基于无退化混沌系统的序列密码研究

赵 亮[1] 赵 耿[1,2] 马英杰[2]
[1](西安电子科技大学 陕西 西安 710000)
[2](北京电子科技学院 北京 100070)

摘 要 针对连续时间混沌系统的退化问题,提出一种基于矩阵特征值配置的方法来构造具有多个正Lyapunov指数的连续时间混沌系统。提出一种基于特征值定义的特征值配置方法,通过设计一个线性反馈控制器,可以配置任何系统为以稳定焦点为原点的渐近稳定线性系统;通过设计一个非线性反馈控制器来配置多个正Lyapunov 指数。相比于现有算法,对于任意受控系统,该方法都能系统地配置该受控系统的 Lyapunov 指数,使之成为无退化混沌系统。将该方法得到的无退化混沌系统转换为二进制序列,对得到的混沌序列进行分析后证明该序列具有良好的加密特性。

关键词 无退化混沌系统 反馈控制 Lyapunov 指数 序列密码

中图分类号 TP309.7 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2022.03.048

STREAM CIPHER ALGORITHM BASED ON NON-DEGENERATE CHAOTIC SYSTEM

Zhao Liang[1] Zhao Geng[1,2] Ma Yingjie[2]
[1](*Xidian University*, *Xi'an 710000*, *Shaanxi*, *China*)
[2](*Beijing Electronic Science & Technology Institute*, *Beijing 100070*, *China*)

Abstract Aiming at the degradation problem of continuous-time chaotic systems, this paper proposes a method based on matrix eigenvalue configuration to construct a continuous time chaotic system with multiple positive Lyapunov exponents. A method for configuring feature values by definition of eigenvalues was proposed. By designing a linear feedback controller, any system could be configured as an asymptotically stable linear system with a stable focus as its origin. Then the positive Lyapunov exponent was configured by designing a nonlinear feedback controller. Compared with the existing algorithms, for any controlled system, this method can systematically configure the Lyapunov exponents of the controlled system to make it a non-degenerate chaotic system. The non-degenerate chaotic system obtained by this method is transformed into binary sequence, and the analysis of the obtained chaotic sequence proves that the sequence has good encryption characteristics.

Keywords Non-degenerate chaotic system Feedback controller Lyapunov exponent Stream cipher algorithm

0 引 言

自 1963 年 Lorenz 发现第一个混沌系统以来,混沌已经被许多研究者广泛研究。随着研究的深入,人们逐渐认识到混沌运动的重要性。人们还发现混沌有许多实际应用,如安全通信、化学反应、神经网络和经济学。当混沌是有害的时,人们需要混沌控制来抑制甚至消除混沌;相应地,当需要混沌时,需要混沌反控制来增强混沌,使系统完全混沌。

在混沌系统的众多特征中,正 Lyapunov 指数的个数和系统全局有界是两个应用广泛的混沌判据,Lyapunov指数是不定维空间中相邻运动轨道平均指数发散强度的一种数值特征,具有多个正 Lyapunov 指数和唯一正 Lyapunov 指数的混沌吸引子相比,超混沌吸引子同时向两个或多个方向扩展[1-3]。对于一个离散

收稿日期:2019-12-23。国家自然科学基金项目(61772047)。**赵亮**,硕士生,主研领域:混沌密码学。**赵耿**,教授。**马英杰**,副教授。

的混沌系统,当这个系统的正 Lyapunov 指数的个数等于系统维数,并且系统全局有界时,可以称其为无退化混沌系统。但在连续混沌系统中,需要同时配置正、负和零的 Lyapunov 指数,所以要保证其 Lyapunov 指数中有一个为零,一个为负,其余全部为正,并且系统全局有界,这样就可以称其为无退化混沌系统。无退化混沌系统的各方面特性远优于存在退化的混沌系统,这也是众多学者研究无退化混沌系统的原因。

混沌系统的退化可能直接影响混沌加密系统的安全性[4]。目前,解决这一问题的方法有多种,对于连续时间混沌系统,主要包括状态反馈控制方法[5-6]、试错法[7]、弱耦合技术[8-9]和参数扰动[10]。虽然已经提出了一些相关的方法来解决一些连续时间混沌系统的产生问题,但大多数方法仍然遵循传统的试错法。该方法很难设计出高维混沌系统,也不能从理论上真正解决这一具有挑战性的研究课题。

