

DOI: 10.7652/xjtuxb201706006

用于保密通信的高安全性混沌振荡器

李石磊, 刘崇新, 胡晓宇, 倪骏康
(西安交通大学电气工程学院, 710049, 西安)

摘要: 针对混沌保密通信中传统振荡器因其混沌映射容易被预测而导致通信安全性降低的问题,提出了一种由单一电压输入控制的四维混沌振荡器。该混沌振荡器由一个直流电压进行控制,通过调节该控制电压,可使振荡器处于周期、倍周期、混沌甚至是超混沌运动状态。由于该振荡器混沌状态下的吸引子是隐藏吸引子,其位置不能通过在线平衡点邻域内选任意初值的方法来确定,从而加强了该混沌振荡器动力学行为的不可预测性,提高了保密通信的安全性。硬件实验结果表明,当控制电压在区间 $[2.80, 3.40]$ V上取值时,该振荡器对外界干扰最为敏感,其混沌运动的不可测性最高,从而使混沌保密通信的安全性达到最佳。

关键词: 保密通信;混沌振荡器;线平衡点

中图分类号: TM132 **文献标志码:** A **文章编号:** 0253-987X(2017)06-0035-06

A Chaotic Oscillator with High Security for Secret Communication

LI Shilei, LIU Chongxin, HU Xiaoyu, NI Junkang
(School of Electrical Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: A 4D chaotic oscillator controlled by a single voltage input is proposed to solve the problem that the security in chaotic secret communication is reduced because the chaotic mappings of traditional chaotic oscillators are easy to predict. The chaotic oscillator is controlled by a DC voltage and it can be kept in motion state of period, period-doubling, chaos or even hyper-chaos through regulating the control voltage. Because the oscillator's attractors are hidden attractors in chaotic state and the locations of these attractors cannot be calculated through choosing points in the neighborhood of line equilibrium, the unpredictability of these chaotic oscillator's dynamic behaviors and the security of secret communication are improved. Hardware experiment shows that when the voltage is controlled within the interval of $[2.80, 3.40]$ V, the chaotic oscillator is the most sensitive to external disturbance, the unpredictability of its chaotic motion is the highest, and the security of chaotic secret communication achieves the best.

Keywords: secret communication; chaotic oscillator; line equilibrium

由于混沌信号具有随机、对初始条件敏感、连续宽频带和似噪声等特点,使得混沌信号很难被破译,所以特别适用于保密通信等领域。然而,随着预测学等相关技术的发展,一些混沌映射能够通过相空

间重构的方法进行精确预测^[1-3],同时,考虑到混沌系统的易实现性,如何得到不易预测且易实现的混沌振荡器就成为了混沌技术应用于保密通信领域的一个重点。

收稿日期: 2016-10-12。 作者简介: 李石磊(1991—),男,硕士生;刘崇新(通信作者),男,教授,博士生导师。 基金项目: 国家自然科学基金资助项目(51177117)。

网络出版时间: 2017-03-13

网络出版地址: <http://www.cnki.net/kcms/detail/61.1069.T.20170313.2130.010.html>

近年来,国内学者对混沌振荡器在理论上进行了很多相关研究^[4-7],文献[4]通过在三阶 Colpitts 混沌振荡器的电感两端并联电容的方式构造了一种新的四阶 Colpitts 混沌振荡器;文献[5]基于文氏桥混沌电路,用第二代电流传输器 CCII(Current Conveyor II)电路替换运放,通过 NMOS 管将 2 个正弦振荡电路耦合实现了电流模式的混沌振荡器;文献[6]采用文氏桥振荡电路和磁通控制的分段线性忆阻器,设计了一种由单一电压输入控制的混沌振荡器;文献[7]在文氏桥混沌电路中引入了广义忆阻器和 LC 吸收网络,提出了一种忆阻文氏桥混沌振荡器并进行了实验验证。

以上对混沌振荡器的研究多围绕文氏桥振荡电路和忆阻器展开,因基于文氏桥振荡电路的混沌系统阶数较低,且实际中忆阻器的真正物理实现尚不多见,故以上文献中的混沌振荡器若用于混沌保密通信,无论是在安全性还是在易实现性上都会存在一定的问题。

