SN Computer Science (2024) 5:420
https://doi.org/10.1007/s42979-024-02766-9

ORIGINAL RESEARCH

Dynamic Analysis and Circuit Design of a New 3D Highly Chaotic System and its Application to Pseudo Random Number Generator (PRNG) and Image Encryption

Aceng Sambas[1,2] · Khaled Benkouider[3] · Sezgin Kaçar[4] · Nurdoğan Ceylan[5] · Sundarapandian Vaidyanathan[1,6] · Ibrahim Mohammed Sulaiman[7,8] · Mohamad Afendee Mohamed[1] · Ahmad Faisal Mohamad Ayob[9] · Sishu Shankar Muni[10]

Received: 4 August 2023 / Accepted: 2 March 2024
© The Author(s), under exclusive licence to Springer Nature Singapore Pte Ltd. 2024

Abstract

In this paper, a new 3D dynamical system with four quadratic nonlinear terms is presented. It is shown that the proposed chaotic system has two saddle-foci, unstable, equilibrium points. Thus, the proposed chaotic system exhibits self-excited chaotic attractors. Dynamical analysis methods such as Lyapunov exponents spectrum, bifurcation diagrams, and phase portraits are used to explore the complex dynamical behaviors of the proposed chaotic system and analyze its basic qualitative properties. It is shown that the maximal Lyapunov exponent (MLE) of the new chaotic system is 7.196, which is a high value. The proposed highly chaotic system exhibits high complexity and it will be very useful for applications in cryptography, encryption and secure communications. The physical feasibility of the proposed system is verified by implementing its electronic circuit schematic using Multisim software. Additionally, a PRNG has been developed using the derived state variables and analyze with NIST-800–22 test. Lastly, we developed a PRNG-based image encryption and employ it for an encryption. The experimental outcomes obtained prove that the 3D chaotic system-based encryption application presented in this section has a very good performance.

Keywords Chaos · Image encryption · Pseudo random number generator

Introduction

Due to their tremendous complexity, chaotic systems are used in a variety of technical and scientific fields, such as cryptography and secure communications [1, 2]. Recently, numerous literatures have studied the chaotic systems. Singh and Roy [3] constructed a new 3D chaotic system that is consider as hardware realizable, and possess real-life application requirement. Yang and Qiao [4] presented a simple chaotic system that can have multiple equilibria.

✉ Aceng Sambas
acengsambas@unisza.edu.my

1 Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Campus Besut, 22200 Kuala, Terengganu, Malaysia

2 Department of Mechanical Engineering, Universitas Muhamadiyah Tasikmalaya, Tamansari Gobras, 46196 Tasikmalaya, Indonesia

3 Department of Electronics, Faculty of Technology, Badji-Mokhtar University, B.P. 12, 23000 Sidi Ammar, Annaba, Algeria

4 Department of Electrical and Electronics Engineering, Sakarya University of Applied Sciences, Sakarya 54050, Serdivan, Turkey

5 Department of Mechanical Engineering, Adıyaman University, 02040 Adıyaman, Merkez, Turkey

6 Centre for Control Systems, Vel Tech University, Chennai 600062, Tamil Nadu, India

7 School of Quantitative Science, University Utara Malaysia, Sintok, 06010 Bukit Kayu Hitam, Kedah, Malaysia

8 Faculty of Education and Arts, Sohar University, Sohar 311, Oman

9 Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu, Gong Badak, 21300 Kuala Terengganu, Terengganu, Malaysia

10 Department of Physical Sciences, Department of Physical Sciences, Indian Institute of Science Education and Research, Kolkata 741246, Mohanpur, India

Published online: 10 April 2024

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Using a smooth piecewise quadratic non-linearity, Signing et al. [5] constructed a new four-wing chaotic system. [6] developed a new multistable jerk chaotic system with three quadratic nonlinear systems and presented a circuit simulation.

In chaotic systems, self-excited attractors and hidden attractors represent distinct aspects of the complex behavior exhibited by dynamic systems [7]. Self-excited attractors are characterized by the intrinsic capacity of a system to generate chaotic trajectories without external forcing. This implies that the chaotic behavior emerges naturally from the system's internal dynamics, such as nonlinear interactions among variables. A classic example is the Lorenz system, a simplified model of atmospheric convection, where chaotic behavior arises due to the system's inherent structure. On the other hand, hidden attractors are attractors that may not be immediately evident in the observable behavior of a system [7]. Trajectories might initially appear periodic or exhibit seemingly regular patterns, masking the underlying chaotic nature [8]. Hidden attractors become apparent only under specific conditions or when certain parameters are chosen, and their existence may go unnoticed without a careful analysis [9]. These elusive attractors have practical implications, particularly in secure communications and cryptography, where their concealed nature can be harnessed for encryption purposes. Unravelling the intricacies of self-excited and hidden attractors is crucial for a comprehensive understanding of chaotic systems and has implications for both theoretical studies and practical applications [10].

Several literatures on chaos system focus on chaos-based image encryption. Yu et al. [11] applied Memristive Hopfield Neural Network (MHNN) to develop a novel pseudo-random number generator (PRNG). The FPGA logic design was implemented on Xilinx XC7Z-020CLG400-2 integrated circuit (IC), programmed via hardware language of Verilog-HDL for the use of image encryption communicated over the Internet of Things (IoT). The framework for creating Elliptic Curve-based PRNG was introduced by AbdElHaleem et al. [12], who also classified current PRNG design techniques as non-iterative or iterative and mapped them into the framework. System key sensitivity analysis, the NIST statistical test suite, differential attack measures, and Statistical metrics have all been used to establish the system's security. The PRNG pro- cess was developed by Abd EL-Latif et al. [13] using a controlled alternate quantum walk and presented as a part of a novel quantum colour picture encryption system. Gafsi et al. [14] improved the chaos-based cryptosystem for speedy operation on secret medical images by revisiting the concepts of permutation, substitution, and diffusion. A lightweight secure cryptographic method for secure picture communication was suggested by Mondal and Mandal [15]. The authors employed pseudo-random number (PRN) as a source to permute followed by Deoxyribo Nucleic Acid (DNA) computation for encrypting the pixels.

Encryption schemes have applications in several areas such as the following:

a) Security, privacy, trust, and anonymity [16–18]
b) Lightweight and efficient privacy-preserving mutual authentication scheme to secure internet of things based smart healthcare [19]
c) DNACDS: Cloud IoE big data security and accessing scheme based on DNA cryptography [20]
d) Profile based access control model in cloud computing environment [21, 22] (e) A lightweight and anonymous mutual authentication scheme for medical big data in distributed smart healthcare systems [23]

The main contribution and novelty of this paper are summarized as follows:

a) The proposed system consists of a total nine terms including four quadratic nonlinear terms.
b) The proposed system is highly chaotic with its maximal Lyapunov exponent (MLE) equal to 7.196. The high value of the MLE for the new chaotic system signifies a high level of complexity of the system.
c) The proposed system has two saddle-foci, unstable, equilibrium points and exhibits self-excited chaotic attractors.
d) High complexity of the proposed system makes it suitable for applications such as cryptography, encryption and secure communications.
e) We have simulated the proposed highly chaotic system using an electronic circuit design, which is developed via Multisim software.
f) As an engineering application, we have developed a PRNG-based image encryption based on the proposed highly chaotic system.

In this study, we propose a dynamical model of a new 3D chaotic system with self-excited chaotic attractors. In addition, we observe that the proposed chaotic system exhibits positive Lyapunov exponent having value larger than seven, and thus the new system is highly chaotic. Specific to this novel 3D chaotic system, we offer a comprehensive dynamic analysis based on bifurcation diagrams and Lyapunov exponents. We

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

construct an electrical circuit for the implementation of the novel 3D chaotic system using Multisim and provide the circuit simulation results. Finally, PRNG based image encryption has been developed and applied for encryption. As future research work, we plan to investigate the applications of chaotic signals for visual image security, which is an innovative method of ensuring image protection without the encryption process being visible to the attacker [24–26].

A New 3D Chaotic System

In this study, we present a new 3D chaotic system, which is mathematically modelled by the dynamics:

$$\begin{cases} \dot{x} = \alpha(y - x) + yz \\ \dot{y} = x(b - z) - 1 \\ \dot{z} = x^2 + xz - cz \end{cases} \tag{1}$$

In (1), x, y, z are the state variables, and a, b, c denotes positive constant parameters.

This work establishes that the system (1) is chaotic when we set the initial state as X (0) to be (1, 1, 1) and the parameters a, b and c to be 20, 50, and 10 respectively.

When we choose the parameter values as (a, b, c) = (20, 50, 10), the con- forming Lyapunov exponents of the system (1) are calculated using Wolf's algorithm [27] incorporated on MATLAB as follows:

$$\begin{cases} LE_1 = 7.196 \\ LE_2 = 0 \\ LE_3 = -37.197 \end{cases} \tag{2}$$

From (2), we notice that the system (1) has a high value of maximal Lyapunov exponent (MLE), viz. LE1 = 7.196, which shows that the system (1) is highly chaotic. Furthermore, the new 3D system (1) has a negative sum of the three Lyapunov exponents, confirming that the system (1) is a dissipative chaotic system [28]. Since the system (1) is highly chaotic, it is very suitable for applications such as cryptosystems and secure communications.

The following formula is used to compute the system's Kaplan-Yorke dimension [29, 30]:

$$D_{KY} = 2 + \frac{LE_1 + LE_2}{|LE_3|} = 2.0605 \tag{3}$$

From Eqn (3), the Kaplan–Yorke dimension value turned out to be fractional. Therefore, the proposed 3D system (1) generates complex chaotic attractors. The comparison of MLE and the nature of attractors of the new system (1) with seven existing chaotic systems in the literature are shown in Table 1.

It is observed that our novel system (1) exhibits a larger MLE value, when compared to seven chaotic systems in the literature. Figure 1 shows the 2-D phase plots of the chaotic attractor of the highly chaotic system (1).

