mathematics

MDPI

Article

Design of a New Chaotic System Based on Van Der Pol Oscillator and Its Encryption Application

Jianbin He [1,2,*] and Jianping Cai [1,2]

[1] College of Mathematics and Statistics, Minnan Normal University, Zhangzhou 363000, China
[2] Institute of Digital Fujian Meteorological Big Data, Minnan Normal University, Zhangzhou 363000, China
* Correspondence: hejianbin@mnnu.edu.cn

Received: 8 July 2019; Accepted: 11 August 2019; Published: 13 August 2019

Abstract: The Van der Pol oscillator is investigated by the parameter control method. This method only needs to control one parameter of the Van der Pol oscillator by a simple periodic function; then, the Van der Pol oscillator can behave chaotically from the stable limit cycle. Based on the new Van der Pol oscillator with variable parameter (VdPVP), some dynamical characteristics are discussed by numerical simulations, such as the Lyapunov exponents and bifurcation diagrams. The numerical results show that there exists a positive Lyapunov exponent in the VdPVP. Therefore, an encryption algorithm is designed by the pseudo-random sequences generated from the VdPVP. This simple algorithm consists of chaos scrambling and chaos XOR (exclusive-or) operation, and the statistical analyses show that it has good security and encryption effectiveness. Finally, the feasibility and validity are verified by simulation experiments of image encryption.

Keywords: Van der Pol oscillator; parameter control; Lyapunov exponent; chaos encryption

1. Introduction

Chaos, as one of the three important discoveries of physics in the 20st century, has attracted wide attention. Many chaotic systems are proposed, such as Chen system, Lü system, and the family of generalized Lorenz systems [1–4]. Van der Pol once studied the electron tube circuit with constant amplitude, and found the Van der Pol oscillator, which is now known as a type of stable limit cycle [5,6]. The modified Van der Pol oscillator and the chaos phenomena of forced oscillation Van der Pol–Duffing equation are investigated by adding an external excitation term [7–10]. In Reference [11], a new VdPD (Van der Pol-Duffing) Jerk oscillator is proposed based on the Van der Pol–Duffing oscillator and Jerk oscillator, and the dynamic characteristics of the VdPD-Jerk oscillator are investigated by numerical results, such as chaotic attractors and symmetrical bifurcations. The dynamics of symmetric and asymmetric Van der Pol–Duffing oscillators with a periodic force are studied in Reference [12], where the existence of parameter regions are investigated for the periodic, quasiperiodic and chaotic behaviors. In Reference [13], a four dimensional autonomous Van der Pol–Duffing snap oscillator is investigated by using standard tools of nonlinear analyis, and the synchronization is achieved by adaptive sliding mode control. An experimental demonstration of a generation of bursting patterns in the Van der Pol oscillator driven by two types of excitation is presented in Reference [14], and the periodic and chaotic bursting oscillations are generated by the slowly sinusoidal voltage source.

In the troublesome case that the chaotic system (irregularity, mess and sensitiveness) is unlikely to be useful, it should be reduced as much as possible, or totally suppressed. However, the irregularity and sensitiveness can actually be useful under certain circumstances, such as the application of information encryption and secure communication [15]. Therefore, researchers propose many encryption algorithms based on chaotic systems or hyperchaotic systems [16–22]. On the other hand, some references investigated the security of the chaos-based encryption method and some

requirements are proposed for designing chaos encryption algorithms [23,24]. In Reference [25], the application of image encryption based on nonlinear dynamics is reviewed, and a checklist is proposed for different algorithms. The chaos-based encryption algorithm is one of the useful ways to design new stream cipher algorithms for the information security.

This paper aims to study a new chaotic system based on the Van der Pol oscillator by the parameter control method. The parameter control method is different from the above references in that the external excitation term is added to Van der Pol oscillator, but only one parameter of the Van der Pol oscillator is controlled by a periodic sinusoidal function. Then, the Van der Pol oscillator with a variable parameter appears chaotic from a stable limit circle, and this kind of new chaotic system is also called a modified Van der Pol oscillator.

The main contributions are given as follows: (1) Without adding new nonlinear or linear terms, only one parameter of the linear term is controlled by the variable parameter; the other parameters and nonlinear terms remain unchanged. Then, the VdPVP appears chaotic from a stable limit circle. (2) The dynamical characters of the VdPVP are analysed via equilibrium point, the Lyapunov exponents and bifurcation diagrams, which show that the VdPVP has a positive Lyapunov exponent, i.e., it is a chaotic system. (3) An encryption algorithm based on the pseudo-random sequences generated from the VdPVP is designed. It consists of the position scrambling encryption and the values encryption by the pseudo-random via XOR (exclusive or) operation. This simple algorithm is very sensitive to the parameters and initial conditions of the VdPVP system, and it is easy to generate pseudo-random sequences. A simulation of image encryption is taken as an example to show the feasibility and effectiveness of encryption algorithms.

The paper is organized as follows. The Van der Pol oscillator is described in Section 2. A new chaotic system VdPVP is proposed by the parameter control method, and the corresponding dynamical characteristics are analyzed in Section 3. In Section 4, an encryption algorithm is designed based on the VdPVP system, and the effectiveness and security are verified by the experiments of image encryption. Section 5 provides the conclusions.

