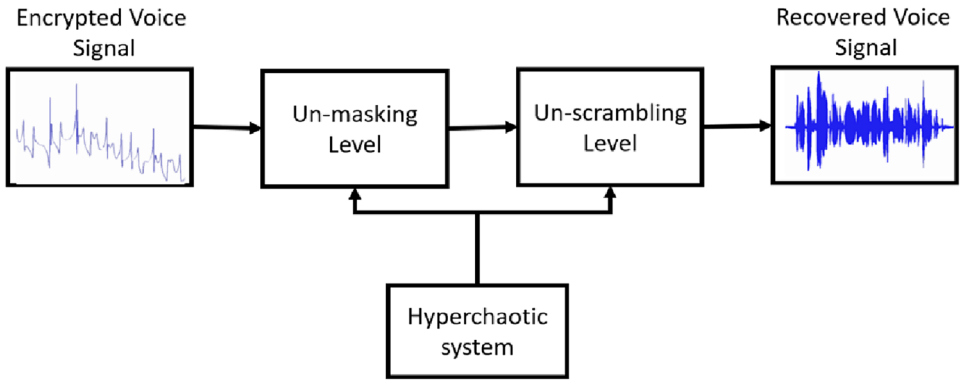


Figure 9. The voice decryption scheme using the new hyperchaotic system.

0.1 for s_1, s_2, and s_3, and 1 for s_4. While the values of the power terms are 1 for p_1, p_2, p_3, and p_4, and 0.5 for the scrambling strength term.

Numerical simulation and security analysis

MATLAB program was used to acquire the simulation results. The suggested system's effectiveness and security were evaluated using various tests, including waveform analysis, PRD, SNR, and correlation measurements. The voice signals use eight quantization bits at 8000 Hz.

The waveforms obtained from the proposed encryption system are illustrated in Fig. 10, the recovered, encrypted, and original voice signals, where the original voice transmission is entirely altered by the encrypted signal. Meanwhile, the recovered and original signals are identical.

Figure 11 depicts the histograms of the encrypted, original, and recovered voice signals. The distributed histogram indicates the randomness of the encrypted voice signal, a stark contrast to the histogram of the original and recovered voice signals, which exhibits a normal distribution, rendering it susceptible to attacks. The analysis reveals that our proposed algorithm provides robust security against various statistical attacks, affirming its efficacy in safeguarding voice communication.