Next, we suppose that the parameter values are set as in the chaotic case, viz. (a, b, c) = (20, 50, 10). For this case, it is found that the highly chaotic system (1) has two equilibrium points given by

$$P_1 = \begin{bmatrix} 8.5385 \\ 2.4437 \\ 49.8829 \end{bmatrix}, P_2 = \begin{bmatrix} -58.5585 \\ -16.7269 \\ 50.0171 \end{bmatrix} \tag{4}$$

The Jacobian matrix of the highly chaotic system (1) at P1 is found as

$$J(P_1) = J_1 \begin{bmatrix} -20.0000 & 69.8829 & 2.4437 \\ 0.1171 & 0 & 50.0000 \\ 66.9599 & 0 & -1.4615 \end{bmatrix} \tag{5}$$

which has the spectral values $S_1 = 55.9180$ and $S_{2;3} = -38.6898 \pm 41.8404i$.

The Jacobian matrix of the highly chaotic system (1) at P2 is found

$$J(P_2) = J_2 \begin{bmatrix} -20.0000 & 70.0171 & -16.7269 \\ -0.1171 & 0 & 50.0000 \\ -67.0999 & 0 & -68.6685 \end{bmatrix} \tag{6}$$

as which has the spectral values $S_1 = = -106.81$ and $S_{2,3} = 9.13 \pm 46.01i$.

This calculation shows that the equilibrium points P1 and P2 are saddle-foci and unstable. Hence, the highly chaotic system (1) exhibits self-excited attractors.

Table 1 Comparison of Maximal Lyapunov Exponent (MLE) of the proposed chaotic system (1) with seven chaotic systems in the chaos literature

System	MLE	Nature of attractors
Singh and Roy [3]	5.587	Self-exited
Dong [31]	1.100	Hidden
Qiu et al. [32]	0.0153	Hidden
Liu et al. [33]	0.3781	Hidden
Yang and Qiao [4]	0.2263	Hidden
Zhou et al. [34]	0.134	Hidden
Rahman and Jasim [35]	0.2643	Hidden
This Work	7.196	Self-exited

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

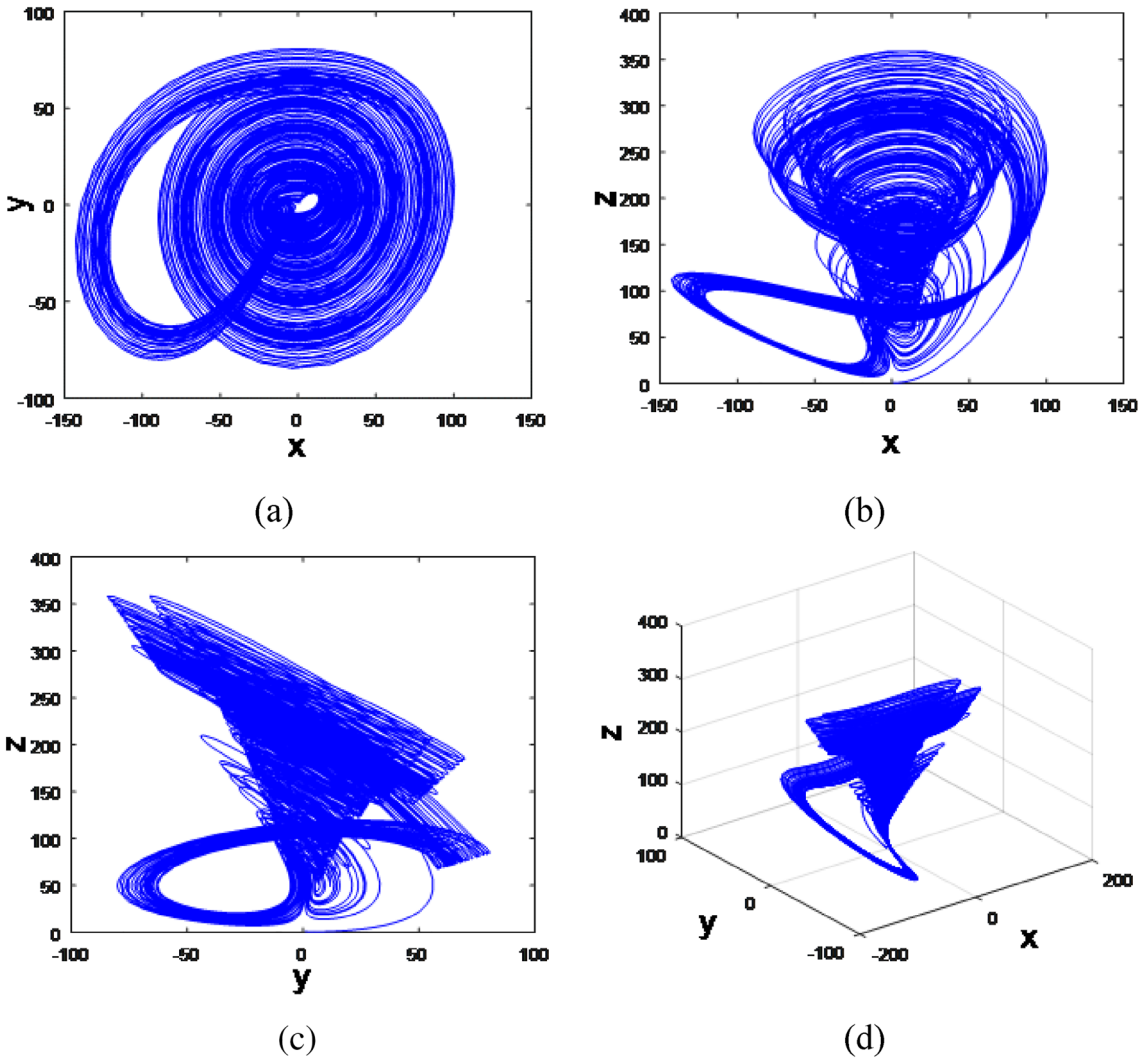


Fig. 1 2-D phase plots of the chaotic attractor of the highly chaotic system (1) for X (0) = (1, 1, 1) and (**a**, **b**, **c**) = (20, 50, 10): (**a**) x − y plane, (**b**) x − z plane, (**c**) y − z plane and (**d**) R^3

Dynamical Analysis

By fixing the parameters b = 50 and c = 10, while a varying in the range [10, 20], we obtain the plots for the respective Lyapunov exponents spectrum (see Fig. 2a) and bifurcation plot (see Fig. 2b) of our proposed system. When 10 < a < 14, system (1) has no positive Lyapunov exponents which means that it exhibits periodic behaviour as shown in Fig. 3a. The corresponding LEs are: $LE_1 = 0$, $LE_2 = -5.248$, $LE_3 = -16.756$. When 14 < a < 20, system (1) exhibits chaotic behaviour with one positive LE as depicted in Fig. 3b. The corresponding LEs are: $LE_1 = 6.358$, $LE_2 = 0$, $LE_3 = -34.756$.

However, when the parameters a and c are fixed as a = 20 and c = 10, and parameter b allow to vary in the range [10, 50], we obtain the plots for the respective Lyapunov exponents spectrum (see Fig. 2c) and bifurcation plot (see Fig. 2d). For 10 < b < 13 and 34 < b < 34.8, system (1) has no positive Lyapunov exponents, which means that it exhibits periodic behaviour as can be seen in Fig. 3c. The corresponding LEs are: $LE_1 = 0$, $LE_2 = -1.562$, $LE_3 = -28.440$. When 13 < b < 50, system (1) exhibits chaotic behaviour with one positive LE as depicted in Fig. 3d. The corresponding LEs are: $LE_1 = 6.526$, $LE_2 = 0$, $LE_3 = -36.528$.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

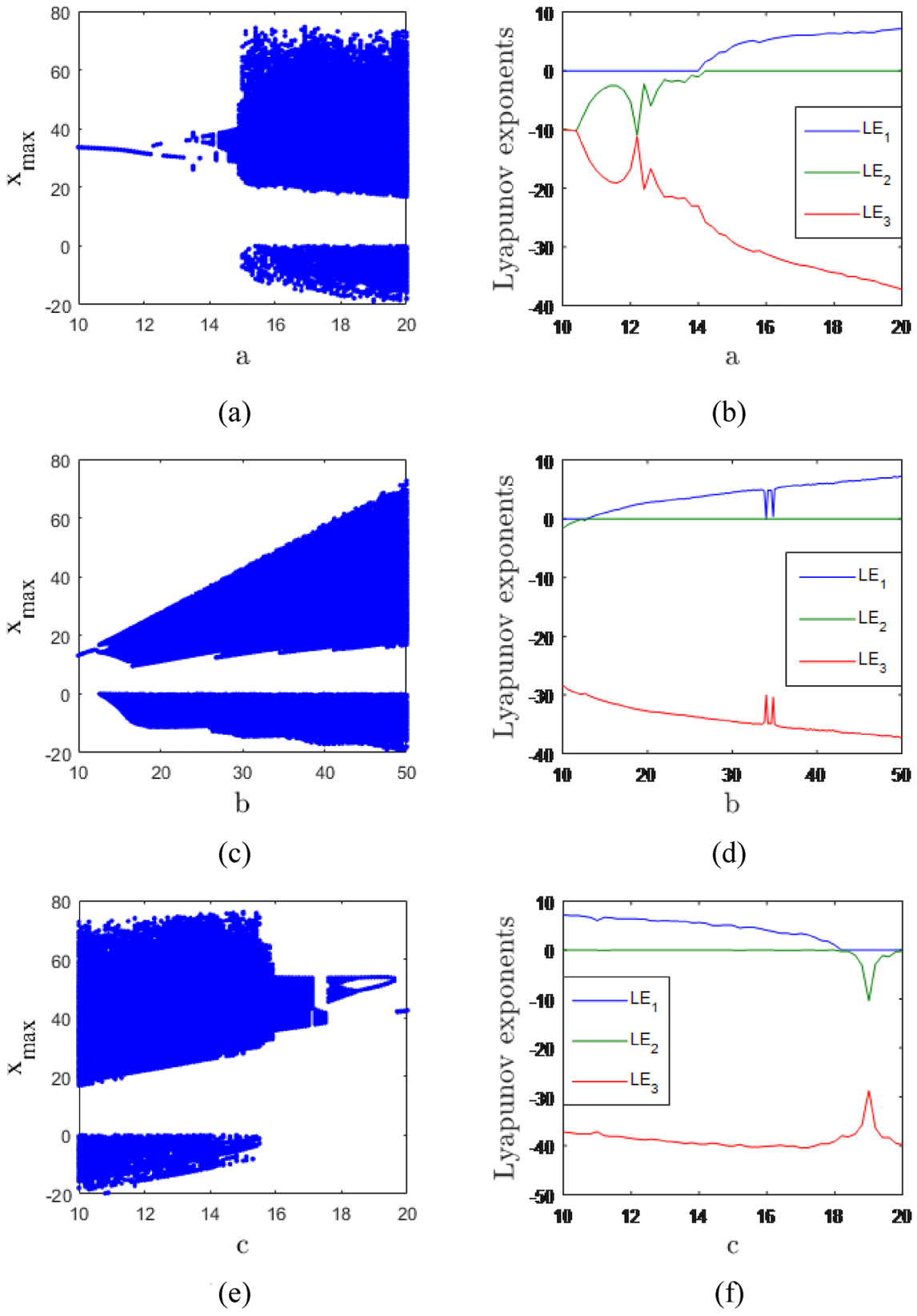


Fig. 2 Bifurcation diagrams and LEs spectrums of the highly chaotic system (1) for specific intervals of parameters