考虑到不易预测性和易实现性,本文提出了一种新的由单一电压输入控制的混沌振荡器,以期混沌保密通信的实现提供一种可供参考的混沌振荡器。该混沌振荡器对应的混沌系统含有一条线平衡点,因为不能通过在该平衡点邻域内选任意初值的方法来确定相应吸引子的位置^[8],所以系统中的吸引子也被称为隐藏吸引子,这样在一定程度上就增加了该混沌振荡器动力学行为的复杂性和不易预测性;同时,因该混沌振荡器是在 Liu 混沌系统^[9-10]的基础上改变得来的,仅有 1 个控制电压输入,硬件上容易实现。

1 系统动力学特性分析及数值仿真

1.1 系统平衡点的计算及稳定性分析

混沌振荡器是一种混沌信号发生装置,本文提出的自激混沌振荡器具有 4 路输出,是在 1 个三维连续自治混沌系统的基础上得到的,系统方程如下

$$\left. \begin{aligned} \dot{x} &= 0.1(y-x) + 2y^2 \\ \dot{y} &= 2.5y - 2xz + w \\ \dot{z} &= 0.5xy - 5z + u \\ \dot{w} &= -0.25y \end{aligned} \right\} \quad (1)$$

式中: x 、 y 、 z 和 w 分别表示混沌振荡器中 4 路输出端的电压; u 表示外部施加的控制电压。

该四维系统在相空间中体积 V 的散度为

$$\operatorname{div} V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{w}}{\partial w} = -2.6 \quad (2)$$

由式(2)可得,体积 V 的散度小于 0,证明该系统在时间趋于无穷时是个耗散系统,同时会呈现相应的动力学特性。

令方程(1)的右侧为 0,得到系统的平衡点方程如下

$$\left. \begin{aligned} 0.1(y-x) + 2y^2 &= 0 \\ 2.5y - 2xz + w &= 0 \\ 0.5xy - 5z + u &= 0 \\ -0.25y &= 0 \end{aligned} \right\} \quad (3)$$

根据控制电压 u 的不同取值,方程(3)的解有以下 2 种情况。

(1)控制电压 $u=0$,方程(1)平衡点的解为原点,即

$$x=0; y=0; z=0; w=0 \quad (4)$$

(2)控制电压 $u \neq 0$,方程(1)平衡点的解为 1 个平衡点集

$$E = \{(x, y, z, w) | x=y=w=0, z=c_0\} \quad (5)$$

式中: $c_0=0.2u$, c_0 为不确定常数,对应着 z 轴,这个平衡点集合 E 也被称为线平衡点。

系统方程式(1)在第 1 种情况时的雅克比矩阵 J_1 为

$$J_1 = \begin{bmatrix} -0.1 & 0.1 & 0 & 0 \\ 0 & 2.5 & 0 & 1 \\ 0 & 0 & -5 & 0 \\ 0 & -0.25 & 0 & 0 \end{bmatrix} \quad (6)$$

矩阵 J_1 的特征多项式为

$$\det(\lambda I - J_1) =$$

$$(\lambda+5)(\lambda+0.1)(\lambda^2-2.5\lambda+0.25)=0 \quad (7)$$

式中: I 表示 4 阶单位阵; λ 表示特征值。

求解式(7)得

$$\lambda_1 = -5; \lambda_2 = -0.1; \lambda_3 \approx 2.4; \lambda_4 \approx 0.1 \quad (8)$$

因以上 4 个特征值中存在 2 个正值,所以该平衡点 $\{x=y=z=w=0\}$ 是不稳定的平衡点。

在第 2 种情况下的雅克比矩阵 J_2 为

$$J_2 = \begin{bmatrix} -0.1 & 0.1 & 0 & 0 \\ -0.4u & 2.5 & 0 & 1 \\ 0 & 0 & -5 & 0 \\ 0 & -0.25 & 0 & 0 \end{bmatrix} \quad (9)$$

矩阵 J_2 的特征多项式为

$$\det(\lambda I - J_2) =$$

$$(\lambda+5)(\lambda^3-2.4\lambda^2+0.04u\lambda+0.025)=0 \quad (10)$$

由式(10)可得 $\lambda_1 = -5$,其余特征根可由下式求得

$$\lambda^3 - 2.4\lambda^2 + 0.04u\lambda + 0.025 = 0 \quad (11)$$

式(11)是一个标准的一元三次方程,根据盛金公式法,其总判别阈值为

$$\Delta = 0.000\ 768u^3 - 0.027\ 648u^2 + 0.129\ 6u - 4.096\ 575 \quad (12)$$

令 $\Delta=0$, 解得 $u_1 \approx 35.48$ 和一对共轭复根 $u_2 \approx 0.26 + 12.26i$ 和 $u_3 = 0.26 - 12.26i$, 由于盛金公式只适用各项系数为实数且3次项系数不为0的情况, 因此下文仅对 u 在实数域内的情况进行分析。