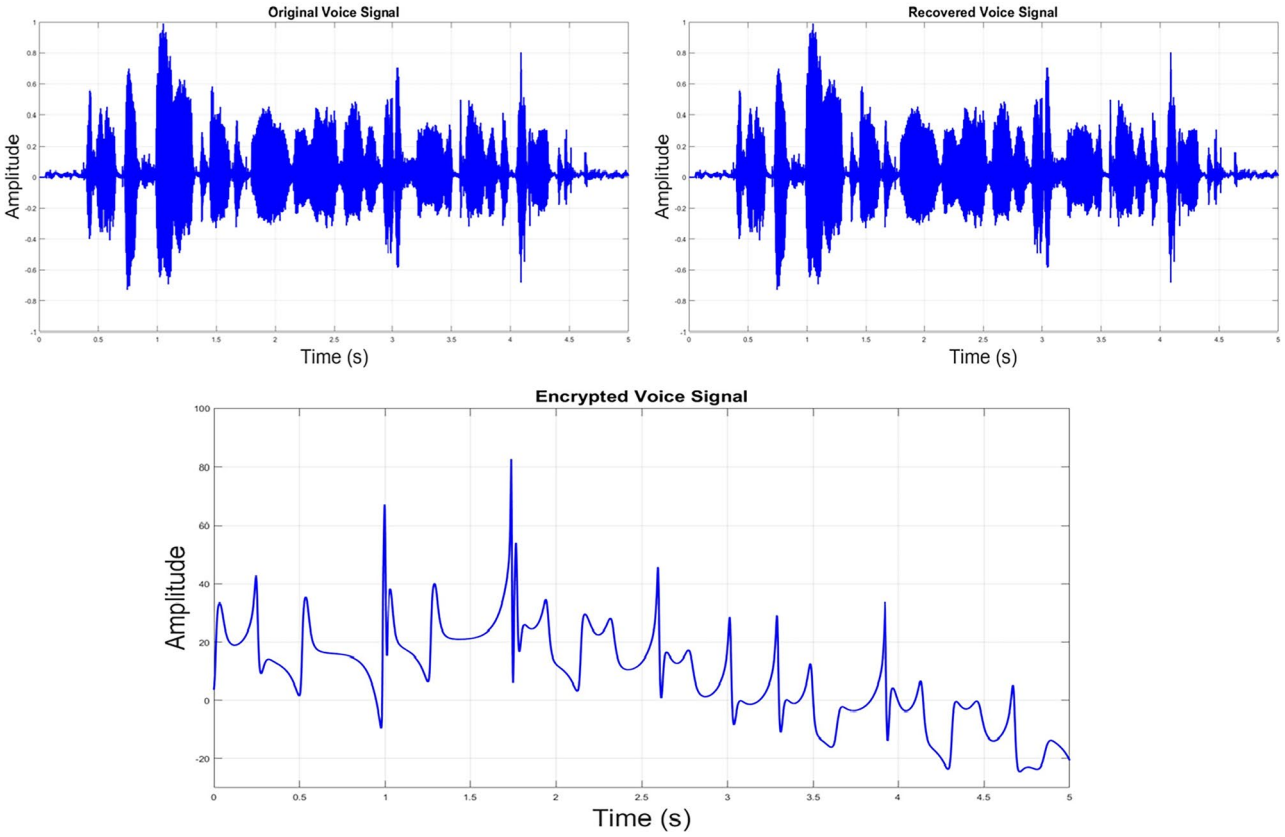


Figure 10. Waveform plots for the encrypted, recovered, and original voice signals.