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

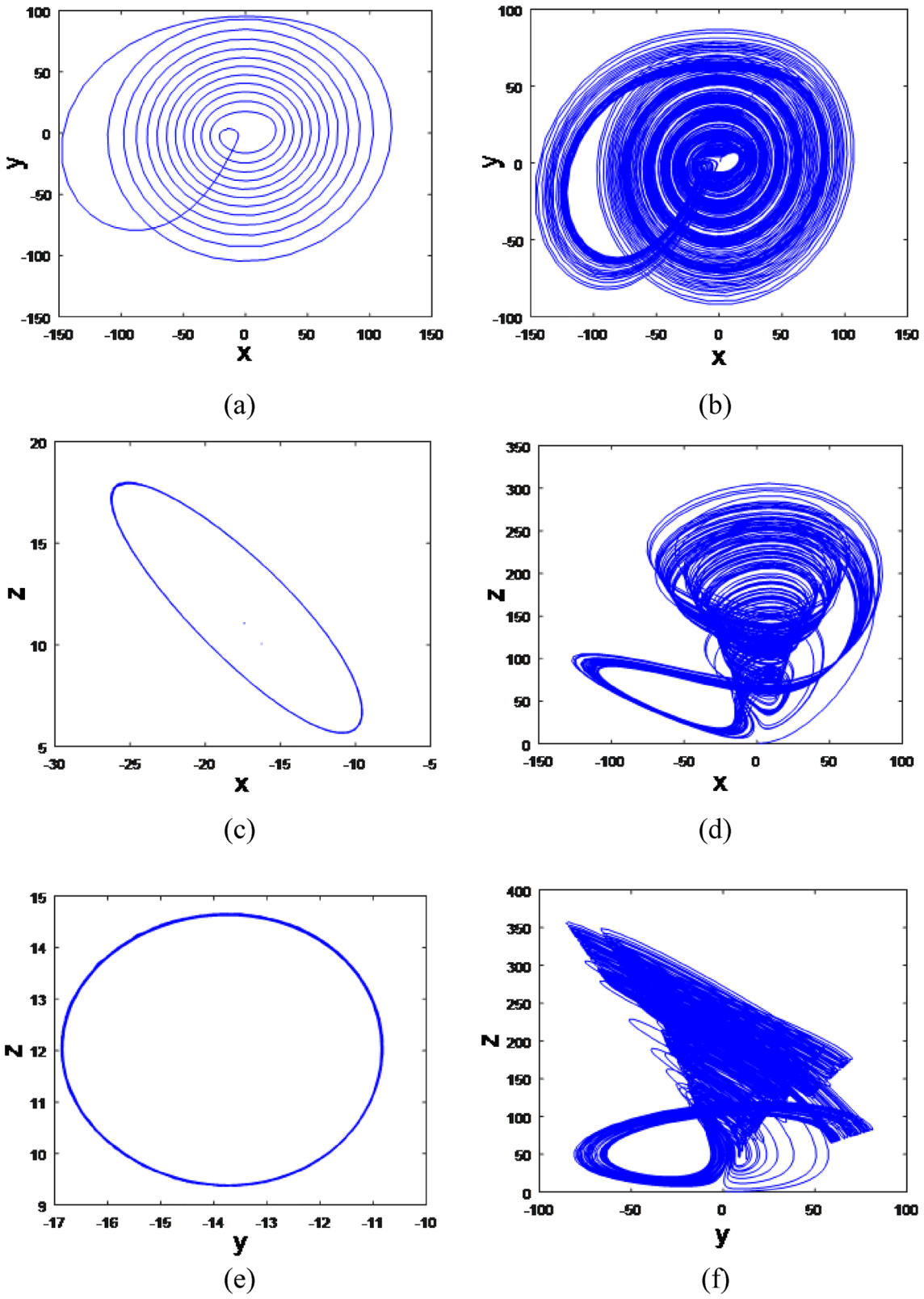


Fig. 3 Phase plots of system (1) for specifics values of its parameters

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Also, by fixing the parameters a = 20 and b = 50, and c allowed in the range [10, 20], we obtain the plots for the respective Lyapunov exponents spectrum (see Fig. 2e) and bifurcation figure (see Fig. 2f). When 10 < c < 18, then, the system (1) would exhibit chaotic behaviour as illustrated in Fig. 3f. The corresponding LEs are: $LE_1 = 6.473$, $LE_2 = 0$, $LE_3 = -38.473$. When 18 < c < 20, system (1) exhibits periodic behaviour as depicted in Fig. 3e. The corresponding LEs are: $LE_1 = 0$, $LE_2 = -10.288$, $LE_3 = -28.712$.

Circuit Design

For this proposed 3D chaotic system (1), its analog circuit design is implemented using MULTISIM by employing analog multipliers AD633JN, operational amplifiers TL082CD, resistors, and capacitors. The schematic design of this 3D chaotic system is illustrated in Fig. 4.

Applying Kirchhoff's laws to Fig. (4), we obtain the following corresponding equations for the circuitry of system (1):

$$\begin{cases} \dot{x} = \frac{1}{R_1 C_1}x + \frac{1}{R_2 C_1}y + \frac{1}{R_3 C_1}yz \\ \dot{y} = \frac{1}{R_4 C_2}x - \frac{1}{R_5 C_2}xz - \frac{1}{R_6 C_2}V_1 \\ \dot{z} = \frac{1}{R_7 C_3}x^2 + \frac{1}{R_8 C_3}xz - \frac{1}{R_9 C_3}z \end{cases} \tag{7}$$

$$\begin{cases} C_1 = C_2 = C_3 = 1nF \\ R_1 = R_1 = 26.67k\Omega \\ R_3 = R_5 = 40k\Omega \\ R_4 = 8k\Omega \\ R_6 = R_9 = 400k\Omega \\ R_7 = R_8 = 4M\Omega \\ R_{10} = R_{11} = R_{12} = R_{13} = 40k\Omega \\ V_1 = 1V \end{cases} \tag{8}$$

MultiSim outputs are shown in Fig. 5, which in accordance with the output from MATLAB shown earlier in Fig. 1. These results confirm the physical feasibility of the proposed mathematical model.

Pseudo Random Number Generator (PRNG) Based on The New 3D Chaotic System

One of the most common applications performed with chaotic systems is PRNG applications [36–38]. The reason for this is to show the adequacy of the proposed systems for applications by testing the dynamic properties of chaotic systems and their ability to generate random numbers. For this purpose, this section presents a novel PRNG constructed using the idea of proposed 3D chaotic system. The flowchart of the developed PRNG is illustrated in Fig. 6.