经计算, 在 $u < 35.48$ 时, Δ 恒小于0, 根据盛金公式, 此时式(11)应有3个实根, 计算结果证明该实根中始终存在1个正值, 说明当 $u < 35.48$ 且 $u \neq 0$ 时式(1)系统的线平衡点都是不稳定的; 在 $u > 35.48$ 时, 根据盛金公式, 此时式(11)应有1个实根和1对共轭虚根, 计算结果证明共轭虚根的实部无限趋近1.2, 说明 $u > 35.48$ 时式(1)系统的平衡点同样是不稳定的。

最后考虑 $\Delta=0$ 的情况, 据上文的计算结果可知 $\Delta=0$ 在实数域内的解为 $u \approx 35.48$, 代入式(11)得 $\lambda_2 = -0.017\ 1$, $\lambda_3 = 1.214\ 9$, $\lambda_4 = 1.202\ 2$, 因为存在正特征值, 所以 $u=35.48$ 时系统的平衡点也是不稳定的。综合上文 $\Delta > 0$ 和 $\Delta < 0$ 时的特征值结果, 可知当控制电压 u 取任意实数值(不含0)时系统的无数个平衡点都是不稳定的。

1.2 控制电压对系统的影响

首先考虑控制电压值 $u=0$ 时的情况, 此时系统方程(1)只有1个不稳定的平衡点(0,0,0,0), 在仿真时间区间取[0, 1 000]s时系统的4个李雅普诺夫指数(从系统方程式(1)计算)分别为 $\lambda_1 = -0.100\ 000$, $\lambda_2 = 2.395\ 687$, $\lambda_3 = 2.392\ 410$, $\lambda_4 = 2.394\ 830$, 据此可判断此时系统的运动从整体上来讲处于一种发散的不稳定状态; 当控制电压取非0值时, 系统会有在一条直线上的无数个平衡点, 且平衡点集 $E = \{(x, y, z, w) | x=y=w=0, z=0.2u\}$ 中的无数个平衡点都是不稳定的。现控制电压 u 的区间取(0, 5]V, 仿真步长取0.01 V, 仿真时间区间分别取[0, 1 000]和[0, 2 000] s, 系统随控制电压变化的李雅普诺夫指数谱和分岔图分别如图1和图2所示。

图1中4条曲线分别表示系统4路输出电压 x 、 y 、 z 和 w 随控制电压变化的李雅普诺夫指数曲线 λ_x 、 λ_y 、 λ_z 、 λ_w 。由图1可以明显观察到, 该系统有3条李雅普诺夫指数曲线 λ_y 、 λ_z 和 λ_w 基本上是重合在一起的。由仿真结果可知, 输出电压 λ_y 和 λ_w 两条李雅普诺夫指数曲线的相似度相对更高。这种多

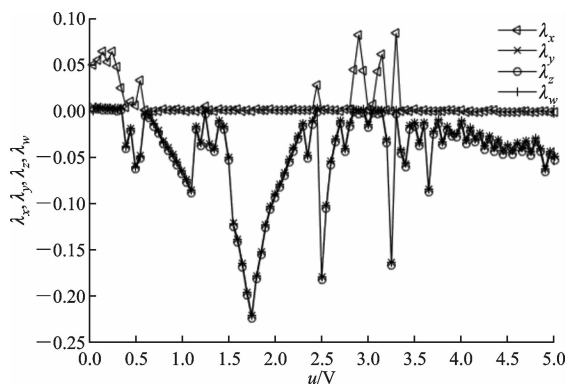


图1 系统随控制电压变化的李雅普诺夫指数谱

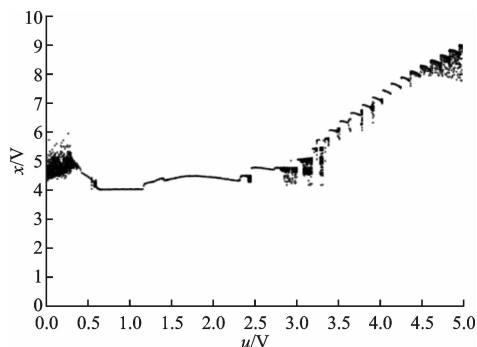


图2 输出电压 x 随控制电压变化的分岔图

路输出电压变量的李雅普诺夫指数曲线具有较高相似度的现象说明了该系统在 y 、 z 和 w 方向运动的收敛或发散程度比较接近。此外, 在图1中可观察到该系统的运动状态主要由输出电压 x 的李雅普诺夫指数决定, 因为其他3路输出电压的李雅普诺夫指数几乎在整个控制电压区间(0, 5] V上都小于0。