2. System Description

The Van Der Pol Oscillator is given by

$$\ddot{x} - 2\rho(1 - x^2)\dot{x} - \sigma x = 0. \tag{1}$$

If let $y = \dot{x}$, then Equation (1) is given in the form of

$$\begin{cases} \dot{x} = & y, \\ \dot{y} = \sigma x + 2\rho y - 2\rho x^2 y. \end{cases} \tag{2}$$

In addition, the Jacobi matrix is

$$J|_{(x,y)} = \begin{bmatrix} 0 & 1 \\ \sigma - 4\rho xy & 2\rho - 2\rho x^2 \end{bmatrix}. \tag{3}$$

As the equilibrium point of the dynamic system is $O(0,0)$, the Jacobi matrix at the equilibrium point is given by

$$J|_{(0,0)} = \begin{bmatrix} 0 & 1 \\ \sigma & 2\rho \end{bmatrix}. \tag{4}$$

Therefore, the eigenvalues of the Jacobi matrix are

$$\lambda_{1,2} = \rho \pm \sqrt{\rho^2 + \sigma}. \tag{5}$$

If the parameters $-1 < \rho < 0$, $\sigma = -1$, then the dynamic system (1) is locally stable at the equilibrium point $O(0,0)$ since the real part of the eigenvalues is less than zero.

When the parameters $\rho = -0.5$, $\sigma = -1$, let initial values $(x_0, y_0) = (1,1)$, and the dynamic system (1) is asymptotically stable. However, if the initial values $(x_0, y_0) = (1,2)$ and $\rho = -0.5$, $\sigma = -1$, then it will go to infinite, so the stability of dynamic system (1) is closely related to the initial values, i.e., it is locally stable in the region near equilibrium point $O(0,0)$.

When the parameters $\rho > 0$, $\sigma = -0.6$, such as $\rho = 0.5$, $\sigma = -0.6$, and let $(x_0, y_0) = (1,2)$, then the dynamic system (1) has a locally stable limit cycle, and its phase diagram is shown in Figure 1.

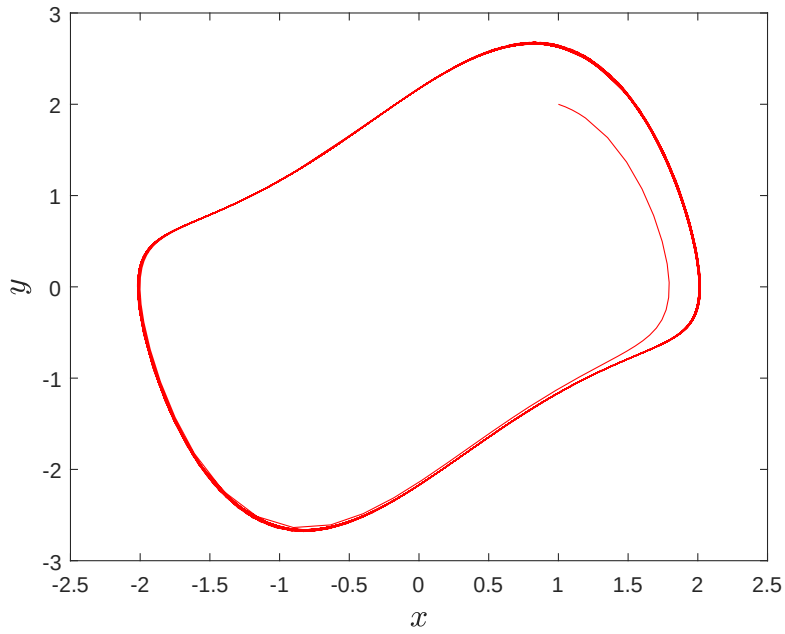


Figure 1. The phase diagram with initial values $(x_0, y_0) = (1,2)$.

3. Design and Analysis of the Dynamic System

3.1. Design of the Dynamic System

In this section, a new control method is designed to control the Van der Pol oscillator by an external excitation term. The excitation term is used to disturb the parameter of dynamic system (1), i.e., the parameter $\sigma = -k \sin \omega t$, then the new Van der Pol oscillator with variable parameter (VdPVP) is given by

$$\begin{cases} \dot{x} = & y, \\ \dot{y} = -k \sin \omega t \cdot x + 2\rho y - 2\rho x^2 y. \end{cases} \tag{6}$$

If let $t = z$, then the VdPVP is given by

$$\begin{cases} \dot{x} = & y, \\ \dot{y} = -k \sin \omega z \cdot x + 2\rho y - 2\rho x^2 y, \\ \dot{z} = 1. \end{cases} \tag{7}$$

In addition, let $\rho = 0.6$, $\omega = 5.9, k = 19.5, x_0 = 0.1, y_0 = 0.2$, the Lyapunov exponents of VdPVP are

$$\lambda_1 = 0.57,\ \lambda_2 = 0,\ \lambda_3 = -4.01.$$

Then, the VdPVP has a chaotic attractor, and its phase diagram is shown in Figure 2.