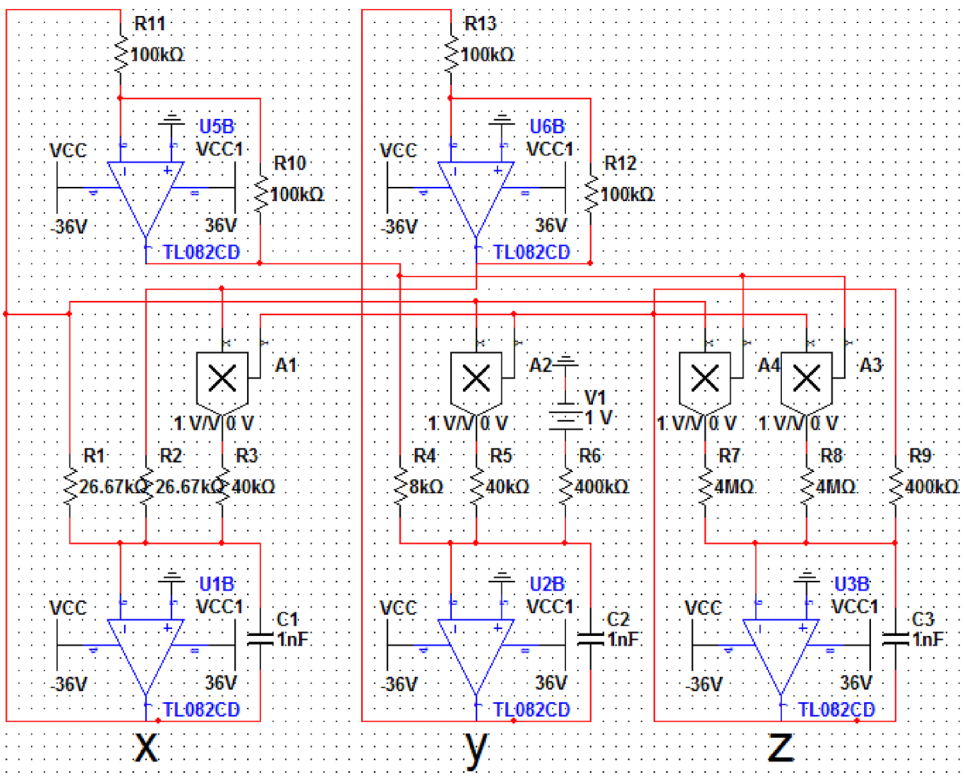


Fig. 4 The schematic of the circuit

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

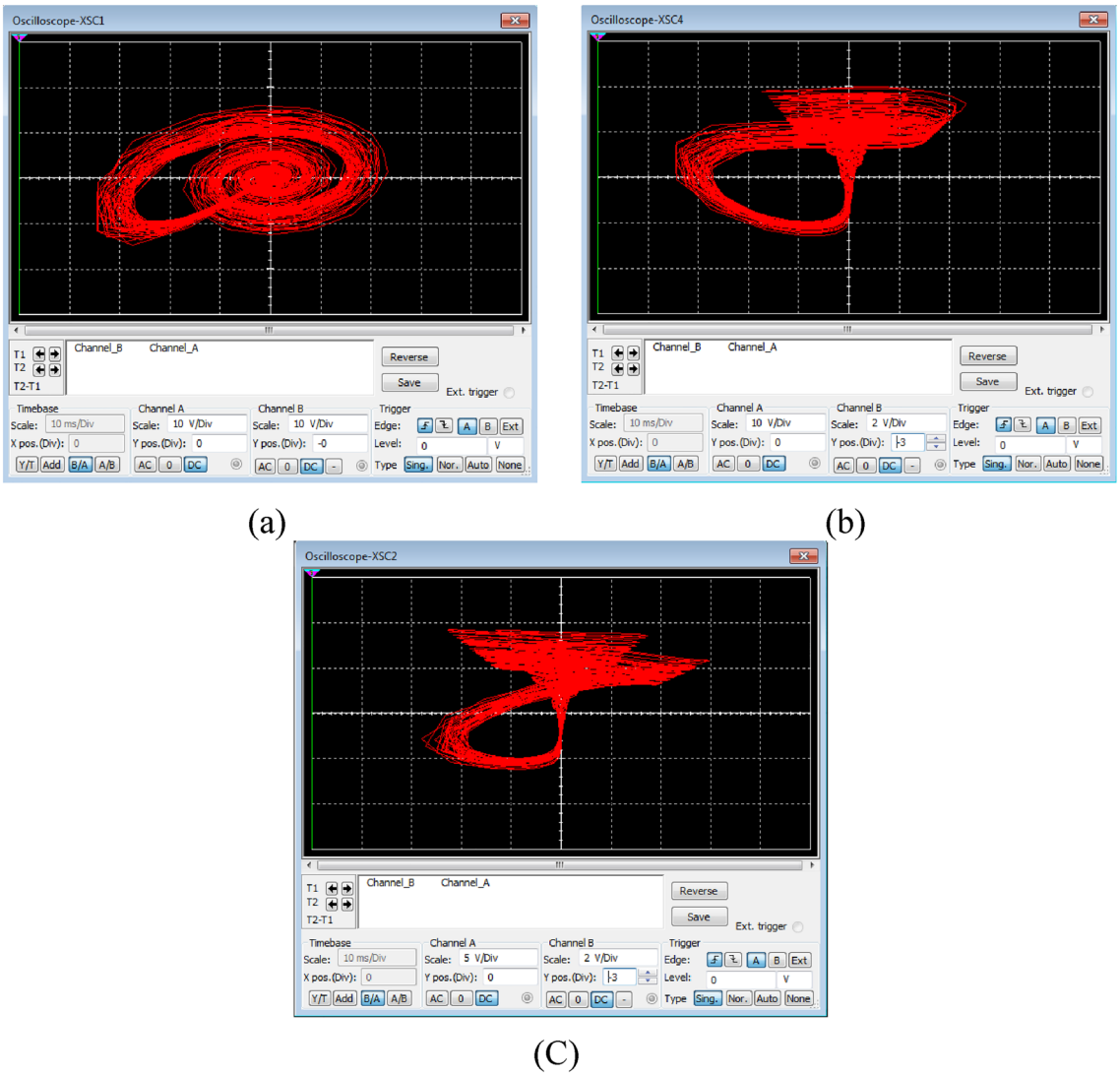


Fig. 5 MultiSim outputs of the highly chaotic system (1) equivalent circuit

As shown in Fig. 6, first the required system parameters, initials, and the number of bits that would be obtained from the state variables in each iteration are determined. State variables are calculated using the Runge–Kutta 4 (RK4) algorithm according to the determined values. The float values in each calculated state variable are converted to binary form and XORed by taking the determined number of LSBs. Here, the XOR operation is to increase the randomness by evaluating the dynamic properties of all state variables. The bits removed from the XOR operation are added to the test array. When the test sequence reaches 1,000,000 bits, the internationally accepted randomness test N I ST – 800 – 22 is applied. There are a total of 15 different tests in this test suit, and in order for an array to be considered random, it must take a value in the range of 1–0.001 from these tests. As seen in Table 2, all results from PRNG are successful. Accordingly, the PRNG developed using the new 3D system has sufficient randomness. If even one of the tests is unsuccessful, the processes are re-turned to the beginning, the input parameters are changed, and a retry is made.

PRNG Based Image Encryption

Sect. "PRNG Based Image Encryption" will demonstrate the implementation of the PRNG-based image encryption on higher-level engineering application. In Fig. 7, the decryption and encryption processes of the implemented application can be seen.

For the encryption process [39], firstly, the image to be encrypted is given as input. Pixel values in this image are converted from decimal to binary. On the other hand, the

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

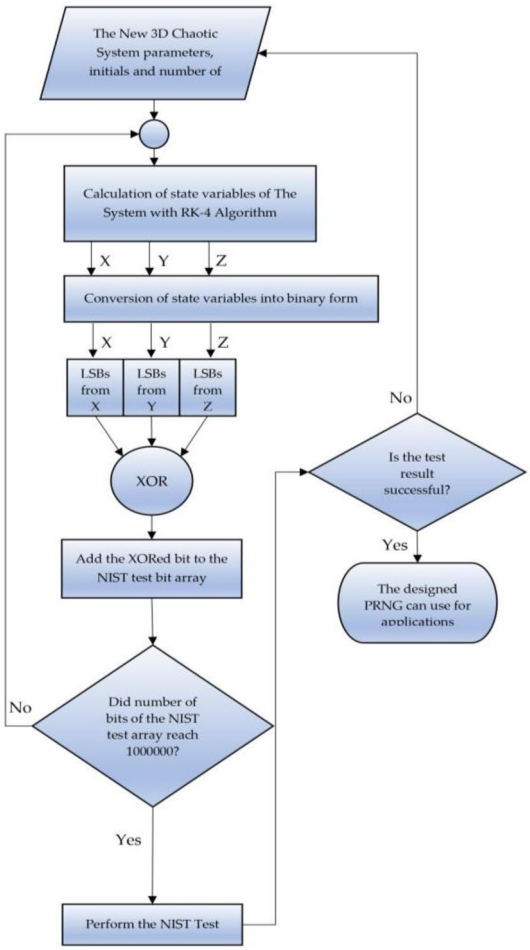


Fig. 6 Matlab Flowchart of PRNG

Table 2 Statistical Tests $X \oplus Y \oplus Z$

	$X \oplus Y \oplus Z$	
Statistical Tests	*P*-value	Results
Random-Excursions Variant Test (x = -9)	0,227,294,828	Pass
Random-Excursions Test (x = -4)	0,369,276,808	Pass
Cumulative-Sums Test	0,405,768,097	Pass
Approximate Entropy Test	0,124,880,062	Pass
Serial Test-1	0,790,547,397	Pass
Serial Test-2	0,647,381,516	Pass
Linear-Complexity Test	0,394,263,523	Pass
Maurer's Universal Statistical Test	0,521,174,276	Pass
Overlapping Templates Test	0,280,869,179	Pass
Non-Overlapping Templates Test	0,002257188	Pass
Discrete Fourier Transform Test	0,861,585,725	Pass
Binary Matrix Rank Test	0,324,783,068	Pass
Longest-Run Test	0,286,026,655	Pass
Runs Test	0,452,847,555	Pass
Block-Frequency Test	0,695,623,736	Pass
Frequency (Monobit) Test	0,411,076,897	Pass

parameters of the system and that of the solution for the proposed 3D system are determined. Again, by obtaining the state variables with the RK4 algorithm, bit arrays are obtained with the PRNG developed in the previous section. The image's binary and PRNG bits are encrypted with the XOR operation. New pixel values are obtained by converting the encrypted bit array from binary to decimal, and an encrypted image is formed.

As shown in Fig. 6, first the required system parameters, initials, and the number of bits that would be obtained from the state variables in each iteration are determined. State variables are calculated using the Runge–Kutta 4 (RK4) algorithm according to the determined values. The float values in each calculated state variable are converted to binary form and XORed by taking the determined number of LSBs. Here, the XOR operation is to increase the randomness by evaluating the dynamic properties of all state variables. The bits removed from the XOR operation are added to the test array. When the test sequence reaches 1,000,000 bits, the internationally accepted randomness test NIST-800-22 is applied.

In Fig. 7, the decryption and encryption processes of the implemented application can be seen. For the encryption process [39], firstly, the image to be encrypted is given as input. Pixel values in this image are converted from decimal to binary. On the other hand, the parameters of the system and that of the solution for the proposed 3D system are determined. Again, by obtaining.

the state variables with the RK4 algorithm, bit arrays are obtained with the PRNG developed in the previous section. The image's binary and PRNG bits are encrypted with the XOR operation. New pixel values are obtained by converting the encrypted bit array from binary to decimal, and an encrypted image is formed.

In the process of decryption, on the one hand, the image encrypted is given as input, and on the other hand, the bit array produced with 3D chaotic system-based PRNG is given. Encrypted image pixel values are transformed to binary form and XOR again where the bit array is taken from PRNG, and the decrypted image is obtained.