图2是当控制电压 u 在区间(0, 5] V变化时输出电压 x 的分岔图, 从整体上来看, 系统在大部分区间上处于周期或倍周期运动状态, 在少部分区间上处于混沌或超混沌运动状态, 这与图1中李雅普诺夫指数谱的结果对应性很强。利用 Matlab 中的 Data Cursor 工具可对图1和图2中数据点的横纵坐标进行测量, 主要测量的是不同控制电压下的李雅普诺夫指数和系统处于不同运动状态时, 对应的控制电压区间: ①在控制电压区间(0, 0.4) V, 系统处于混沌或超混沌运动状态, 且图2中在该电压区间的后半部有明显的混沌运动向周期运动过渡的现象; ②在控制电压区间[0.4, 2.8] V, 系统主要处于周期或倍周期运动状态, 只有在其中的3个小区间上处于混沌或超混沌运动状态, 经过相图等具体验证, 这3个小区间分别是 $u = 0.554$ V 附近的小区间、

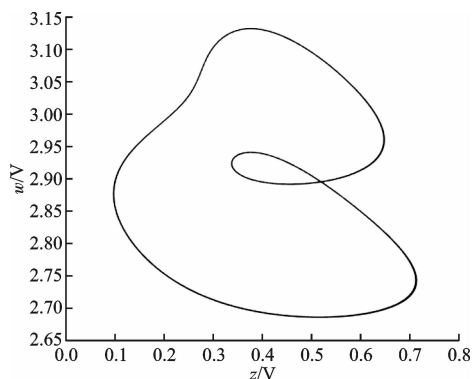
$[0.58, 0.65]$ V 和 $[2.41, 2.45]$ V; ③在控制电压区间 $(2.80, 3.40)$ V, 系统主要处于混沌运动状态, 其中存在个别小区间和点使系统处于周期或倍周期运动状态, 比如在区间 $[3.25, 3.27]$ V, 系统会处于周期运动状态, 在区间 $[3.19, 3.22]$ V 和 $[3.34, 3.36]$ V, 系统会处于倍周期运动状态; ④在控制电压区间 $[3.40, 4.02]$ V, 系统主要处于周期运动状态, 在该区间上输出电压变量 x 分岔图的主要特征是存在多个由周期向倍周期甚至混沌运动过渡的分岔现象, 经过相图等具体验证, 每次这种分岔后都出现了倍周期或者混沌运动, 如在区间 $[3.48, 3.50]$ V 和 $[3.62, 3.64]$ V, 系统中都出现了倍周期运动, 在控制电压 $u=3.77$ V 附近系统中出现了混沌运动; ⑤在区间 $(4.02, 5.00]$ V, 系统主要做周期运动, 但在控制电压区间 $(4.35, 5.00]$ V, 系统在做周期运动的同时, 也存在一些明显的混沌运动特征, 表现在分岔图中就是该控制电压区间上表征系统运动状态的部分点会杂乱无章地分布, 这些点说明了系统存在一定的局部振荡发散运动, 这种现象在输出电压的时域图中可得到准确验证, 后面的实验相图也验证了这一点。

现选取典型控制电压 $u=2.00, 3.10, 3.50, 4.50$ V, 仿真时间区间取 $[0, 2\ 000]$ s, 步长取 0.1 s 时分别绘制系统的二维相图如图 3、图 4 所示, 这里要注意的是以上相图在绘制时去掉了前 $5\ 000$ 个点。