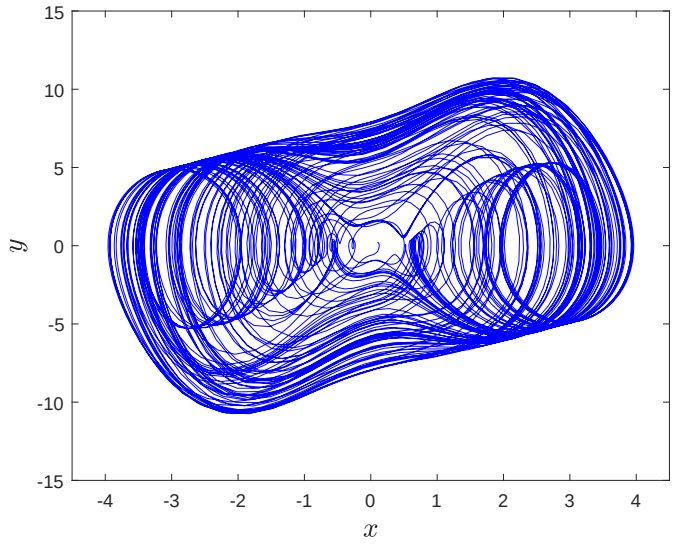


Figure 2. The attractor of dynamic system (6) with initial values $(x_0, y_0) = (0.1, 0.2)$.

3.2. Equilibrium Point

The equilibrium of VdPVP is the original point $O(0, 0)$, and the corresponding Jacobi matrix is given by

$$J|_{(0,0)} = \begin{bmatrix} 0 & 1 \\ \sigma & 2\rho \end{bmatrix}, \tag{8}$$

where $\sigma = -k \sin \omega t$, so the parameter of matrix is varied with time t and the eigenvalues of Jacobi matrix (8) are

$$\lambda_{1,2} = \rho \pm \sqrt{\rho^2 + \sigma}. \tag{9}$$

If $\rho > 0$, $\sigma = -1$, then the VdPVP has a locally stable limit cycle. However, let $\sigma = -k \sin \omega t$, i.e., $-k \leqslant \sigma \leqslant k$, the eigenvalues of VdPVP change between positive and negative values periodically, which results in the breaking of the limit cycle and a chaos phenomenon appearing. For example, let $\rho = 0.6$, $\omega = 5.9, k = 19.5$ and initial values $(x_0, y_0) = (-8, -10)$, the VdPVP will enter the chaotic attractor after a transient period, where the chaotic attractor is shown in Figure 3.

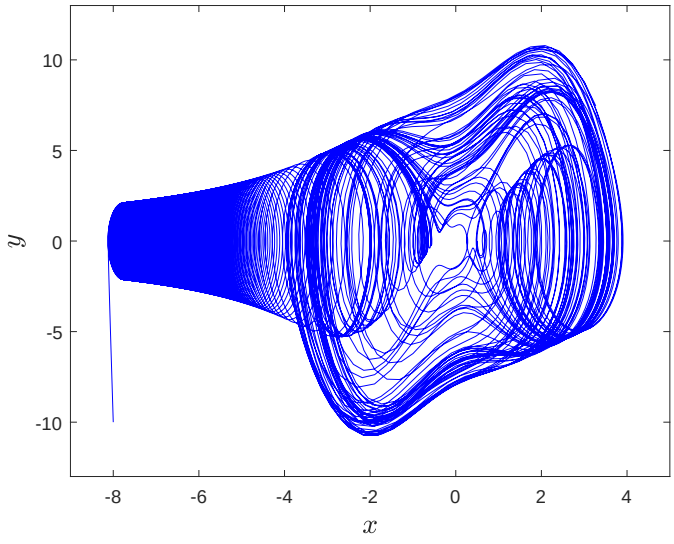


Figure 3. The attractor of dynamic system (6) with initial values $(x_0, y_0) = (-8, -10)$.

3.3. Lyapunov Exponent Analysis

A positive Lyapunov exponent is an important quantitative index for judging whether the dynamic system is chaotic or not. There are two parameters k, ω in the parameter controller $\sigma = -k \sin \omega t$; the corresponding Lyapunov exponents can be calculated for different parameter values k or ω.

Let $\rho = 0.6$, $k = 19.5$. The Lyapunov exponent spectrum of VdPVP with respect to parameter ω is shown in Figure 4; it shows that the VdPVP is chaotic in the interval $\omega \in (1, 6)$. Similarly, let $\rho = 0.6$, $\omega = 5.9$. The Lyapunov exponent spectrum of VdPVP with respect to parameter k is shown in Figure 5, and it shows that the VdPVP has a chaotic attractor in the interval $k \in (19, 25)$.

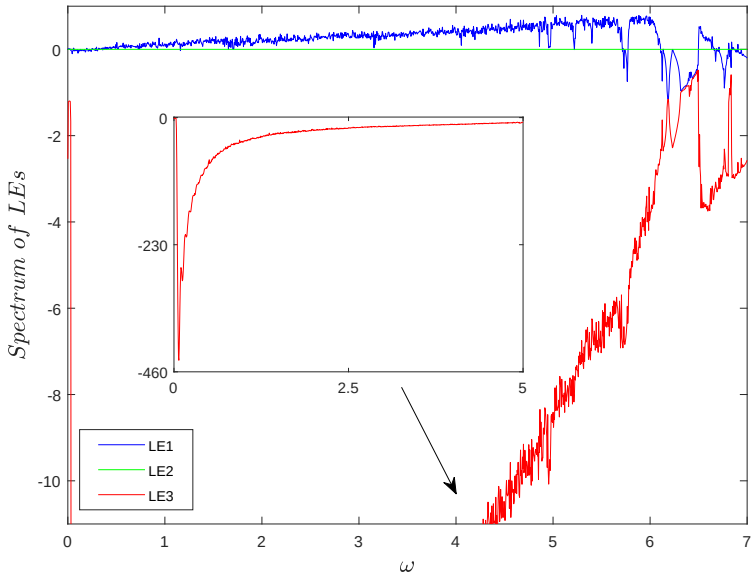


Figure 4. The Lyapunov exponent spectrum of VdPVP (Van der Pol oscillator with variable parameter) with respect to parameter ω when $\rho = 0.6, k = 19.5$. (The blue line represents the positive Lyapunov exponent, the green line represents the zero Lyapunov exponent, and the red line represents the negative Lyapunov exponent).