Performance Analysis

Experimental Environment

A histogram is a graphical representation that plots pixel values to illustrate the distribution of pixels in images. The statistical properties of images are conveyed through histograms. Random numbers generated from chaotic systems are uniformly distributed as white noise, in accordance with the histogram of the encryption algorithm. In histograms, the distributions of strongly encrypted images must be uniform.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

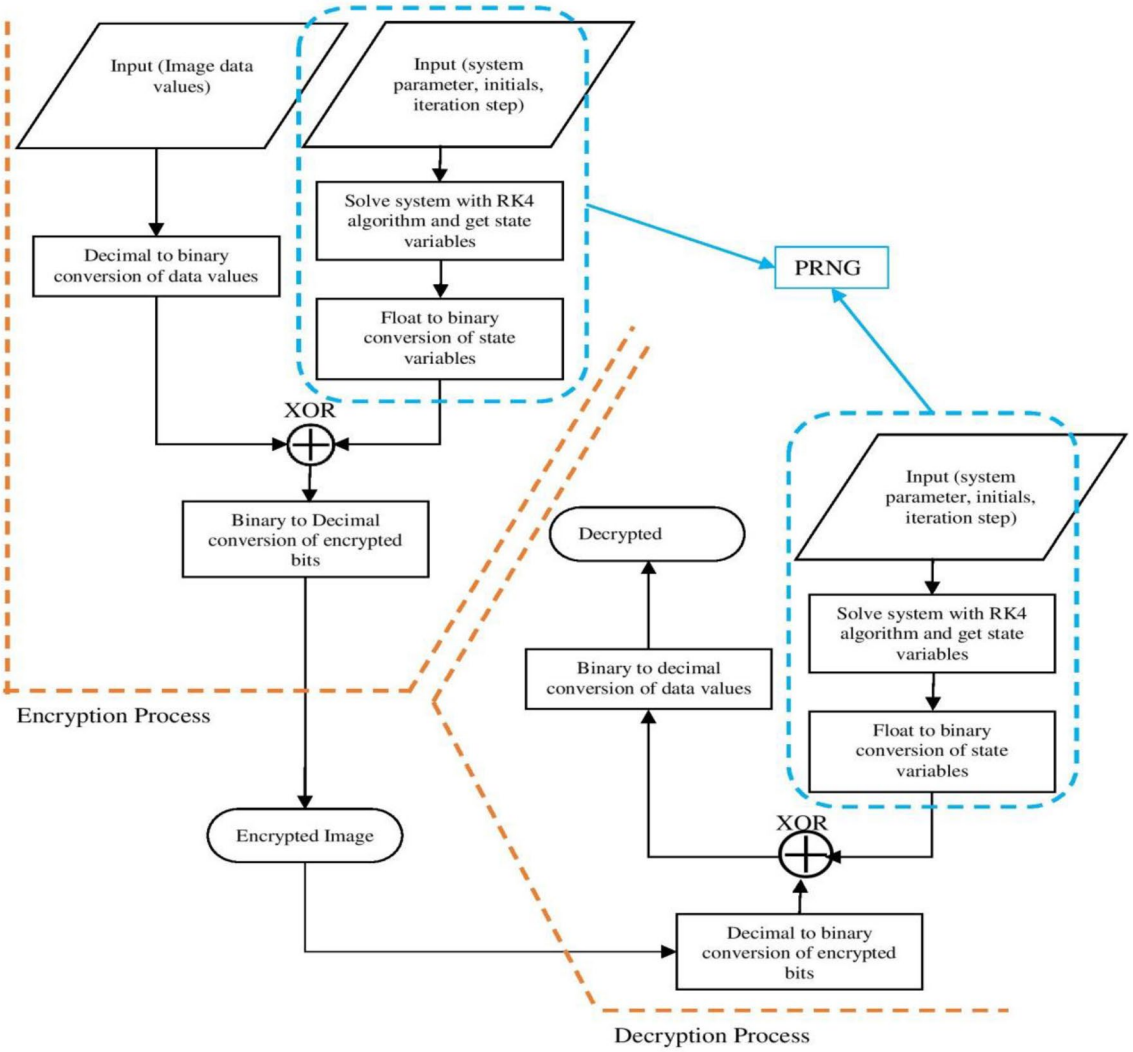


Fig. 7 Flowchart of encryption and decryption

A histogram, representing the distribution of pixel values in an image, is denoted by H. If the matrix I represents an image matrix, then the histogram H is given by:

$$H(i) = count\{pixelsI(x, y) : I(x, y) = 1\} \tag{9}$$

Correlation distribution serves as a crucial tool employed to assess and enhance the security properties of encryption algorithms. Robust encryption ensures that the correlation distributions of encrypted images diverge, thereby bolstering security.

The correlation distribution C between two images is given by:

$$C(i, j) = \frac{\sum_x \sum_y \left[I_1(x, y)\right]\left[I_2(x + i, y + j) - \mu_2\right]}{\sigma_1 \sigma_2} \tag{10}$$

Four different images (cameraman, baboon, pepper, and Lena) were used to demonstrate the performance and effectiveness of the encryption application. Histogram, Correlation, Entropy, Contrast, Homogeneity, Energy, MAD (MAE), Encryption Quality, NPCR, UACI, MSE, and PSNR results were obtained with the obtained encrypted images. The resulting encrypted images, histograms, and correlation distributions are given in Figs. 8, 9, 10, 11. When Figs. 8, 9, 10, 11 are examined, it is seen that all encrypted image

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

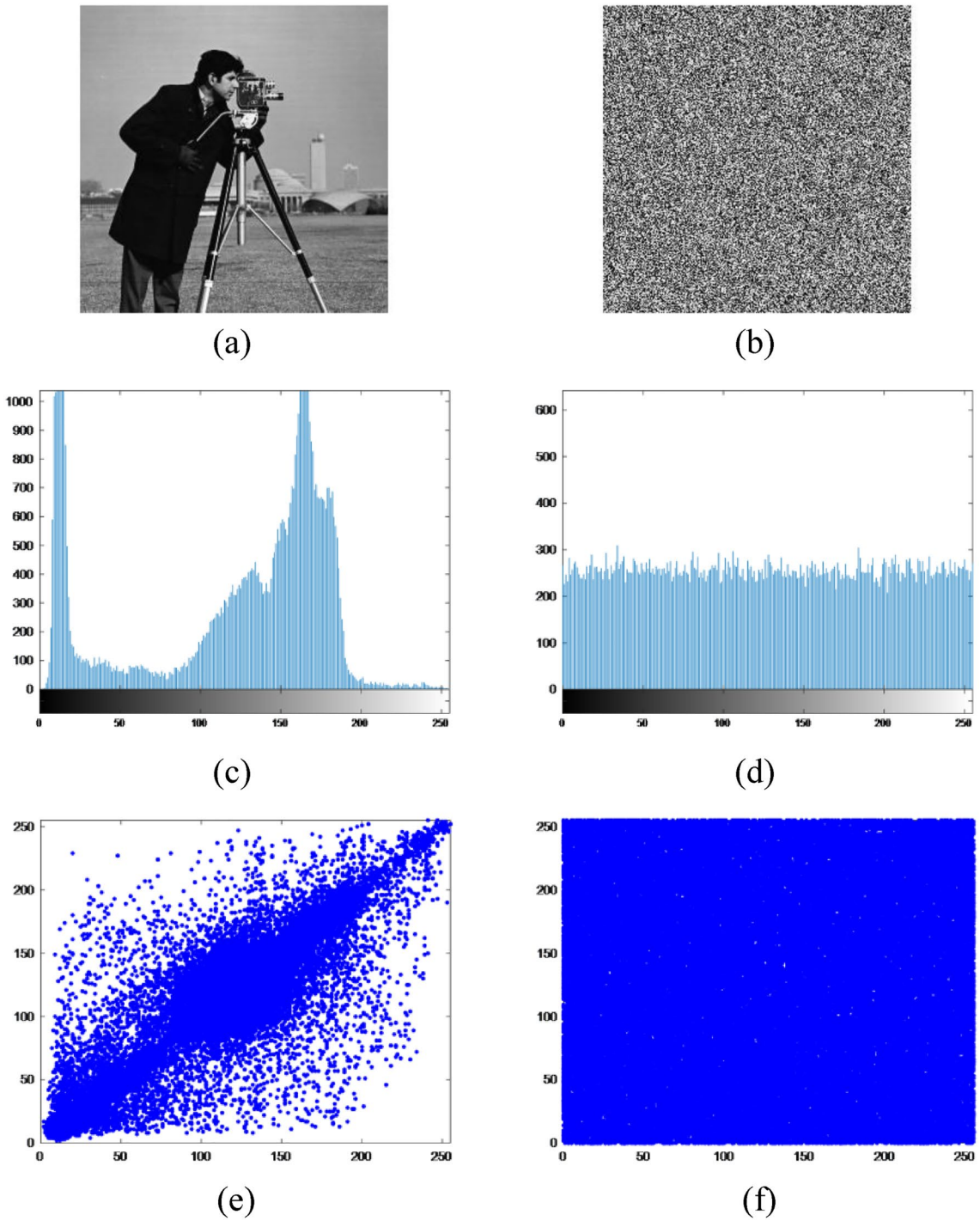


Fig. 8 **a** Original and **b** encrypted images of cameraman: **c** original—**d** encrypted histograms and **e** original—**f** encrypted correlation distributions

pixels, histograms, and correlation distributions have a perfectly homogeneous distribution. This shows that the implemented encryption application performs well for different images.