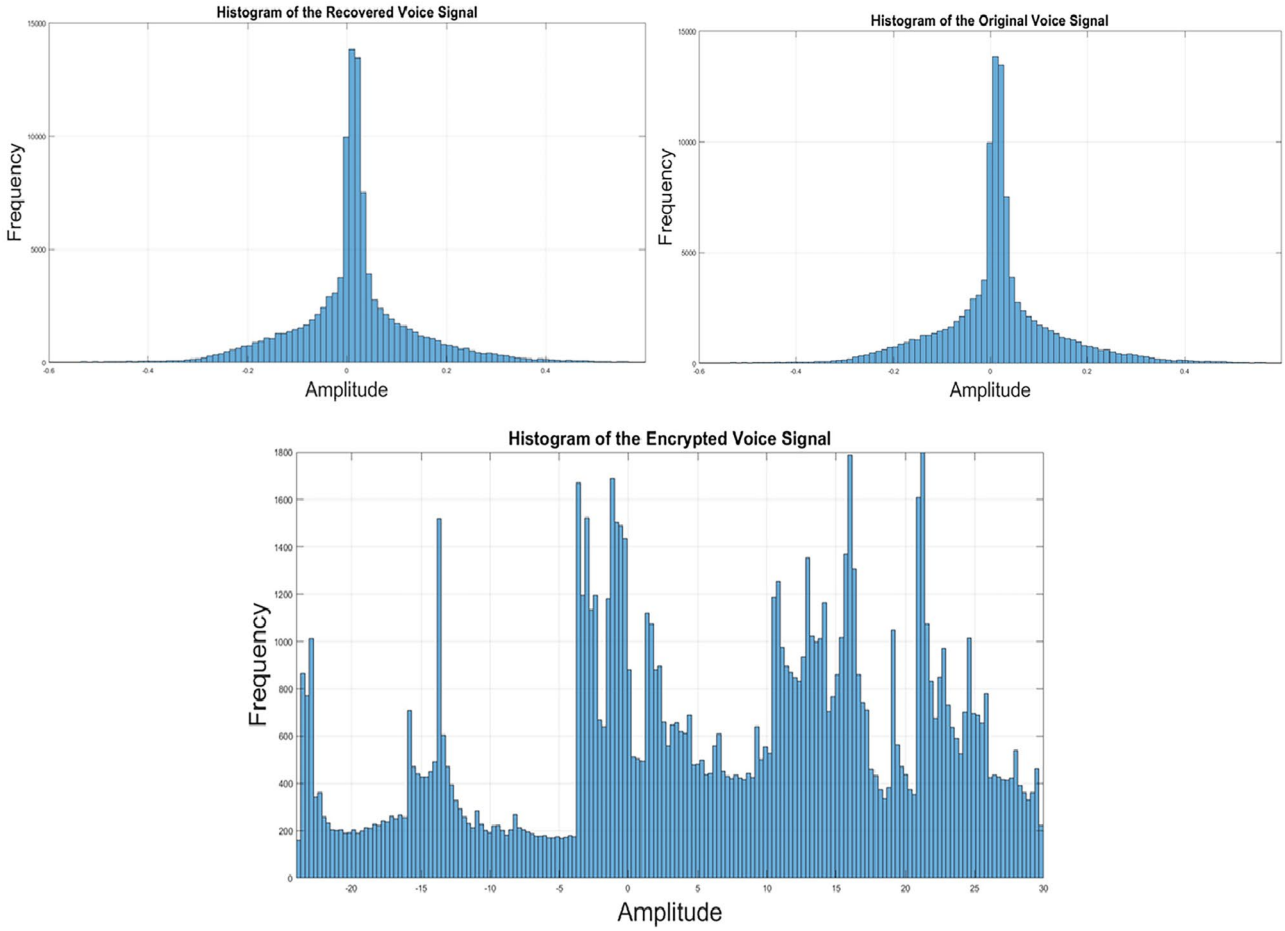


Figure 11. The histograms for the encrypted, recovered, and original voice signals.

Statistical tests

The Percentage Residual Deviation (PRD), Signal Noise Ratio (SNR), and Correlation Coefficient (CC) are employed to analyse the proposed scheme's immunity against statistical intruders[31–33]. Table 2 displays the values that were computed for various voice signals. The (PRD) is a statistical tool used to measure the deviation between encrypted and original audio signals. Low PRD values suggest a similarity between encrypted and original signals, indicating high fidelity and minimal distortion. Conversely, high PRD values imply significant differences, potentially indicating a decline in signal integrity and increased distortion. Table 2 provides the computed percent residual deviation values for a range of original and encrypted voice signals.

One of the widely considered objective metrics for assessing the strength of the original audio signal is the signal–noise ratio (SNR). The measurements of the SNR in Table 2 are highly negative, indicating an enormous quality of the encrypted speech signals. The correlation coefficient is a numerical correlation measure between -1 and 1. Table 2 provides the calculation for various speech signals. The small value of the (CC) obtained demonstrates how severely jumbled the encrypted signal is in comparison to the original voice signal. The higher PRD values suggest a significant deviation between the encrypted and original signals. The large negative SNR value indicates that the noise power is higher than the signal power, which makes it difficult to detect. On the other hand, near-zero correlation values imply a reduced similarity between the encrypted and original signals.

Voice	PRD	SNR	Correlation (cc)
Voice-1	1.2366e + 05	-61.8448	0.0005
Voice-2	1.5318e + 05	-63.7043	0.0011
Voice-3	1.6546e + 05	-64.3737	0.0013
Voice-4	1.4497e + 05	-63.2255	0.001
Voice-5	1.4331e + 05	-63.1255	0.0014
Voice-6	1.4320e + 05	-63.1189	0.0016

Table 2. The measurements of statistical metrics for different voice samples.

Key sensitivity
A key sensitivity analysis has been conducted to assess the responsiveness of the new encryption scheme to slight variations in the key values. A small change in one key, for example, the initial value of the x state variable is changed by 0.000000000000001, will entirely deviate the decrypted signal, as shown in Fig. 12, which reflects the immunity of the proposed encryption system against attacks.