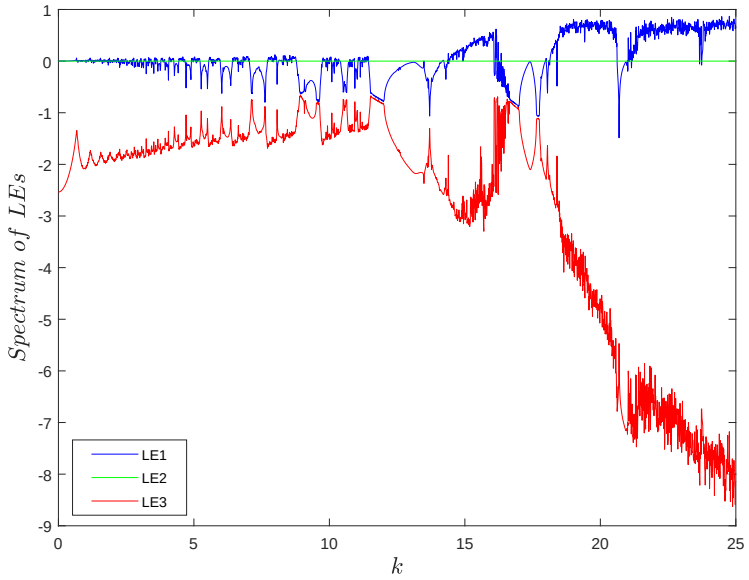


Figure 5. The Lyapunov exponent spectrum of VdPVP with respect to parameter k when $\rho = 0.6$, $\omega = 5.9$. (The blue line represents the positive Lyapunov exponent, the green line represents the zero Lyapunov exponent, and the red line represents the negative Lyapunov exponent).

3.4. Bifurcation Diagram Analysis

Chaotic systems are highly sensitive to the parameters. Different parameters lead the dynamic system to behave in different states, such as periodic motion, limit cycle and chaotic attractor.

According to the Poincare cross-section of $x = y$, and letting $\rho = 0.6, k = 19.5$, the bifurcation diagram with respect to parameter ω is shown in Figure 6. Obviously, the VdPVP has chaos when $\omega \in (1, 6)$. If one lets $\rho = 0.6$, $\omega = 5.9$, the corresponding bifurcation diagram with respect to parameter k is shown in Figure 7; the VdPVP appears to be chaotic when $k \in (19, 25)$.

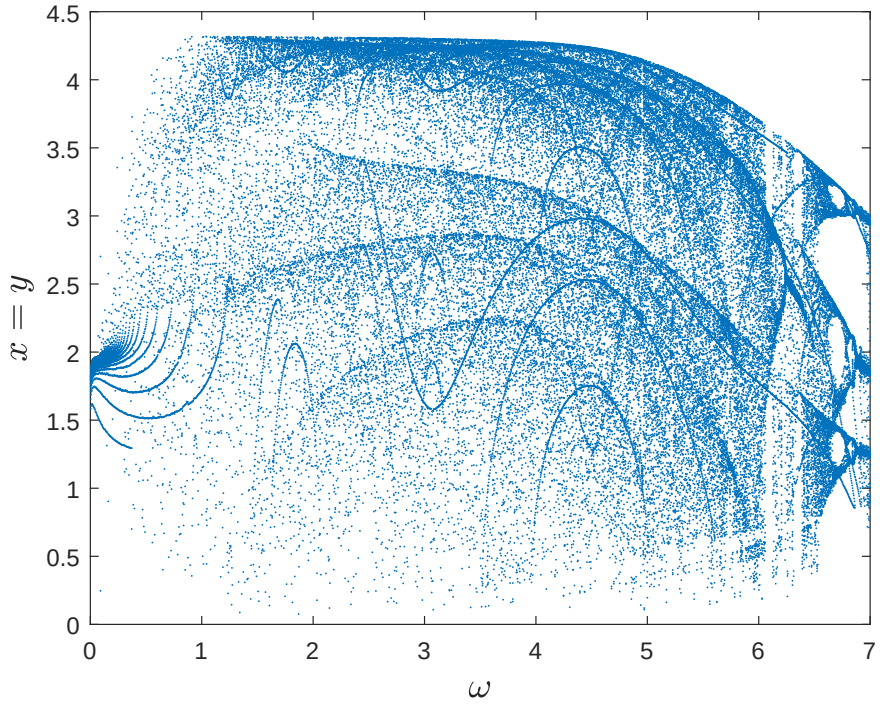


Figure 6. Bifurcation diagrams with respect to parameter ω of Poincare cross-section when $x = y$.