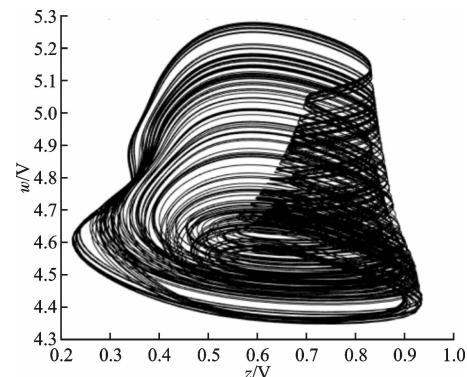
图 3 分别是控制电压 $u=2.00, 3.10, 3.50$ V 时系统在 $z-w$ 平面内的相轨迹。其中图 3a 中的相轨迹是一条闭合曲线, 与图 1 中控制电压 $u=2.00$ V 时系统最大李雅普诺夫指数近似为 0 和图 2 中分岔图上的点集中分布区段相互验证, 可证明在控制电压 $u=2.00$ V 时系统处于周期运动状态。此外, 据图 3c 可观察到该系统在 $z-w$ 平面内的相轨迹是缠绕在一起的 2 条闭合曲线, 与控制电压 $u=3.50$ V 时图 1 中系统最大李雅普诺夫指数近似为 0 和图 2 中的叉型分岔现象相互验证, 可证明控制电压 $u=3.50$ V 时系统处于倍周期运动状态。

图 3b 是控制电压 $u=3.10$ V 时系统的部分相图, 可观察到系统在 $z-w$ 平面内的相轨迹具有明显的混沌运动的特征, 即相轨迹是在一定区域内随机分离、永不重复的轨线; 与控制电压 $u=3.10$ V 时图 1 中系统的最大李雅普诺夫指数大于 0 和图 2 中分岔图是杂乱无章的点相互验证, 证明控制电压 $u=3.10$ V 时系统处于混沌运动状态。

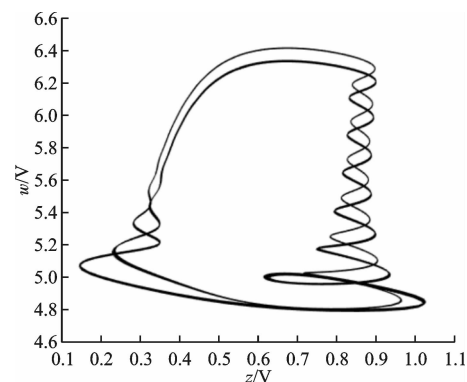
此外, 如前文所述, 在控制电压区间 $[4.35,$



(a) $u=2.00$ V



(b) $u=3.10$ V



(c) $u=3.50$ V

图 3 3 种控制电压下系统在 $z-w$ 平面内的相轨迹

$5.00]$ V, 由图 2 中的分岔图所反映出来的一个现象是系统在整体做周期运动的同时局部会呈现一部分混沌运动的特征。比如控制电压 $u=4.50$ V 时, 系统在 $z-w$ 平面上的相轨迹如图 4 所示。由图 4 可观察到, 该相轨迹是一条闭合曲线, 且仿真时间取 $1\ 000$ s 时系统的最大李氏指数 $\lambda_1 = -0.000\ 033$, 近似为 0, 结合相图可判断系统此时处于周期运动状态。仔细观察图 4a 中相图可发现, 该相轨迹不同位置的宽度明显不同, 相轨迹下半部宽度比上半部大一些; 图 4b 是控制电压 $u=4.50$ V 时系统输出电压 z 时域图的局部放大图, 由图可知, 系统在整体