Figure 12 shows the original and decrypted images of cameraman, baboon, pepper, and Lena. For all images in Fig. 12, the Peak signal-to-noise ratio (PSNR), in Eq. 11,

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

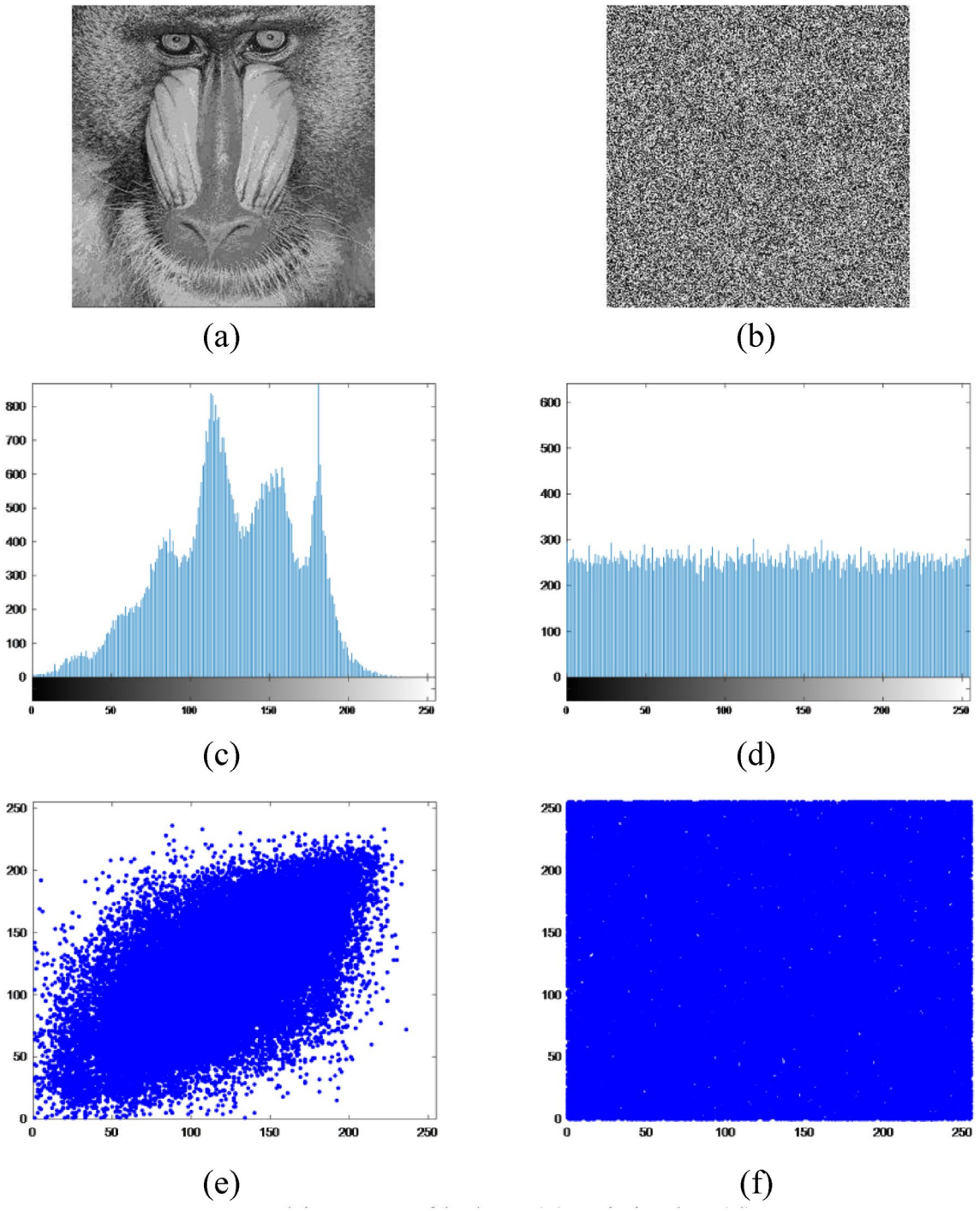


Fig. 9 **a** Original and **b** encrypted images of baboon: **c** original—**d** encrypted histograms and **e** original—**f** encrypted correlation distributions

and Multiscale Structural Similarity (MSSIM), in Eq. 13, values between original and decrypted are calculated as infinitive and 1, respectively. The ratio of a signal's maximum potential power to the power of corrupting noise that degrades the representational fidelity is known as PSNR in engineering. Furthermore, Multiscale SSIM (MSSIM), a more sophisticated version of structural similarity index (SSIM), is similar to multiscale processing in the early visual system in that it operates at multiple scales using a multi-step down sampling procedure. By calculating the SSIM between the original and decrypted images, one can quantify perceived quality. MSSIM index through the

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

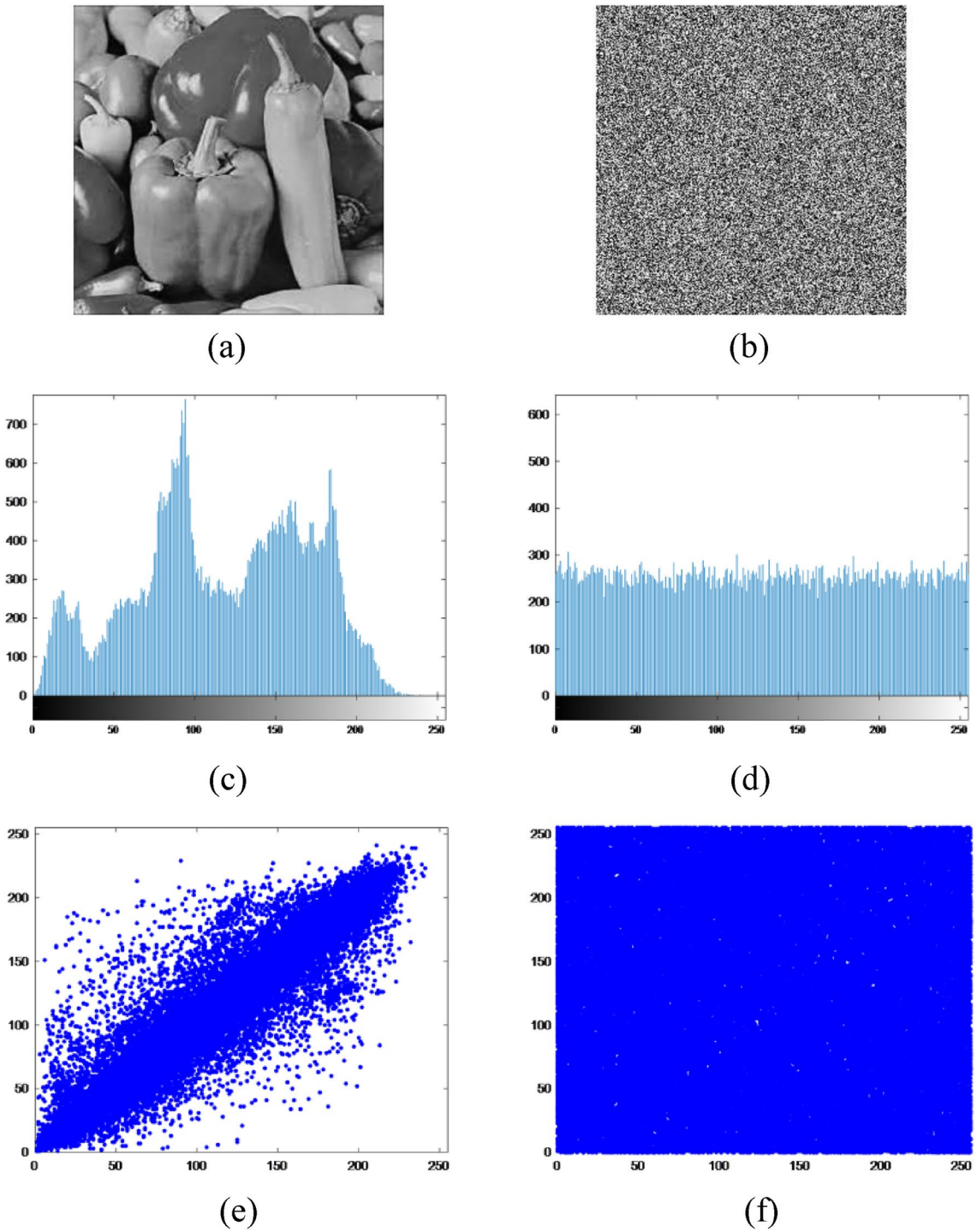


Fig. 10 **a** Original and **b** encrypted images of pepper: **c** original—**d** encrypted histograms and **e** original—**f** encrypted correlation distributions

amalgamation of multiple image versions' SSIM indexes at different scales.

$$PSNR = 10log_{10}(peakval^2/MSE) \tag{11}$$

In Eq. 11 peakval is either specified by the user or taken from the range of the image data type. For example, for an image of data type uint8, the peakval is 255. MSE is the mean square error between original and decrypted images.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