NIST statistical randomness tests
Utilizing the NIST 800–22 test package, which is provided by the US National Institute of Standards and Technology, we examined the randomness of the encrypted speech signal in this test. This research primarily aims to test the randomness of encrypted and original voice signals. As indicated in Table 3, the tests were used to investigate the degree of randomness of each signal. The bit-stream of the original speech signal passed only 2 of the NIST tests. The results also suggest that the encrypted voice signal performs favorably in several statistical tests, meeting the criteria for randomness and passing certain NIST assessments.

Conclusion
This article presents a novel 4-D hyperchaotic system characterized by a high level of complexity, capable of exhibiting periodic, quasi-periodic, chaotic, and hyperchaotic behaviors through parameter adjustments. The system demonstrates the well-known dynamical property of multistability, showcasing various coexisting attractors

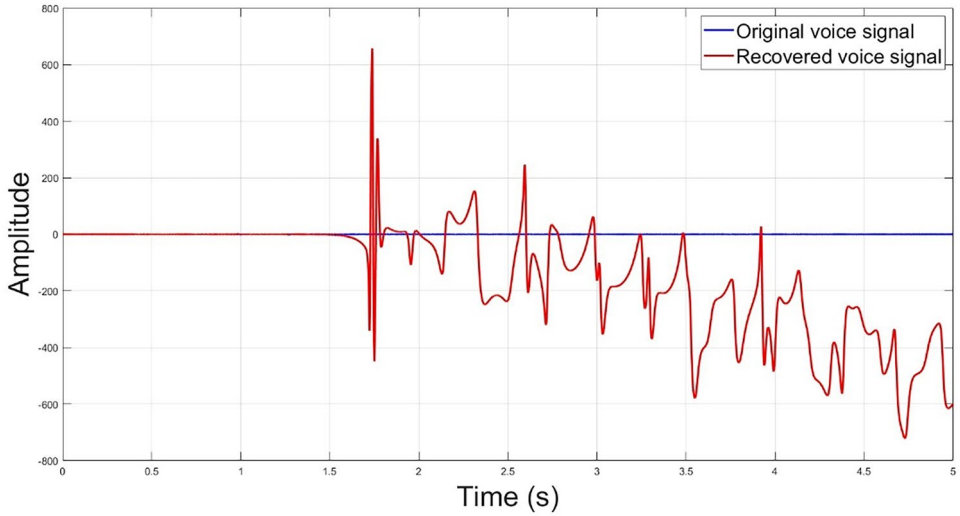


Figure 12. Decrypted speech signal with a bit of change in the initial values × 0.

Name	Original voice signal	Encrypted voice signal
random excursions	F	P
random excursions variant	F	P
Linear complexity	P	P
Serial	F	F
Universal	F	P
Overlapping template	P	P
Non-overlapping template	P	P
Fast Fourier transform	F	P
Rank	F	F
Longest Run	F	P
Runs	F	P
Approximate entropy	F	P
Cumulative sum	F	P
Block Frequency	F	P
Frequency	F	P

Table 3. The outcome of NIST statistical test for encrypted and original voice signals. *F* denotes fail, *P* denotes pass.

for identical parameter values. The dynamical characteristics of the proposed system are explored via bifurcation diagrams, Lyapunov exponents, stability analysis of equilibrium points, dissipativity, and phase plots. To validate the mathematical model, Multisim software is used to implement an electronic circuit. The system's offset boosting control capability is highlighted as an attractive and unique feature. Consequently, the new found 4D system proves to be highly advantageous for applications relying on chaos, given its hyperchaotic behavior, multistability, offset boosting property, and the ease with which its electronic circuit can be implemented. We conducted comprehensive tests, including histogram analysis, PRD, SNR, CC, key sensitivity, and NIST randomness, to evaluate its effectiveness against attacks. Our findings demonstrate robust performance, highlighting the system's capability to safeguard voice signals effectively. This work advances cryptography through innovative encryption methods tailored for voice communication security. In future research, we will make enhancements to the voice encryption system to bolster its resilience against various attacks. This could involve investigating advanced encryption algorithms, incorporating additional layers of security, or exploring techniques from other domains.