文献[11]提出了一种配置多个正 Lyapunov 指数的方法,其通过给定受控系统的基础上加入控制器,改变该受控系统的雅可比矩阵,该方法实现的目标就是使受控系统的正 Lyapunov 指数的个数达到最大,得到无退化的混沌系统。文献[12]提出了一种对受控系统加入控制器得到高维无退化混沌系统的方法,该方法给定一个矩阵,通过对其相似变换得到想要的受控系统。由于受控系统是所给出的指定系统,对于每个维度,受控系统是同一个系统,即对于任给一个受控系统,该方法将不能适用。本文提出了一种新的 Lyapunov指数配置方法,对于全局有界系统,根据 Shilnikov 定理,配置零和负 Lyapunov 指数很容易[13-17],当系统的特征值具有 $r(r\leqslant 2)$ 个正实部时,系统将能够产生 r 个正 Lyapunov 指数[14-17]。对于任意的受控系统,通过引入两个控制器,改变受控系统雅可比矩阵,配置系统矩阵的特征值与相对应的特征向量来配置正 Lyapunov 指数的个数,使系统的正 Lyapunov 指数个数达到最大,从而达到系统无退化的目的。因为本文方法对于任意受控系统都能适用,故相比文献[11-12]方法通用性更强。

1　系统的超混沌系统配置方法

对于如下一个 n 维的连续时间线性系统:

$$\dot{\boldsymbol{x}}=\boldsymbol{A}\boldsymbol{x} \tag{1}$$

式中:$\boldsymbol{x}=[x_1,x_2,\cdots,x_n]^{\mathrm{T}}$,$\dot{\boldsymbol{x}}=[\dot{x}_1,\dot{x}_2,\cdots,\dot{x}_n]^{\mathrm{T}}$;$\boldsymbol{A}$ 为 n 阶方阵。

$$\boldsymbol{A}=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \tag{2}$$

接下来,本文设计了一个线性反馈控制器 $\boldsymbol{B}\boldsymbol{x}$,使得控制系统的原点为一个渐近稳定的不动点;以及设计了一个合适的非线性反馈控制器 $\boldsymbol{f}(\sigma\boldsymbol{x},\varepsilon)$,使得控制系统能够产生无退化的混沌行为:

$$\dot{\boldsymbol{x}}=\boldsymbol{A}\boldsymbol{x}+\boldsymbol{B}\boldsymbol{x}+\boldsymbol{f}(\sigma\boldsymbol{x},\varepsilon) \tag{3}$$

$\boldsymbol{B}\boldsymbol{x}$ 是一个线性反馈控制器,其中矩阵 $\boldsymbol{B}$ 为:

$$\boldsymbol{B}=\begin{pmatrix} b_{11} & & & 0 \\ & b_{22} & & \\ & & \ddots & \\ 0 & & & b_{nn} \end{pmatrix}$$

定义　设 $\boldsymbol{A}$ 是 n 阶方阵,如果数 λ 和 n 维非零列向量 $\boldsymbol{x}$ 使关系式 $\boldsymbol{A}\boldsymbol{x}=\lambda\boldsymbol{x}$ 成立,那么这样的数 λ 称为矩阵 $\boldsymbol{A}$ 特征值,非零向量 $\boldsymbol{x}$ 称为 $\boldsymbol{A}$ 的对应于特征值 λ 的特征向量。

$\boldsymbol{A}\boldsymbol{x}=\lambda\boldsymbol{x}$ 也可写成 $(\boldsymbol{A}-\lambda\boldsymbol{E})\boldsymbol{x}=0$,它有非零解的充分必要条件是系数行列式 $|\boldsymbol{A}-\lambda\boldsymbol{E}|=0$,即:

$$\begin{vmatrix} a_{11}-\lambda & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-\lambda & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}-\lambda \end{vmatrix}=0$$