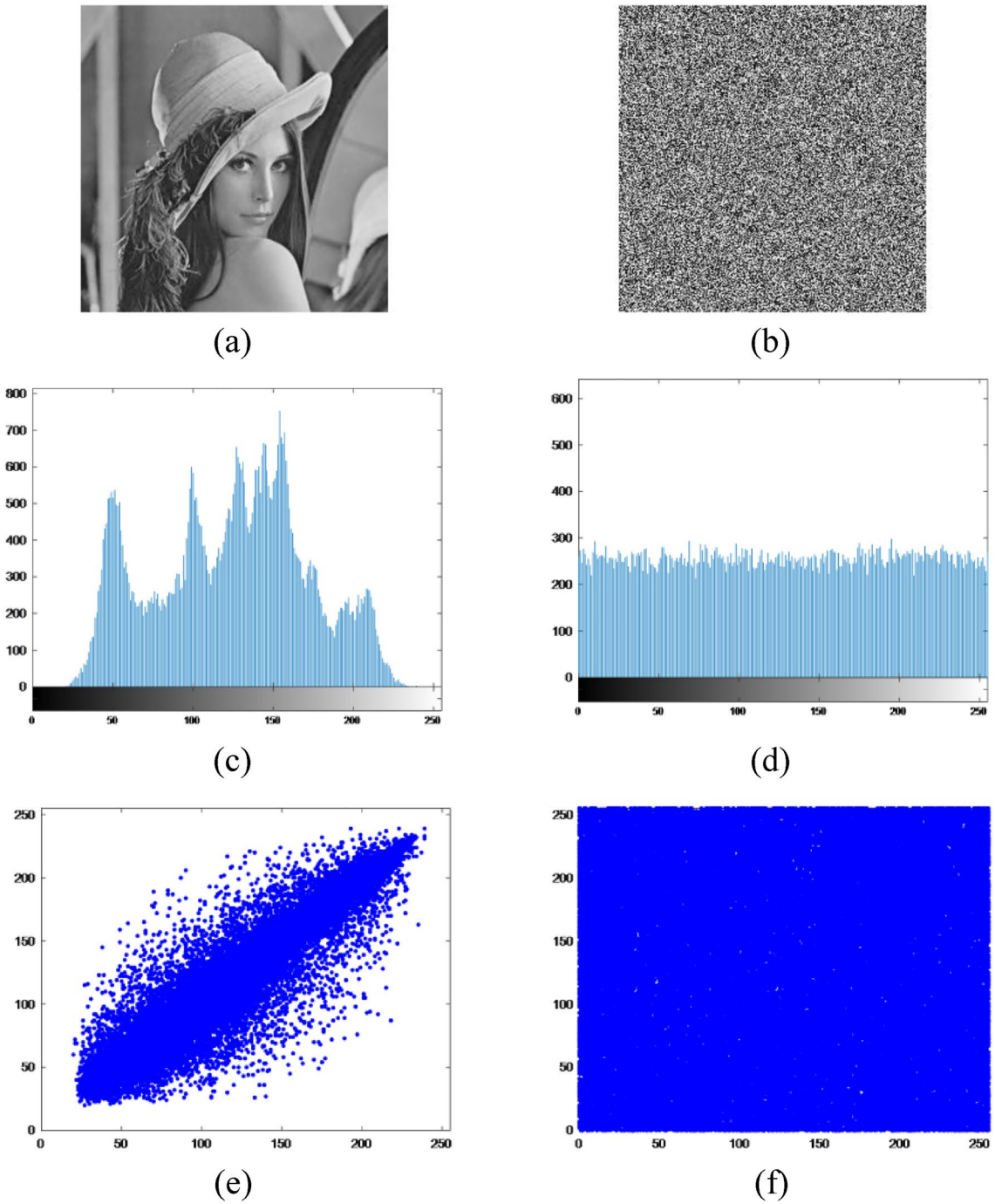


Fig. 11 **a** Original and **b** encrypted images of lena: **c** original—**d** encrypted histograms and **e** original—**f** encrypted correlation distributions

$$SSIM(x,y) = \frac{(2\mu_x\mu_x + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{12}$$

$$MSSIM(x,y) = \frac{1}{M}\sum_{j=1}^{M} SSIM(x_j, y_j) \tag{13}$$

In Eq. 12 μ_x, μ_y, σ_x,σ_y, and σ_{xy} are the local means, standard deviations, and cross-covariance for original and decrypted images. In Eq. 13, M is the dimension of the images.

The reason why the PSNR and MSSIM results obtained for all images in Fig. 12 are infinitive and 1 is that the original and decrypted images are the same. The reason why the

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

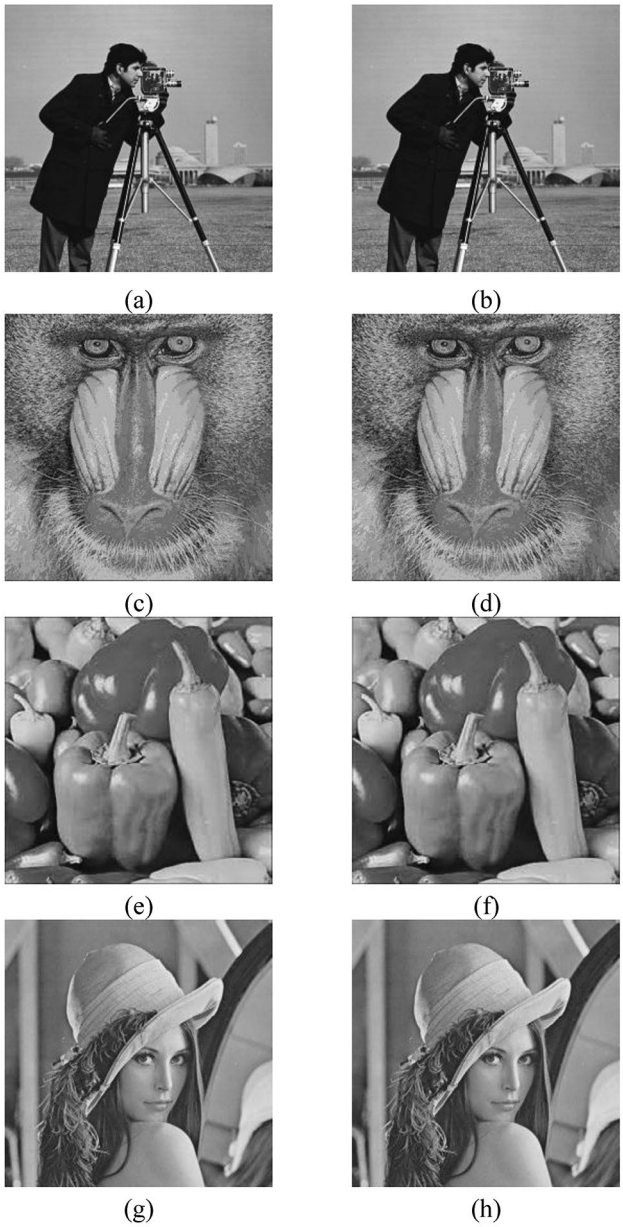


Fig. 12 **a** original cameraman, **b** decrypted cameraman, **c** original baboon, **d** decrypted baboon, **e** original pepper, **f** decrypted pepper, **g** original Lena, **h** decrypted Lena

two images are the same is that there are no differences or noise-generating errors such as compression, floating point errors, quantization errors caused by the encryption and decryption algorithms presented in the study. Because in these algorithms, pixels are directly processed as binary and bit-based operations are performed. Therefore, the resulting decrypted image is the same as the original image. Therefore, PSNR and MSSIN take the values infinitive and 1.

Next, we give details about the computer we used and the running time of encryption and decryption process to evaluate the practicability of the pro- posed method in real-world contexts. The specifications of the computer used are processor 11th Gen Intel(R) Core (TM) i5-11400H @ 2.70 GHz 2.69 GHz, RAM 16.0 GB and the system has 64-bit operating system, ×64-based processor. On this computer, the encryption and decryption times of all images vary between 0.008 and 0.012 s.

Results and Discussion

The correlation, Entropy, Contrast, Homogeneity, Energy, MAD (MAE), Encryption Quality, NPCR, UACI, MSE, and PSNR statistical results are given in Table 3. In Table 3, correlation, entropy, contrast, homogeneity, and energy results are given for original and encrypted images separately to show the effect of the encryption process. According to these results, original images with different properties before encryption take values close to each other after encryption. This again shows that the encryption process performs well independently of the original images. On the other hand, correlation, entropy, contrast, homogeneity, and energy results obtained for encrypted images are quite good values for any encrypted images. MAD (MAE), Encryption Quality, NPCR, UACI, MSE, and PSNR results are presented in Table 3 demonstrate the relationship between encrypted images and the original images and to evaluate a performance accordingly. By examining these results, it is obvious that for all the four images considered, there is not much relationship between the original images and those encrypted. So, these results show that original images become completely different images after encryption. Furthermore, for the encrypted pepper image, we compared our proposed method with seven recent encryption algorithms [40–46] and presented our comparison results in Table 4.

According to all these results, we conclude as follows: the 3D chaotic system-based encryption application presented in this paper has a very good performance.

Conclusion

In this paper, we presented a new 3D dynamical system with four quadratic nonlinear terms and showed the proposed chaotic system has two saddle- foci, unstable, equilibrium points. Thus, the proposed chaotic system exhibits self-excited chaotic attractors. Dynamical analysis methods such as Lyapunov exponents spectrum, bifurcation diagrams, and phase portraits were carried out to explore the complex dynamical behaviors of the proposed chaotic system and analyze its basic qualitative properties. We showed that the maximal Lyapunov exponent (MLE) of the new chaotic system is 7.196, which is a high value. Thus, we conclude that the proposed highly chaotic system exhibits high complexity

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Table 3 Statistical analysis results

	Cameraman	Cameraman	Baboon	Baboon	Pepper	Pepper	Lena	Lena
Test	Original	Encrypted	Original	Encrypted	Original	Encrypted	Original	Encrypted
Correlation	0.9546	-0.0028	0.8380	-0.0023	0.9803	-0.0066	0.9786	-0.0016
Entropy	7.0435	7.9970	7.3129	7.9973	7.5897	7.9969	7.4519	7.9972
Contrast	0.5866	0.3970	0.9083	0.4376	0.3192	0.3865	0.3575	0.3880
Homogeneity	0.8964	0.9929	0.7304	0.9921	0.8904	0.9930	0.8816	0.9930
Energy	0.1826	0.9838	0.0774	0.9822	0.1118	0.9842	0.1228	0.9842
MAD or MAE	–	79.8421	–	70.6711	–	75.7706	–	73.3092
Enc. Quality	–	39,138	–	48,196	–	41,578	–	44,900
NPCR	–	99.5834	–	99.6582	–	99.6002	–	99.6063
UACI	–	31.3106	–	27.7141	–	29.7139	–	28.7487
MSE	–	9497.126	–	7149.870	–	8433.320	–	7799.106
PSNR	–	39.7759	–	– 38.5429	–	– 39.2599	–	– 38.9204

Table 4 Comparison Table giving Encryption results for the Pepper Image

Name of the Method	Entropy	Correlation	Differential Attack	
			NPCR	UACI
Proposed method	7.9973	−0.0016	99.6582	31.3106
Zhang et al. [40]	7.9976	−0.0059	99.6246	33.4043
Li et al. [41]	7.9993	−0.0038	99.6094	30.9762
Wang et al. [42]	7.9972	0.0042	99.9802	30.0634
Li et al. [43]	7.9021	−0.0013	99.6090	33.4664
Musanna et al. [44]	7.9962	0.0132	99.5778	33.4431
Liu et al. [45]	7.9917	0.0039	99.6223	33.4312
Kaur et al. [46]	7.9956	0.0128	99.6078	32.9312

and it will be very useful for applications in cryptography, encryption and secure communications.