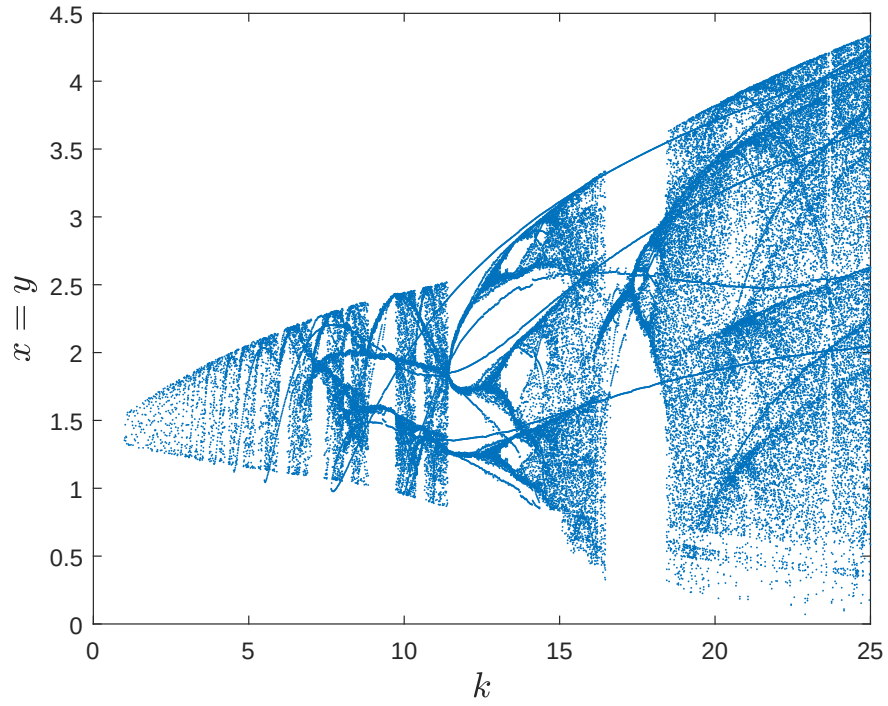


Figure 7. Bifurcation diagrams with respect to parameter k of Poincare cross-section when $x = y$.

4. Design and Application of Chaotic Encryption Algorithms

A chaotic stream cipher encryption scheme based on the VdPVP is designed. The flowchart of the encryption scheme is shown in Figure 8. The sender chooses the initial values as the keys to generate chaotic pseudo-random sequences, and completes chaos scrambling and chaos XOR encryption for the original information. The encrypted information can be transmitted to the receiver through a public channel, and the keys need to be transmitted through a secret channel for security. On the receiver side, the receiver recovers the information through the inverse operation of chaotic encryption with the correct keys.

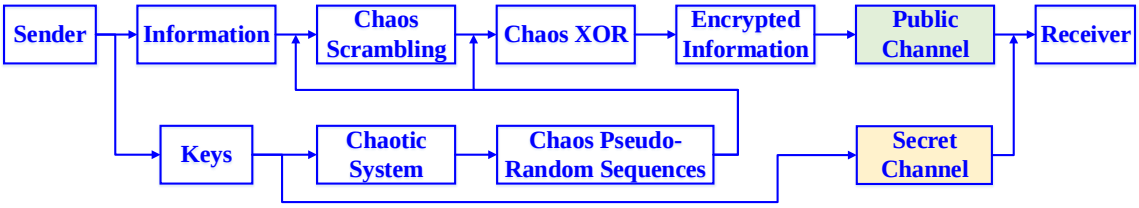


Figure 8. Design of the chaotic stream cryptographic encryption flowchart.

4.1. Algorithm Design

According to the VdPVP proposed in Section 3, a chaos-based encryption algorithm is designed, and it is divided into several steps:

Step 1 Generate pseudo-random sequences from VdPVP.

The fourth-order Runge–Kutta algorithm is employed to solve the VdPVP in Equation (6), and it is given by

$$\begin{cases} X_{m+1} = X_m + \dfrac{h}{6}\left(k_1 + 2k_2 + 2k_3 + k_4\right), \\ k_1 = f(t_m, X_m), \\ k_2 = f(t_m + \dfrac{h}{2}, X_m + \dfrac{h}{2} \cdot k_1), \\ k_3 = f(t_m + \dfrac{h}{2}, X_m + \dfrac{h}{2} \cdot k_2), \\ k_4 = f(t_m + h, X_m + \dfrac{h}{2} \cdot k_3). \end{cases} \tag{10}$$

With initial values $X_0 = (x_0, y_0)$, step h, length of time T, and the total iteration N, then one gets the chaotic sequences $X = [x, y]$ in the length of N.

Step 2 Remove the pseudo-random sequences in $[0, t_z]$ before the dynamic system enters the chaotic state, and get the pseudo-random sequences $X_{[t_z,T]}$ after t_z.

Step 3 Multiplying the pseudo-random sequence by 10^θ (θ is an integer), and obtaining the integer parts, one gets

$$S^\theta = \mathrm{Fix}\left\lfloor \left(X_{[t_z,T]} - \mathrm{Fix}\left\lfloor X_{[t_z,T]} \right\rfloor \right) \times 10^\theta \right\rfloor,$$

where Fix is an integral function.