做周期运动的同时,在 z 方向上存在局部振荡发散的非周期运动,故而会造成不同位置的相轨迹宽度有一定的差别。

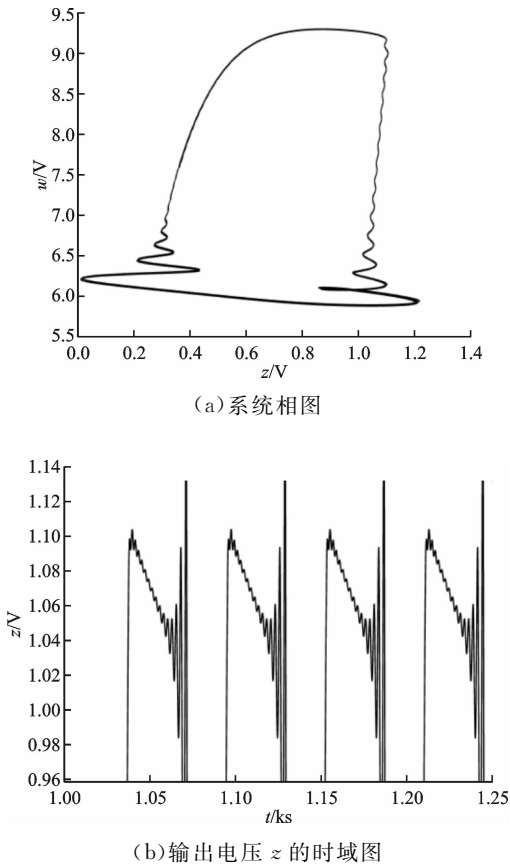


图 4 $u=4.50\text{ V}$ 时系统的相图和时域图

2 振荡器的电路实验

根据系统方程式(1)对振荡器进行电路设计,然后进行物理实验,对上文中振荡器在典型控制电压下的运动状态进行验证,得到相应的实验相图如图 5 所示。

图 5 中的 4 个相图分别是在相应控制电压附近对图 3 和图 4a 中 4 个二维相图的实验验证,依次将实验得到的二维相图与相应的仿真相图比较,可发现各实验相图在横纵坐标幅值上都存在一定的失真;此外,控制电压 $u=2.05\text{ V}$ 时的实验相轨迹在形状上发生了较大的失真。相图失真的可能原因如下:①虽然实验中实际电路是在 PCB 板上实现的,但使用的电阻都是阻值误差为 5% 的普通色环电阻,而混沌电路对初值和微小变化都很敏感;②实验中使用的模拟乘法器是 AD633,器件总误差标称为满量程的 2%,该误差因素也可能会对根轨迹的准确度产生一定的影响;③实验过程中可能存在的其

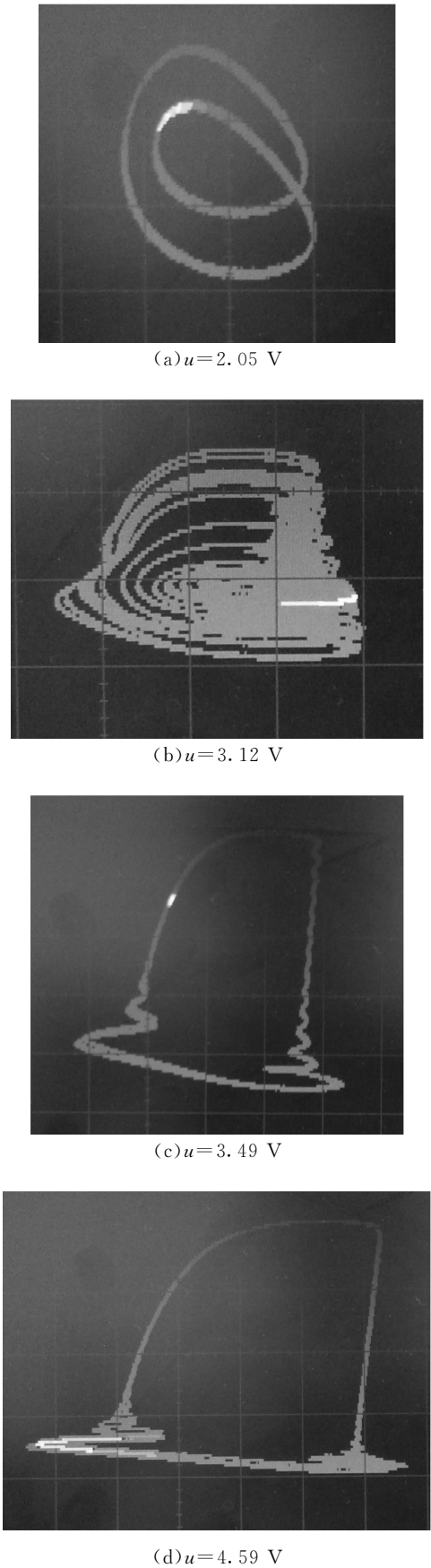


图 5 控制电压取不同值时系统在 $z-w$ 平面内的实验相图

他一些干扰等非理想因素,所以实验相轨迹在幅值或形状上出现了一定的失真。虽然各实验相图存在一定的失真,但仍较为准确地验证了相应控制电压下系统的运动状态。比如当控制电压 $u = 3.12 \text{ V}$ 时实验相轨迹是相平面内随机分离、永不重复的轨线,这个结果验证了上文同一控制电压下系统相图的正确性,证明了该控制电压下本文系统应处于混沌运动状态。此外,图 5d 中相轨迹不同位置的宽度明显存在差异,可从一定程度上验证上文相应电压下系统在做周期运动时局部存在振荡发散非周期运动的特点。