这意味着对于式(1)中给定 n 的阶方阵 $\boldsymbol{A}$,要配置指定的特征值,只须将矩阵 $\boldsymbol{A}$ 中 $n(n-1)$ 个元素和给定的特征值 λ_1、λ_2、$\cdots$、λ_n 代入上式,剩下的 n 个元素作为未知量,就可以得到一组方程,如下所示:

$$\begin{cases} \begin{vmatrix} a_{11}-\lambda_1 & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-\lambda_1 & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}-\lambda_1 \end{vmatrix}=0 \\ \cdots \\ \begin{vmatrix} a_{11}-\lambda_n & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-\lambda_n & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}-\lambda_n \end{vmatrix}=0 \end{cases} \tag{4}$$

这个 n 维方程组中有 n 个未知数,因此一定有解,求解这个方程组可以得到剩余的 n 个元素,并用这些 n 个元素替换 $\boldsymbol{A}$ 中相应的元素,得到具有指定特征值的矩阵。

如上所述,矩阵的所有特征值都可以配置为任意值。因此,控制器 $\boldsymbol{B}\boldsymbol{x}$ 可以用来配置 $\boldsymbol{A}+\boldsymbol{B}$ 的特征值,

使得 $\boldsymbol{Ax}+\boldsymbol{Bx}$ 的原点是渐近稳定的不动点。接下来,令:

$$\boldsymbol{C}=\boldsymbol{A}+\boldsymbol{B}=\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix} \tag{5}$$

假设控制器只包含一个非线性函数。考虑到耗散,控制器不应影响矩阵 $\boldsymbol{A}$ 的主对角线,因此可以选择:

$$\boldsymbol{f}(\sigma\boldsymbol{x},\varepsilon)=\begin{pmatrix} 0 \\ \vdots \\ f_i(\sigma x_j,\varepsilon) \\ \vdots \\ 0 \end{pmatrix} \tag{6}$$

式中:f_i 是状态变量 $\boldsymbol{x}$ 的第 i 个元素;$x_j(i\neq j)$是状态变量 $\boldsymbol{x}$ 的第 j 个元素。显然,这不会影响 $\boldsymbol{A}$ 的主对角线。接下来,设:

$$f_i(\sigma x_j,\varepsilon)=\varepsilon\sin(\sigma x_j)\quad i,j=1,2,\cdots,n\quad i\neq j \tag{7}$$

式中:ε、σ 为可以调整的控制器参数。

容易证明式(3)的所有解都是全局有界的[18],区间如下所示:

$$\sup_{0\leqslant t<\infty}\|x(t)\|\leqslant\alpha\|x(0)\|+\frac{\alpha}{\beta}\|\varepsilon\|<\infty \tag{8}$$

式中:ε、σ 是常数;$x(0)$是初始值。

让 $\dot{x}_i=0(i=1,2,\cdots,n)$,由式(3)、式(5)得到:

$$\begin{cases} c_{11}x_1^{(e)}+c_{12}x_2^{(e)}+\cdots+c_{1n}x_n^{(e)}=0 \\ c_{21}x_1^{(e)}+c_{22}x_2^{(e)}+\cdots+c_{2n}x_n^{(e)}=-f_2(\sigma_j x_j^{(e)},\varepsilon_j) \\ \vdots \\ c_{i1}x_1^{(e)}+c_{i2}x_2^{(e)}+\cdots+c_{in}x_n^{(e)}=-f_i(\sigma_j x_j^{(e)},\varepsilon_j) \\ \vdots \\ c_{n1}x_1^{(e)}+c_{n2}x_2^{(e)}+\cdots+c_{nn}x_n^{(e)}=0 \end{cases} \tag{9}$$

式中:$e=0,\pm1,\cdots$。

由式(9),本文定义如下行列式:

$$\det\boldsymbol{C}=\begin{vmatrix} c_{11} & \cdots & c_{1k} & \cdots & c_{1n} \\ \vdots & & \vdots & & \vdots \\ c_{i1} & \cdots & c_{ik} & \cdots & c_{in} \\ \vdots & & \vdots & & \vdots \\ c_{n1} & \cdots & c_{nk} & \cdots & c_{nn} \end{vmatrix}$$