Step 4 Model the pseudo-random sequences S^θ by 2^{32}, and convert them into binary sequences S, i.e.,

$$S = \mathrm{Dec2bin}\left(\mathrm{Mod}\left(S^\theta,\ 2^{32}\right)\right),$$

where Mod is a modulus function and Dec2bin is a decimal-to-binary function.

Step 5 Encrypt information by pseudo-random sequence S, S^θ.

In order to improve the effect of information encryption, a chaos scrambling process is added. The algorithm is given as follows:

The sequences $S^\theta = [S_1^\theta, S_2^\theta]$ are modeled by L (the length of information), and the new sequences or sequence pairs are used as new positions to exchange the positions of the original information, i.e., adjust the positions of the original information as

$$I(i) \leftrightarrow I(S_1^\theta), \text{ or } I(i) \leftrightarrow I(S_2^\theta), \text{ or } I(i,j) \leftrightarrow I(S_1^\theta, S_2^\theta),$$

where $I(0) \leftrightarrow I(\text{end})$, or $I(0,0) \leftrightarrow I(\text{end}, \text{end})$.

Step 6 Transform the information data I into binary sequences, and obtain the encrypted information E by

$$E = I \oplus S,$$

where $\oplus$ is exclusion-or (XOR) operation.

Finally, the encrypted information is transmitted to the receiver via the public channel. On the receiving side, the decryption process is the inverse operation of above encryption, and the recovered information is given by

$$I' = E \oplus S,$$

and the positions of I' is replaced by

$$I'(i) \leftrightarrow I'(S_1^\theta), \text{ or } I'(i) \leftrightarrow I'(S_2^\theta), \text{ or } I'(i,j) \leftrightarrow I'(S_1^\theta, S_2^\theta),$$

where $I'(0) \leftrightarrow I'(\text{end})$, or $I'(0,0) \leftrightarrow I'(\text{end}, \text{end})$. Then, the original information can be recovered successfully.

4.2. Simulation Experiment

The simulation experiment of the encryption algorithm based on Matlab software (R2018a, The MathWorks, Inc., Natick, Massachusetts, USA) is verified by taking the image as an example. Firstly, the color image I is converted into RGB-channel images I_R, I_G, I_B, respectively. With initial values and parameters

$$(x_0, y_0, z_0) = (0.21, 0.12, 0.31),\ \rho = 0.6,\ \omega = 5.9,\ k = 19.5,\ \theta = 12,\ T = 300,\ h = 0.001,$$

the pseudo-random sequences can be generated based on the VdPVP system, and they are used to encrypt images I_R, I_G, I_B by chaos scrambling and XOR operation. By the encryption algorithm, the experiment results of image encryption are shown in Figure 9.

(**a**) (**b**) (**c**)

Figure 9. (**a**) original image; (**b**) encrypted image after chaos scrambling; (**c**) encrypted image after chaos XOR (exclusive-or) operation.

4.3. Security Analysis

4.3.1. Key Sensitivity and Key Space

There are two kinds of keys in chaotic encryption algorithms: one is the initial values, the other is the parameters of the chaotic system. The keys sensitivity is tested by initial conditions with small errors. If we let

$$(x_0, y_0', z_0) = (0.21, 0.1200000000000001, 0.31),$$

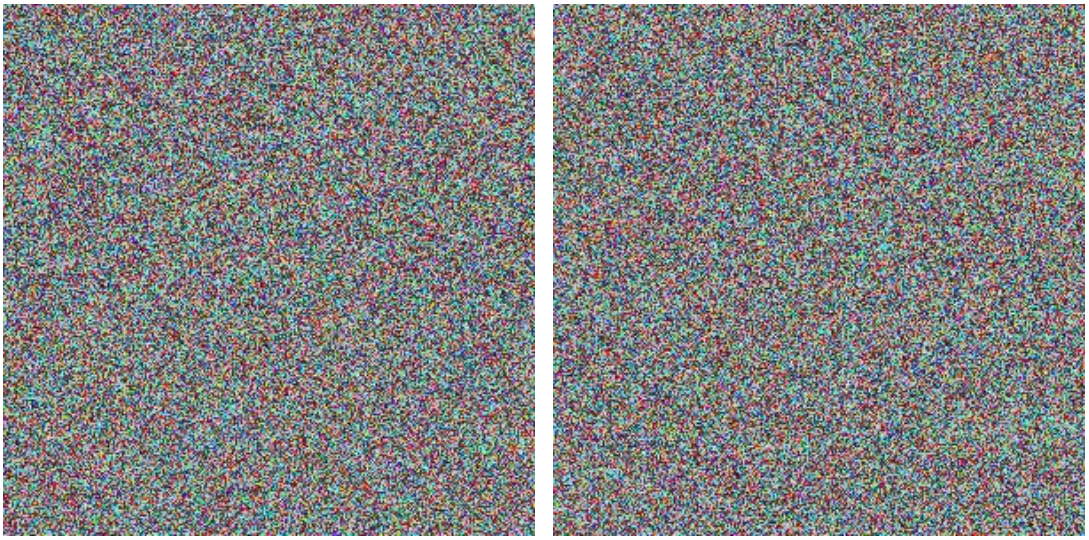
and $\rho = 0.6$, $\omega = 5.9$, $k = 19.5$, $\theta = 12$, the error of initial value y_0 is 10^{-16}; then, the decryption image is shown in Figure 10a. If we let

$$\rho' = 0.6000000000000001,\ \omega = 5.9,\ k = 19.5,\ \theta = 12,$$

and initial values $(x_0, y_0, z_0) = (0.21, 0.12, 0.31)$, the error of initial parameter ρ is 10^{-16}; then, the decryption image is shown in Figure 10b. Some initial conditions are tested and the results are given in Table 1.