Data availability

The data that support the findings of this study are available from the corresponding author on reasonable request.

Received: 30 January 2024; Accepted: 3 June 2024
Published online: 06 June 2024

References

1. Nestor, T. *et al.* A new 4D hyperchaotic system with dynamics analysis, synchronization, and application to image encryption. *Symmetry* **14**(2), 424 (2022).
2. Leutcho, G. D. *et al.* Dynamics of a new multistable 4D hyperchaotic Lorenz system and its applications. *Int. J. Bifurc. Chaos* **32**(01), 2250001 (2022).
3. Dong, C. & Wang, J. Hidden and coexisting attractors in a novel 4D hyperchaotic system with no equilibrium point. *Fractal Fract.* **6**(6), 306 (2022).
4. Lai, Q., Wang, Z. & Kuate, P. D. K. Dynamical analysis, FPGA implementation and synchronization for secure communication of new chaotic system with hidden and coexisting attractors. *Mod. Phys. Lett. B* **36**(01), 2150538 (2022).
5. Lai, Q. & Lai, C. Design and implementation of a new memristive chaotic system with coexisting attractors and offset boosting behaviors. *Indian J. Phys.* https://doi.org/10.1007/s12648-022-02344-w (2022).
6. Ma, C. *et al.* Dynamical analysis of a new chaotic system: Asymmetric multistability, offset boosting control and circuit realization. *Nonlinear Dyn.* **103**(3), 2867–2880 (2021).
7. Wen, H. & Lin, Y. Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding. *Expert Syst. Appl.* **237**, 121514 (2024).
8. Wen, H., Lin, Y., Xie, Z. & Liu, T. Chaos-based block permutation and dynamic sequence multiplexing for video encryption. *Sci. Rep.* **13**(1), 14721 (2023).
9. Bonny, T. Chaotic or hyper-chaotic oscillator? Numerical solution, circuit design, MATLAB HDL-coder implementation, VHDL code, security analysis, and FPGA realization. *Circuits Syst. Signal Process.* **40**(3), 1061–1088 (2021).
10. Bonny, T., Al Debsi, R., Majzoub, S. & Elwakil, A. S. Hardware optimized FPGA implementations of high-speed true random bit generators based on switching-type chaotic oscillators. *Circuits Syst. Signal Process.* **38**, 1342–1359 (2019).
11. Wen, H., Huang, Y. & Lin, Y. High-quality color image compression-encryption using chaos and block permutation. *J. King Saud Univ.-Comput. Inf. Sci.* **35**(8), 101660 (2023).
12. Bonny, T., Nassan, W. A., Vaidyanathan, S. & Sambas, A. Highly-secured chaos-based communication system using cascaded masking technique and adaptive synchronization. *Multimed. Tools Appl.* **82**(22), 34229–34258 (2023).
13. Bonny, T., Nassan, W. A. & Baba, A. Voice encryption using a unified hyper-chaotic system. *Multimed. Tools Appl.* **82**(1), 1067–1085 (2023).
14. Xu, C., Liu, Z., Pang, Y., Saifullah, S. & Khan, J. Torus and fixed-point attractors of a new hyperchaotic 4D system. *J. Comput. Sci.* **67**, 101974 (2023).
15. Hui, Y., Liu, H. & Fang, P. A DNA image encryption based on a new hyperchaotic system. *Multimed. Tools Appl.* **82**(14), 21983–22007 (2023).
16. Fu, S., Cheng, X. & Liu, J. Dynamics, circuit design, feedback control of a new hyperchaotic system and its application in audio encryption. *Sci. Rep.* **13**(1), 19385 (2023).
17. Li, S., Wu, Y. & Zhang, X. Analysis and synchronization of a new hyperchaotic system with exponential term. *Mathematics* **9**(24), 3281 (2021).
18. Yang, L., Yang, Q. & Chen, G. Hidden attractors, singularly degenerate heteroclinic orbits, multistability and physical realization of a new 6D hyperchaotic system. *Commun. Nonlinear Sci. Numer. Simul.* **90**, 105362 (2020).
19. Jiang, D., Liu, L., Wang, X. & Rong, X. Image encryption algorithm for crowd data based on a new hyperchaotic system and Bernstein polynomial. *IET Image Process.* **15**(14), 3698–3717 (2021).
20. Gu, S., Du, B. & Wan, Y. A new four-dimensional non-Hamiltonian conservative hyperchaotic system. *Int. J. Bifurc. Chaos* **30**(16), 2050242 (2020).
21. Yu, F. *et al.* Dynamics analysis, synchronization and FPGA implementation of multiscroll Hopfield neural networks with non-polynomial memristor. *Chaos Solitons Fractals* **179**, 114440 (2024).
22. Kong, X. *et al.* Memristor-induced hyperchaos, multiscroll and extreme multistability in fractional-order HNN: Image encryption and FPGA implementation. *Neural Netw.* **171**, 85–103 (2024).
23. Wolf, A., Swift, J. B., Swinney, H. L. & Vastano, J. A. Determining Lyapunov exponents from a time series. *Phys. D Nonlinear Phenom.* **16**(3), 285–317 (1985).
24. Sambas, A. *et al.* A New Hyperjerk system with a half line equilibrium: Multistability, Period doubling reversals, antimonotonocity, electronic circuit, FPGA design and an application to image encryption. *IEEE Access* **12**, 9177–9194 (2024).
25. Benkouider, K. *et al.* A new 5-D multistable hyperchaotic system with three positive Lyapunov exponents: Bifurcation analysis, circuit design, FPGA realization and image encryption. *IEEE Access* **10**, 90111–90132 (2022).
26. Flores-Carapia, R., Silva-García, V. M. & Cardona-López, M. A. A Dynamic hybrid cryptosystem using chaos and Diffie-hellman protocol: An image encryption application. *Appl. Sci.* **13**(12), 7168 (2023).
27. Luis, M., Daniel, L., Isabel, A. & Deicy, A. A new multimedia cryptosystem using chaos, quaternion theory and modular arithmetic. *Multimed. Tools Appl.* **82**(23), 35149–35181 (2023).
28. Chen, X., Mou, J., Cao, Y. & Banerjee, S. Chaotic multiple-image encryption algorithm based on block scrambling and dynamic DNA coding. *Int. J. Bifurc. Chaos* **33**(16), 2350190 (2023).