$$\det\boldsymbol{C}_k=\begin{vmatrix} c_{11} & \cdots & c_{1k} & \cdots & c_{1n} \\ \vdots & & \vdots & & \vdots \\ c_{i1} & \cdots & -\varepsilon\sin(\sigma x_j) & \cdots & c_{in} \\ \vdots & & \vdots & & \vdots \\ c_{n1} & \cdots & c_{nk} & \cdots & c_{nn} \end{vmatrix} \tag{10}$$

$$\det\boldsymbol{C}_{ik}=(-1)^{i+k}\begin{vmatrix} c_{11} & \cdots & c_{1,k-1} & c_{1,k+1} & \cdots & c_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ c_{i-1,1} & \cdots & c_{i-1,k-1} & c_{i-1,k+1} & \cdots & c_{i-1,n} \\ c_{i+1,1} & \cdots & c_{i+1,k-1} & c_{i+1,k+1} & \cdots & c_{i+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ c_{n1} & \cdots & c_{n,k-1} & c_{n,k+1} & \cdots & c_{nn} \end{vmatrix}$$

$$k=1,2,\cdots,n$$

$$x_k^{(e)}=\frac{\det\boldsymbol{C}_k}{\det\boldsymbol{C}}=-\frac{\det\boldsymbol{C}_{ik}}{\det\boldsymbol{C}}\varepsilon\sin(\sigma x_j^{(e)}) \tag{11}$$

$$k=1,2,\cdots,n$$

由式(11)可以得到:

$$Kx_k^{(e)}=\sin(\sigma x_j^{(e)}) \tag{12}$$

其中 K 为斜率,其计算如下:

$$K=-\frac{\det\boldsymbol{C}}{\varepsilon\det\boldsymbol{C}_k} \tag{13}$$

由式(12),$x_j^{(e)}$ 可以由 e 导出。x_j 的下界 $\sup_{0\leqslant t<\infty}\|x_j(t)\|$ 完全由式(8)给出。因此,区间$[-\sup_{0\leqslant t<\infty}\|x_j(t)\|,\sup_{0\leqslant t<\infty}\|x_j(t)\|]$中平衡点的数量为:

$$E=2\times\operatorname{round}\left(\frac{\sigma}{\pi}\cdot\sup_{0\leqslant t<\infty}\|x_j(t)\|\right)+1 \tag{14}$$

在得到 $x_j^{(e)}$ 之后,可以从式(11)中推导出平衡点的所有其他分量 $x_k^{(e)}(k=1,2,\cdots,n,k\neq j)$。因此,可以得到 $P^{(e)}(x_1^{(e)},x_2^{(e)},\cdots,x_n^{(e)})(e=0,\pm1,\cdots,\pm E/2)$。这意味着可以完全确定控制系统中所有平衡点的分布。

上述控制系统各平衡点 $P^{(e)}(x_1^{(e)},x_2^{(e)},\cdots,x_n^{(e)})$对应的雅可比矩阵如下:

$$\boldsymbol{J}=\begin{pmatrix} c_{11} & \cdots & c_{1j} & \cdots & c_{1n} \\ \vdots & & \vdots & & \vdots \\ c_{i1} & \cdots & c_{ij}+\varepsilon\cos(\sigma x_j) & \cdots & c_{in} \\ \vdots & & \vdots & & \vdots \\ c_{n1} & \cdots & c_{nj} & \cdots & c_{nn} \end{pmatrix} \tag{15}$$

然后,令斜率$|K|\ll1$。假设所有的平衡分布非常接近水平轴,所以 $\cos(\sigma x_j)\approx\pm1(e=0,\pm1,\cdots,\pm E/2)$。

因此,式(3)的系统只包含两种鞍焦点平衡,相应的雅可比矩阵如下:

$$\boldsymbol{J}_{1,2}=\begin{pmatrix} c_{11} & \cdots & c_{1j} & \cdots & c_{1n} \\ \vdots & & \vdots & & \vdots \\ c_{i1} & \cdots & c_{ij}+\varepsilon\sigma & \cdots & c_{in} \\ \vdots & & \vdots & & \vdots \\ c_{n1} & \cdots & c_{nj} & \cdots & c_{nn} \end{pmatrix} \tag{16}$$

详细设计标准如下:

(1) 全局有界设计准则。使标称系统 $\boldsymbol{Cx}$ 为渐近

稳定的线性系统,式(6)所示的非线性反馈控制器一致有界。然后,式(2)的 n 维控制系统是全局有界且满足式(8)区间。

(2) Lyapunov 指数设计准则。设计控制系统(式(2))满足以下条件:对于 n 维连续系统,所有平衡点对应的特征值至少具有 $r=n-2$ 个正实部和$r=n-2$ 个不同的发散方向。因此,式(2)的 n 维控制系统具有 $L=n-2$ 个正 Lyapunov 指数。

具体的设计步骤如下:

1) 对于任意一个连续系统(式(1)),设计一个合适的控制器 $\boldsymbol{Bx}$,该控制器可以将标称系统 $\boldsymbol{Ax}+\boldsymbol{Bx}$ 配置为以原点为稳定焦点的渐近稳定线性系统。需要保证 $\lambda_1,\lambda_2,\cdots,\lambda_n$ 的实部为负,使其稳定焦点为原点,由式(4)得到了一个方程组如式(17)所示。

$$\begin{cases}\begin{vmatrix} c_{11}-\lambda_1 & a_{12} & \cdots & a_{1n} \\ a_{12} & c_{22}-\lambda_1 & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & c_{nn}-\lambda_1 \end{vmatrix}=0 \\ \vdots \\ \begin{vmatrix} c_{11}-\lambda_n & a_{12} & \cdots & a_{1n} \\ a_{21} & c_{22}-\lambda_n & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & c_{nn}-\lambda_n \end{vmatrix}=0 \end{cases} \tag{17}$$

其中 $\lambda_1,\lambda_2,\cdots,\lambda_n$ 可以任意给定,只需要保证其实部均为负,所以这个方程组只有 $b_1,b_2,\cdots,b_n$ 为未知数,所以该方程组一定有解。

2) 设计合适的控制器式(6)、式(7),上述控制系统可通过调节参数 ε 和 σ 有效控制。具体地说,对于式(16)所示的雅可比矩阵,特征值的正实部的个数是确定的。同样地,由式(4)可以得到:

$$\begin{cases}\begin{vmatrix} c_{11}-\lambda_1' & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \cdots & c_{ij}+\varepsilon\sigma & \cdots & c_{in} \\ \vdots & & \vdots & & \vdots \\ c_{n1} & \cdots & c_{nj} & \cdots & c_{nn}-\lambda_1' \end{vmatrix}=0 \\ \vdots \\ \begin{vmatrix} c_{11}-\lambda_n' & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \cdots & c_{ij}+\varepsilon\sigma & \cdots & c_{in} \\ \vdots & & \vdots & & \vdots \\ c_{n1} & \cdots & c_{nj} & \cdots & c_{nn}-\lambda_n' \end{vmatrix}=0 \end{cases} \tag{18}$$

$$\begin{cases}\begin{vmatrix} c_{1}-\lambda_1'' & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \cdots & c_{ij}+\varepsilon\sigma & \cdots & c_{in} \\ \vdots & & \vdots & & \vdots \\ c_{n1} & \cdots & c_{nj} & \cdots & c_{nn}-\lambda_1'' \end{vmatrix}=0 \\ \vdots \\ \begin{vmatrix} c_{11}-\lambda_n'' & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \cdots & c_{ij}+\varepsilon\sigma & \cdots & c_{in} \\ \vdots & & \vdots & & \vdots \\ c_{n1} & \cdots & c_{nj} & \cdots & c_{nn}-\lambda_n'' \end{vmatrix}=0 \end{cases} \tag{19}$$

同样,$\lambda_1',\lambda_2',\cdots,\lambda_n'$和 $\lambda_1'',\lambda_2'',\cdots\lambda_n''$为任意给定的值,根据 Lyapunov 指数设计准则,本文只需要保证其实部为 $r_1=n-1$ 和 $r_2=n-2$。这两个方程组的未知数都只有 $b_1,b_2,\cdots,b_n$ 和 $\varepsilon\sigma$,共 $n+1$ 个,所以式(18)、式(19)也一定有解。