We also employed the Multisim soft- ware to affirmed the feasibility of the proposed system using electronic circuitry design. Finally, PRNG-based image encryption has been developed and applied for encryption. Our experimental results conclusively demonstrate that the 3D chaotic system-based encryption application we presented in this work is effective and performs well.

Data availability Not applicable.

Declarations

Conflict of interests The authors declare that they have no conflicts of interest.

Ethical Approval Not applicable.

References

1. Sambas A, Vaidyanathan S, Zhang X, Koyuncu I, Bonny T, Tuna M, Alcin M, Zhang S, Sulaiman IM, Awwal AM, Kumam P. A novel 3D chaotic system with line equilibrium: Multi-stability, integral sliding mode control, electronic circuit, FPGA implementation and its image encryption. IEEE Access. 2022;10:68057–74.
2. Guo, S., Fu, Y., Yu, L.: An encrypted multitone modulation method for physical layer security based on chaotic cryptography. Physical Communication 47 (2021). Article ID 101389
3. Singh JP, Roy BK. A more chaotic and easily hardware implementable new 3-d chaotic system in comparison with 50 reported systems. Nonlinear Dyn. 2018;93(3):1121–48.
4. Yang Q, Qiao X (2019) Constructing a new 3D chaotic system with any num- ber of equilibria. Int J Bifurcation Chaos 29(5). Article ID 1950060
5. Signing VRF, kengne J, Kana LK (2018) Dynamic analysis and multista- bility of a novel four-wing chaotic system with smooth piecewise quadratic nonlinearity. Chaos, Solitons and Fractals 113, 263–274
6. Vaidyanathan S, Benkouider K, Sambas A. A new multistable jerk chaotic system, its bifurcation analysis, backstepping control-based syn- chronization design and circuit simulation. Arch Control Sci. 2022;32(1):123–52.
7. Chowdhury SN, Ghosh D. Hidden attractors: A new chaotic system without equilibria. Euro Phys J Spec Topics. 2020;229(6):1299–308.
8. Ren S, Panahi S, Rajagopal K, Akgul A, Pham V, Jafari S (2018) A new chaotic flow with hidden attractor: The first hyperjerk system with no equilibrium. Zeitschrift fu¨r Naturforschung A 73(3): 239–249
9. Dong C (2022) Dynamics, periodic orbit analysis, and circuit implementation of a new chaotic system with hidden attractor. Fractal Fractional 6(4) (2022). Article ID 190
10. Sambas A, Mmat M, Vaidyanathan S, Mohamed M, Sanjaya W. A new 4-d chaotic system with hidden attractor and its circuit imple- mentation. Int J Eng Technol. 2018;7(3):1245–50.
11. Yu F, Zhang Z, Shen H, Huang Y, Cai S, Du S (2022) Fpga imple- mentation and image encryption appli-cation of a new prng based on a memristive hopfield neural network with a special activation gradient. Chin Phys B 31(2). Article ID 020505

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

12. AbdElHaleem SH, Abd-El-Hafiz SK, Radwan AG (2022) A generalized framework for elliptic curves based PRNG and its utilization in image encryption. Sci Rep 12(1). Article ID 13278
13. Abd El-Latif AA, Abd-El-Atty B, Venegas-Andraca SE (2020) Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption. Physica A 547 (2020). Article ID 123869
14. Gafsi M, Abbassi N, Hajjaji MA, Malek J, Mtibaa A (2020) Improved chaos-based cryptosystem for medical image encryption and decryption. Scientific Programming 2020. Article ID 6612390
15. Mondal B, Mandal T. A light weight secure image encryption scheme based on chaos and dna computing. J King Saud Univ-Comput Inform Sci. 2017;29(4):499–504.
16. Namasudra S, Deka GC. Advances of DNA computing in cryptogra- phy. New York, USA: CRC Press; 2018.
17. Zhu H, Zhang X, Xing H, Feng L. Lightweight terminal cross-domain authentication protocol in edge computing environment. Chinese J Netw Inform Secur. 2023;9(4):74–89.
18. Kumar ASK, Razak TA. A secure crypto-based data outsourcing model for monitoring the smart environment in cloud. Int J Sci Technol Res. 2020;9(1):124–31.
19. Das S, Singh MP, Namasudra S (2023) A lightweight authentication and key agreement protocol for Iot-based smart healthcare system. (2023). DOI:https://doi.org/10.1109/WCONF58270.2023.10235225
20. Singh A, Kumar A, Namasudra S (2024) DNACDS: Cloud IoE big data security and accessing scheme based on DNA cryptography. Front Comput Sci 18(1) (2024). Article ID 181801
21. Namasudra, S., Nath, S., Majumder, A.: Profile Based Access Control Model in Cloud Computing Environment. (2014). DOI:https://doi.org/10.1109/ICGCCEE.2014.6921420
22. Hameed A, Violos J, Leivadeas A. A deep learning approach for IoT traffic multi-classification in a smart-city scenario. IEEE Access. 2022;10:21193–210.
23. Das S, Namasudra S (2022) A lightweight and anonymous mutual authentica- tion scheme for medical big data in distributed smart healthcare systems. IEEE/ACM Trans Comput Biol Bioinform 1–12 (2022). DOI:https://doi.org/10.1109/TCBB.2022.3230053
24. Castro, F., Impedovo, D., Pirlo, G.: A medical image encryption scheme for secure fingerprint-based authenticated transmission. Applied Sciences 13(10) (2023). Article ID 6099
25. Patel S, Vaish A (2023) Block based visually secure image encryption algorithm using 2d-compressive sensing and nonlinearity. Optik 272. Article ID 170341
26. Zhu L, Jiang D, Ni J, Wang X, Rong X, Ahmad M. A visually secure image encryption scheme using adaptive-thresholding sparsification compression sensing model and newly-designed memristive chaotic map. Inf Sci. 2022;607:1001–22.
27. Wolf A, Swift JB, Swinney HL, Vastano JA. Determining lyapunov exponents from a time series. Physica D. 1985;16(3):285–317.
28. Grond F, Diebner HH, Sahle S, Mathias A, Fischer S, Rossler OE. A robust, locally interpretable algorithm for lyapunov exponents. Chaos, Solitons Fractals. 2003;16(5):841–52.
29. Silva-Juarez A, Tlelo-Cuautle E, de la Fraga LG, Li R Optimization of the Kaplan-Yorke dimension in fractional-order chaotic oscillators by metaheuristics. Applied Mathematics and Computation 394 (2021). Article ID 125831
30. Chen Z-M. A note on Kaplan-Yorke-type estimates on the fractal dimension of chaotic attractors. Chaos, Solitons Fractals. 1993;3(5):575–82.
31. Dong C (2022) Dynamic analysis of a novel 3d chaotic system with hidden and coexisting attractors: Offset boosting, synchronization, and circuit realization. Fractal Fractional 6(10). Article ID 547
32. Qiu H, Xu X, Jiang Z, Sun K, Cao C (2023) Dynamical behaviors, circuit design, and synchronization of a novel symmetric chaotic system with coexisting attractors. Scientific Reports 13(1) (2023). Article ID 1893
33. Liu, T., Yan, H., Banerjee, S., Mou, J.: A fractional-order chaotic system with hidden attractor and self-excited attractor and its DSP implementation. Chaos, Solitons and Fractals 145 (2021). Article ID 110791
34. Zhou W, Wang G, Shen Y, Yuan F, Yu S (2018) Hidden coexisting attrac- tors in a chaotic system without equilibrium point. International Journal of Bifurcation and Chaos 28(10) (2018). Article ID 1830033
35. Rahman Z-A, Jasim BH (2022) Hidden dynamics investigation, fast adaptive synchronization, and chaos-based secure communication scheme of a new 3d fractional-order chaotic system. Inventions 7(4) (2022). Article ID 108
36. Kacar S. A new data-hiding algorithm for multi-channel biomedical signals based on variable-order fractional chaotic neural networks with frequency effect. Euro Physical Journal. 2022;231(5):929–43.
37. Kacar S. Digital circuit implementation and PRNG-based data secu- rity application of variable-order fractional Hopfield neural network under electromagnetic radiation using Gr´' unwald-Letnikov method. Euro Phys J. 2022;231(10):1969–81.
38. Aricioglu B, Kacar S. Circuit implementation and PRNG applications of time delayed Lorenz system. Chaos Theory Appl. 2022;4(1):4–9.
39. Benkouider K, Bouden T, Sambas A, Mohamed MA, Sulaiman IM, Mamat M, Ibrahim MAH. Dynamics, control and secure transmission electronic circuit implementation of a new 3d chaotic system in comparison with 50 reported systems. IEEE Access. 2021;9:152150–68.
40. Zhang X, Wang L, Zhou Z, Niu Y. A chaos-based image encryption technique utilizing Hilbert curves and H-fractals. IEEE Access. 2019;7:74734–46.
41. Li H, Wang Y, Zuo Z. Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms. Opt Lasers Eng. 2019;115:197–207.
42. Wang X, Akgul A, Kacar S, Pham V-T (2017) Multimedia security application of a ten-term chaotic system without equilibrium. Complexity 2017 (2017). Article ID 8412093
43. Li Z, Peng C, Tan W, Li L (2021) An effective chaos-based image encryp- tion scheme using imitating jigsaw method. Complexity 2021. Article ID 8824915
44. Musanna F, Kumar S. A novel fractional order chaos-based image encryption using fisher yates algorithm and 3-D cat map. Multimedia Tools and Applications. 2019;78(11):14867–95.
45. Liu H, Xu Y, Ma C (2020) Chaos-based image hybrid encryption algorithm using key stretching and hash feedback. Optik 216. Article ID 164925
46. Kaur G, Agarwal R, Patidar V. Chaos based multiple order optical transform for 2D image encryption. Eng Sci Technol Int J. 2020;23(5):998–1014.

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.

Content courtesy of Springer Nature, terms of use apply. Rights reserved.

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH (“Springer Nature”).
Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users (“Users”), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use (“Terms”). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.
These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.
We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.
While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval , sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.
These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.
To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.
Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.
If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com