实验过程中发现,当控制电压在 $[2.80, 3.40] \text{ V}$ 区间取值时,本文所提混沌振荡器的动力学行为对外界干扰最为敏感,可进一步增加混沌动力学行为的复杂度和不可测性,从而可使混沌保密通信的安全性达到最佳。

3 结 论

本文提出了一种新的由单一电压输入控制的混沌振荡器,该振荡器是在 Liu 混沌系统的基础上修改得来的,继承了原系统的对称性和耗散性。本文所提的四维混沌振荡器比较显著的特点是只有一个控制电压输入,控制电压取 0 时系统只有一个不稳定的平衡点;控制电压取非 0 值时系统会有一条不稳定的线平衡点,从而导致系统隐藏吸引子的位置不能够通过相应的计算方法进行确定,大大提高了该混沌振荡器用于保密通信的不可预测性和安全性。根据该振荡器数学模型设计进行的硬件实验结果表明,当控制电压在 $[2.80, 3.40] \text{ V}$ 区间取值时,该振荡器对外界干扰最为敏感,其混沌动力学行为的不可测性最强,从而可使保密通信的安全度达到最佳。

参考文献:

- [1] 张家树,肖先赐. 混沌时间序列的 Volterra 自适应预测 [J]. 物理学报, 2000, 49(3): 403-408.
ZHANG Jiashu, XIAO Xianci. The Volterra adaptive prediction of chaotic time series [J]. Acta Physica Sinica, 2000, 49(3): 403-408.
- [2] ZHANG Jiashu, XIAO Xianci. Fast evolving multi-

layer perceptions for noisy chaotic time series modeling and predictions [J]. Chinese Physics, 2000, 9(9): 408-413.

- [3] ZHANG Jiashu, XIAO Xianci. Prediction of chaotic time series by using adaptive higher-order nonlinear Fourier infrared filter [J]. Physics, 2000, 49(7): 1221-1227.
- [4] 禹思敏. 四阶 Colpitts 混沌振荡器 [J]. 物理学报, 2008, 57(6): 3374-3379.
YU Simin. Fourth-order Colpitts chaotic oscillator [J]. Acta Physica Sinica, 2008, 57(6): 3374-3379.
- [5] 郭燕,贾华宇. 基于 CCII 的集成混沌振荡器设计 [J]. 电子器件, 2015, 38(5): 1064-1069.
GUO Yan, JIA Huayu. Design of integrated chaotic oscillator based on CCII [J]. Chinese Journal of Electron Devices, 2015, 38(5): 1064-1069.
- [6] 李志军,曾以成. 基于文氏振荡器的忆阻混沌电路 [J]. 电子与信息学报, 2014, 36(1): 88-93.
LI Zhijun, ZENG Yicheng. A memristor chaotic circuit based on Wien-bridge oscillator [J]. Journal of Electronics & Information Technology, 2014, 36(1): 88-93.
- [7] 俞清,包伯成,胡丰伟,等. 基于一阶广义忆阻器的文氏桥混沌振荡器研究 [J]. 物理学报, 2014, 63(24): 240505.
YU Qing, BAO Bocheng, HU Fengwei, et al. Wien-bridge chaotic oscillator based on first-order generalized memristor [J]. Acta Physica Sinica, 2014, 63(24): 240505.
- [8] JAFARIA S, SPOTTB J C. Simple chaotic flows with a line equilibrium [J]. Chaos, Solitons & Fractals, 2013, 57(4): 79-84.
- [9] 王发强,刘崇新. Liu 混沌系统的混沌分析及电路实验的研究 [J]. 物理学报, 2006, 55(10): 5061-5069.
WANG Faqiang, LIU Chongxin. Liu chaotic system's chaotic analysis and research of circuit experiment [J]. Acta Physica Sinica, 2006, 55(10): 5061-5069.
- [10] 刘凌,苏燕辰,刘崇新. 一个新混沌系统及其电路仿真实验 [J]. 物理学报, 2006, 55(8): 3933-3937.
LIU Ling, SU Yanchen, LIU Chongxin. A new chaotic system and its circuit emulation [J]. Acta Physica Sinica, 2006, 55(8): 3933-3937.

(编辑 刘杨)