3) 联立式(17)、式(18)、式(19)三个方程组,有 $3n$ 个方程,只有 $n+1$ 个未知数,理论上解有无数组。求解这三组方程,就能得到线性反馈控制器 $\boldsymbol{Bx}$ 以及非线性反馈控制器$\boldsymbol{f}(\sigma\boldsymbol{x},\varepsilon)$。

4) 对于得到的系统,如果系统的简并度 $d>0$,返回步骤 3),得到另一组解。当 $d=0$ 时,整个循环停止。最后,正 Lyapunov 指数的数目达到最大值 $L=n-2$。

2　有两个正 Lyapunov 指数的四维混沌系统

给定一个四维连续系统:

$$\begin{pmatrix}\dot{x}_1\\ \dot{x}_2\\ \dot{x}_3\\ \dot{x}_4\end{pmatrix}=\begin{pmatrix}a_{11}&a_{12}&a_{13}&a_{14}\\ a_{21}&a_{22}&a_{23}&a_{24}\\ a_{31}&a_{32}&a_{33}&a_{34}\\ a_{41}&a_{42}&a_{43}&a_{44}\end{pmatrix}\begin{pmatrix}x_1\\ x_2\\ x_3\\ x_4\end{pmatrix}$$

其中,假定系统矩阵为:

$$\boldsymbol{A}=\begin{pmatrix}a_{11}&a_{12}&a_{13}&a_{14}\\ a_{21}&a_{22}&a_{23}&a_{24}\\ a_{31}&a_{32}&a_{33}&a_{34}\\ a_{41}&a_{42}&a_{43}&a_{44}\end{pmatrix}=\begin{pmatrix}2&-3&4&2\\ 3&1&0.3&1\\ -4.5&1&3&-1\\ -2&2&1&3\end{pmatrix}$$

设非线性反馈控制器为:

$$\boldsymbol{f}(\sigma\boldsymbol{x},\varepsilon)=\begin{pmatrix}0\\ \varepsilon\sin(\sigma x_4)\\ 0\\ 0\end{pmatrix}$$

由式(3),可以得到:

$$\begin{pmatrix}\dot{x}_1\\ \dot{x}_2\\ \dot{x}_3\\ \dot{x}_4\end{pmatrix}=\begin{pmatrix}a_{11}&a_{12}&a_{13}&a_{14}\\ a_{21}&a_{22}&a_{23}&a_{24}\\ a_{31}&a_{32}&a_{33}&a_{34}\\ a_{41}&a_{42}&a_{43}&a_{44}\end{pmatrix}\begin{pmatrix}x_1\\ x_2\\ x_3\\ x_4\end{pmatrix}+$$

$$\begin{pmatrix}b_{11}&&&\\ &b_{22}&&\\ &&b_{33}&\\ &&&b_{44}\end{pmatrix}\begin{pmatrix}x_1\\ x_2\\ x_3\\ x_4\end{pmatrix}+\begin{pmatrix}0\\ \varepsilon\sin(\sigma x_4)\\ 0\\ 0\end{pmatrix}$$

由具体设计步骤 1) - 步骤 2),能得到三组方程如下:

$$\begin{cases}\begin{vmatrix}2+b_{11}-\lambda_1&-3&4&2\\ 3&1+b_{22}-\lambda_1&0.3&1\\ -4.5&1&3+b_{33}-\lambda_1&-1\\ -2&2&1&3+b_{44}-\lambda_1\end{vmatrix}=0\\ \vdots\\ \begin{vmatrix}2+b_{11}-\lambda_4&-3&4&2\\ 3&1+b_{22}-\lambda_4&0.3&1\\ -4.5&1&3+b_{33}-\lambda_4&-1\\ -2&2&1&3+b_{44}-\lambda_4\end{vmatrix}=0\end{cases}$$

$$\begin{cases}\begin{vmatrix}2+b_{11}-\lambda'_1&-3&4&2\\ 3&1+b_{22}-\lambda'&0.3+\varepsilon\sigma&1\\ -4.5&1&3+b_{33}-\lambda'_1&-1\\ -2&2&1&3+b_{44}-\lambda'_1\end{vmatrix}=0\\ \vdots\\ \begin{vmatrix}2+b_{11}-\lambda'_4&-3&4&2\\ 3&1+b_{22}-\lambda'_4&0.3+\varepsilon\sigma&1\\ -4.5&1&3+b_{33}-\lambda'_4&-1\\ -2&2&1&3+b_{44}-\lambda'_4\end{vmatrix}=0\end{cases}$$