Then, the key space size can be estimated from the above key sensitivity accuracy, i.e.,

$$\text{Ks} = 10^{16} \times 10^{15} \times 10^{17} \times 10^{18} \times 10^{15} \times 10^{14} = 10^{95} > 2^{315}.$$



(**a**) (**b**)

Figure 10. (**a**) recovered image with initial value y_0'; (**b**) recovered image with parameter ρ'.

Table 1. Test results of key sensitivity for the parameters and initial variables of VdPVP (Van der Pol oscillator with variable parameter).

Variable Errors	Parameter Errors	Recover Original Image
$\lvert x_0 - x_0' \rvert \geqslant 10^{-15}$	0	No
$\lvert y_0 - y_0' \rvert \geqslant 10^{-16}$	0	No
$\lvert z_0 - z_0' \rvert \geqslant 10^{-17}$	0	No
0	$\lvert \rho - \rho' \rvert \geqslant 10^{-16}$	No
0	$\lvert \omega - \omega' \rvert \geqslant 10^{-15}$	No
0	$\lvert k - k' \rvert \geqslant 10^{-14}$	No

4.3.2. Statistical Analysis

For the encrypted image, the correlation coefficient is a statistical method to analyze the effect of encryption algorithm, and it is defined by the following two formulas [20]:

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)),\ r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, x, y$ are grey-scale values of two adjacent pixels in the image.

The correlation of images can be divided into three directions: horizontal, vertical and diagonal. Five thousand pairs of points are randomly selected, and then correlation coefficients are calculated according to the formula of the correlation coefficient. The test results are shown in Table 2. The original image correlation coefficient is close to 1, but, after the position scrambling and chaotic stream cipher encryption, it is close to 0. Obviously, the correlation of image pixels becomes nearly irrelevant after chaos encryption.

Table 2. Correlation coefficient of the original image and ciphered image.

Direction	Original Image	Chaos Scrambling Image	Ciphered Image
Horizontal	0.9535	0.0105	−0.0076
Vertical	0.9754	−0.0011	0.0141
Diagonal	0.93334	0.0061	−0.0107

4.3.3. NIST Test

NIST (The National Institute of Standards and Technology) provides a necessary test for the randomness; it contains 15 major items, such as frequency, block frequency and so on. By probabilistic methods, the randomness is determined by the test p-value. If the p-value is greater than the significance level 0.01, then it indicates that the sequence is random [26–28]. For the sequences $S = \mathrm{Dec2bin}\left(\mathrm{Mod}\left(S^{\theta}, 2^{32}\right)\right)$, the test results of NIST are given in Table 3. Obviously, the p-values are greater than 0.01, so it passes all the tests of NIST.

Table 3. The results of the NIST test.

Statistical Tests	p-Value
Frequency	0.2248
Block frequency	0.0519
Cumulative sums	0.6583
Runs	0.3345
Longest run	0.3191
Rank	0.5141
FFT	0.8831
Non-overlapping template	0.4824
Overlapping template	0.8165
Universal	0.4944
Approximate entropy	0.3345
Random excursions	0.5587
Random excursions variant	0.4683
Linear complexity	0.3041
Serial	0.4950
Success	All

5. Conclusions

In this paper, a new VdPVP chaotic system is proposed through the external excitation control of the Van der Pol oscillator. The characteristics of equilibrium point, exponent spectrums and bifurcation diagrams of the dynamic system are analyzed. According to the VdPVP, an encryption algorithm of chaos scrambling and chaos XOR encryption is designed, and the feasibility and validity of the scheme are verified by simulation experiments with the image as an example. Security analyses show that the encryption algorithm has good pseudo-randomness and high key sensitivity. It will be applied to information encryption in the future.

Author Contributions: Methodology, J.H. and J.C.; software, J.H.; formal analysis, J.C.; writing—original draft preparation, J.H.; writing—review and editing, J.H. and J.C.; project administration, J.H. and J.C.

Funding: The work was supported by the National Natural Science Foundation of China (Grant No. 11847051), and the Natural Science Foundation of Fujian Province (Grant No. 2019J01742, 2019J05107).

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

Abbreviation

The following abbreviations are used in this manuscript:

VdPVP Van der Pol oscillator with variable parameter

References

1. Chen, G.; Ueta, T. Yet another chaotic attractor. *Int. J. Bifurc. Chaos* **1999**, *9*, 1465–1466. [CrossRef]
2. Felicio, C.C.; Rech, P.C. On the dynamics of five- and six-dimensional Lorenz models. *J. Phys. Commun.* **2018**, *2*, 025028. [CrossRef]
3. Sooraksa, P.; Chen, G. Chen system as a controlled weather model-physical principle, engineering design and real applications. *Int. J. Bifurc. Chaos* **2018**, *28*, 1830009-12. [CrossRef]
4. Yang, Q.; Bai, M. A new 5D hyperchaotic system based on modified generalized Lorenz system. *Nonlinear Dyn.* **2017**, *88*, 189–221. [CrossRef]
5. Cui, J.; Liang, J.; Lin, Z. Stability analysis for periodic solutions of the Van der Pol–Duffing forced oscillator. *Phys. Scr.* **2016**, *91*, 015201-7. [CrossRef]
6. Brizard, A.J.; Westland, M.C. Motion in an asymmetric double well. *Commun. Nonlinear Sci. Numer. Simul.* **2017**, *43*, 351–368. [CrossRef]
7. Ueda, Y.; Akamatsu, N. Chaotically transitional phenomena in the forced negative-resistance oscillator. *IEEE Trans. Circuits Syst.* **1981**, *28*, 217–224. [CrossRef]
8. Wiggers, V.; Rech, P.C. Multistability and organization of periodicity in a Van der Pol–Duffing oscillator. *Chaos Solitons Fractals* **2017**, *103*, 632–637. [CrossRef]
9. Roup, A.V.; Bernstein D.S. Adaptive stabilization of a class of nonlinear systems with nonparametric uncertainty. *IEEE Trans. Autom. Control* **2001**, *46*, 1821–1825. [CrossRef]
10. Chedjou, J.C.; Fotsin, H.B.; Woafo, P. Behavior of the van der pol oscillator with two external periodic forces. *Phys. Scr.* **1997**, *55*, 390–393. [CrossRef]
11. Kamdoum, T.V.; Takougang K.S.; Fautso K.G.; Bertrand F.H.; Kisito T.P. Coexistence of attractors in autonomous Van der Pol–Duffing Jerk oscillator: Analysis, chaos control and synchronisation in its fractional-order form. *Pramana* **2018**, *91*, 1–12.
12. Wiggers, V.; Rech, P.C. On symmetric and asymmetric Van der Pol–Duffing oscillators. *Eur. Phys. J. B* **2018**, *91*, 144–146. [CrossRef]
13. Kuiate, G.F.; Rajagopal, K.; Kingni, S.T.; Tamba, V.K.; Jafari, S. Autonomous Van der Pol–duffing snap oscillator: Analysis, synchronization and applications to real-time image encryption. *Int. J. Dyn. Control* **2018**, *6*, 1008–1022. [CrossRef]
14. Makouo, L.; Woafo, P. Experimental observation of bursting patterns in van der pol oscillators. *Chaos Solitons Fractals* **2017**, *94*, 95–101. [CrossRef]

15. Chen, G.; Lai, D. Anticontrol of chaos via feedback. *Proc. IEEE Conf. Decis. Control* **1998**, *1*, 367–372. [CrossRef]
16. Hu, G.; Xiao, D.; Zhang, Y.; Xiang T. An efficient chaotic image cipher with dynamic lookup table driven bit-level permutation strategy. *Nonlinear Dyn.* **2017**, *87*, 1359–1375. [CrossRef]
17. Hamdi, B.; Hassene, S. Innovative image encryption scheme based on a new rapid hyperchaotic system and random iterative permutation. *Multimed. Tools Appl.* **2018**, *77*, 30841–30863.
18. Wang, X.; Wang, Y.; Wang S.; Zhang Y.; Wu X. A novel pseudo-random coupled LP spatiotemporal chaos and its application in image encryption. *Chin. Phys. B* **2018**, *27*, 423–433. [CrossRef]
19. Rehman, A.; Liao, X. A novel robust dual diffusion/confusion encryption technique for color image based on Chaos, DNA and SHA-2. *Multimed. Tools Appl.* **2019**, *78*, 2105–2133. [CrossRef]
20. Chen, G.; Mao, Y.; Chui C.K. A symmetric image encryption scheme nased on 3D chaotic cat maps. *Chaos Solitons Fractals* **2004**, *21*, 749–761. [CrossRef]
21. Zhu, Z.; Zhang, W.; Wong, K.W.; Yu, H. A chaos-based symmetric image encryption scheme using a nit-level permutation. *Inf. Sci.* **2011**, *181*, 1171–1186. [CrossRef]
22. Lin, Z.; Yu, S.; Lu, J.; Cai, S.; Chen, G. Design and ARM-embedded implementation of a chaotic map-based real-time secure video communication system. *IEEE Trans. Circuits Syst. Video Technol.* **2015**, *25*, 1203–1216.
23. Alvarez, G.; Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos* **2016**, *16*, 2129–2153. [CrossRef]
24. Li, C.; Lin, D.; Lü, J. Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. *IEEE Multimed.* **2016**, *24*, 64–71. [CrossRef]
25. Özkaynak F. Brief review on application of nonlinear dynamics in image encryption. *Nonlinear Dyn.* **2018**, *92*, 305–313. [CrossRef]
26. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E.; Leigh, S.; Levenson, M.; Vangel, M.; Banks, D.; Heckert, A.; et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Special Publication 800–22 Revision 1, National Institute of Standards and Technology. 2008. Available online: http://csrc.nist.gov/publications/PubsSPs.html (accessed on 1 May 2019)
27. Murillo-Escobar, M.A.; Cruz-Hernández, C.; Cardoza-Avendaño, L.; Méndez-Ramírez, R. A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. *Nonlinear Dyn.* **2017**, *87*, 407–425. [CrossRef]
28. He, J.; Yu, S.; Cai, J. Topological horseshoe analysis for a three-dimensional anti-control system and its application. *Optik* **2016**, *127*, 9444–9456. [CrossRef]