29. Zhou, T., Guo, A., Xu, S., Chen, X. & Swingle, B. Hydrodynamic theory of scrambling in chaotic long-range interacting systems. *Phys. Rev. B* **107**(1), 014201 (2023).
30. Tang, J. *et al.* An image layered scrambling encryption algorithm based on a novel discrete chaotic map. *IET Image Process.* **17**(2), 518–532 (2023).
31. Al-Mhadawi, M. M., Albahrani, E. A. & Lafta, S. H. Efficient and secure chaotic PRNG for color image encryption. *Microprocess. Microsyst.* **101**, 104911 (2023).
32. Alexan, W., Elkandoz, M., Mashaly, M., Azab, E. & Aboshousha, A. Color image encryption through chaos and kaa map. *IEEE Access* **11**, 11541–11554 (2023).
33. Gupta, M., Singh, V. P., Gupta, K. K. & Shukla, P. K. An efficient image encryption technique based on two-level security for internet of things. *Multimed. Tools Appl.* **82**(4), 5091–5111 (2023).

Author contributions

Conceptualization, A.S. and K.B; methodology, T.B and W.A.N; software, K.B, W.A.N and T.B; formal analysis, I.M.S, and I.A.R.M.; investigation, B.A.H, M.M and T.B; Methodology, I.M.S, B.A.H and M.M; Funding, I.A.R.M and I.M.S; writing—original draft preparation, A.S, K.B and W.A.N; writing—review and editing, I.A.R.M, B.A.H and M.M.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to I.A.R.M.

Reprints and permissions information is available at www.nature.com/reprints.

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

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

© The Author(s) 2024