$$\begin{cases}\begin{vmatrix}2+b_{11}-\lambda''_1&-3&4&2\\ 3&1+b_{22}-\lambda''_1&0.3-\varepsilon\sigma&1\\ -4.5&1&3+b_{33}-\lambda''_1&-1\\ -2&3&1&1+b_{44}-\lambda''_1\end{vmatrix}=0\\ \vdots\\ \begin{vmatrix}2+b_{11}-\lambda''_4&-3&4&2\\ 3&1+b_{22}-\lambda''_4&0.3-\varepsilon\sigma&1\\ -4.5&01.1&3+b_{33}-\lambda''_4&-1\\ -2&3&1&3+b_{44}-\lambda''_4\end{vmatrix}=0\end{cases}$$

由具体设计步骤 3),得到一组解 $\varepsilon\sigma=225$,

$$B=\begin{pmatrix}-3&&&\\ &-4.5&&\\ &&-1&\\ &&&-2.88\end{pmatrix}$$

由于在求解方程之前,所有矩阵特征值已被设置为满足设计准则,令 $\varepsilon=15$ 和 $\sigma=15$,则受控矩阵的正 Lyapunov 指数的个数是 $L=\min\{r_1,r_2\}=2$,也就是说,该混沌系统具有两个正 Lyapunov 指数,该系统是一个无退化混沌系统,如图 1 所示。

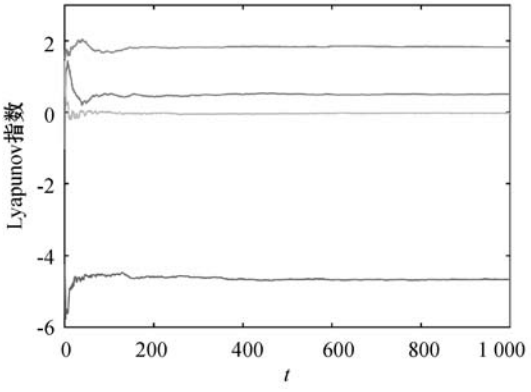

图 1 四维无退化混沌系统的 Lyapunov 指数谱

3 混沌系统量化与性能分析

3.1 混沌序列的生成

为了生存混沌序列密码,必须将混沌系统的输出 $x(t)$ 转换为二进制的序列 $S(t)$。因此引入不可逆函数 $T_n(x(t))$,转换函数 $T_n(x(t))$ 的定义如下:

$$S(t)=T_n(x(t))=\begin{cases}0,x(t)\in\bigcup_{d=0}^{2^{n-1}-1}I_{2d}^n\\ 1,x(t)\in\bigcup_{d=0}^{2^{n-1}-1}I_{2d+1}^n\end{cases}\tag{20}$$

式中:$n>0$ 为任意正整数;$I_0^n,I_1^n,I_2^n,\cdots$ 是区间[0,1]上的 2^n 个连续的等分区间。因为无退化混沌系统相比一般的系统具有良好的随机性,这样生成的二进制序列 $S(t)$ 理论上具有优秀的 0 - 1 平衡性以及初值敏感性。

3.2 混沌序列性能分析

3.2.1 游程测试

游程是指序列中连续不间断的同一比特所构成的子序列。游程测试的目的是计算待测序列中游程的个数,判断“0”或“1”的游程个数是否与随机序列相近似。若以 20 000 比特长度的序列进行游程测试,如果各个游程长度所对应的子序列个数与满足相应的范围要求,则可以认为通过测试。表 1 为游程测试的范围要求和结果对比。

表 1　游程测试

游程长度	游程的范围要求	游程数
1	2 315 ~ 2 685	2 487
2	1 114 ~ 1 386	1 245
3	527 ~ 723	616
4	240 ~ 384	324
5	103 ~ 209	152
6 及以上	103 ~ 209	147

3.2.2　相关性检验

相关性包括序列自相关性和互相关性。

序列的均值为:

$$S_{av} = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} S(t) \tag{21}$$

式中:$S(t)$为系统输出的二值序列。

设 S'、S''为两个混沌二值序列,k 为整数。如果自相关函数 $r(k)$满足:$r(k) = 0(k \neq 0)$;互相关函数$p(k)$满足:$p(k) \to 0$,则序列通过检验。$\gamma(k)$、$p(k)$计算如下:

$$r(k) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} (S'(i) - S_{av})(S'(i+k) - S_{av}) \tag{22}$$

$$p(k) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} (S'(i) - S_{av})(S''(i+k) - S_{av}) \tag{23}$$

序列的相关性函数如图 2 所示。

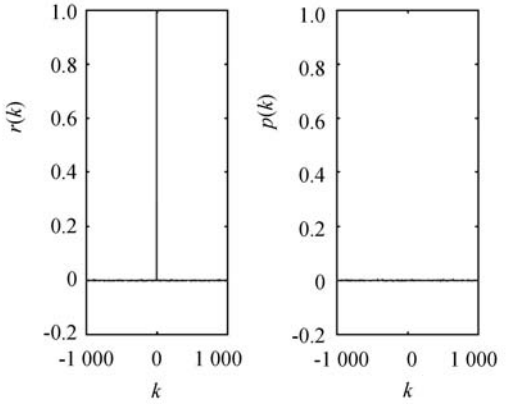

图 2　方案一相关性函数

3.2.3　初值敏感性测试

对初值微小改变后,序列变化率能反映序列的产生对初值的敏感性。理想情况下,序列变化率应为 50%。本文在原初值的基础上增加 10^{-10},仿真得到变化率为 49.97%,由此可知,序列的产生有很强的初值敏感性。

4　结　语

本文提出了一种基于改变矩阵特征值配置具有多个正 Lyapunov 指数连续混沌系统的构造方法。通过引入两个反馈控制器,配置任意受控系统轨道全局稳定,并且将正 Lyapunov 指数的个数配置为最大。通过本文方法,将配置正 Lyapunov 指数的问题转化为求解方程组。如果受控系统任意给定,按照本文方法能够很好地配置正 Lyapunov 指数。之后对无退化混沌系统进行量化,经过性能分析,量化后的序列能很好地应用在序列密码之中。

参　考　文　献

[1] Matsumoto T, Chua L, Kobayashi K. Hyper chaos: Laboratory experiment and numerical confirmation[J]. IEEE Transactions on Circuits and Systems, 1986, 33(11): 1143 - 1147.

[2] Rech P C, Albuquerque H A. A hyperchaotic Chua system [J]. International Journal of Bifurcation and Chaos, 2009, 19(11):3823 - 3828.

[3] Barboza R. Dynamics of a hyperchaotic Lorenz system[J]. International Journal of Bifurcation and Chaos, 2007, 17(12): 4285 - 4294.

[4] 傅文渊,李国刚,王燕琼. 区间长度可变的反向混沌优化算法[J]. 电子学报,2019,47(1):113 - 121.

[5] 付景超,张中华. 超混沌 Bao 系统线性状态反馈控制及自适应控制[J]. 控制与决策,2016,31(9):1707 - 1710.

[6] 张良,唐驾时. 四维超混沌系统 Hopf 分岔分析与反控制[J]. 计算力学学报,2018,35(2):188 - 194.

[7] Li Y X, Chen G R, Tang W K S. Controlling a unified chaotic system to hyperchaotic[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2005, 52(4): 204 - 207.

[8] 张玢. 弱耦合对耦合映像集体动力学行为的影响[J]. 渭南师范学院学报,2019,34(2):82 - 86,96.

[9] Shen C W, Yu S M, Lü J H, et al. Designing hyperchaotic systems with any desired number of positive Lyapunov exponents via a simple model[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2017, 61(8):2380 - 2389.

[10] 杨昌烨,陈艳峰,张波,等. 基于参数扰动的混沌控制方案在 Buck-Boost 变换器中的应用研究[J]. 电源学报,2018, 16(2):32 - 37.

[11] Shen C W, Yu S M, Lü J H, et al. A systematic methodology for constructing hyperchaotic systems with multiple positive Lyapunov exponents and circuit implementation [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2014, 61(3):854 - 864.

[12] Shen C W, Yu S M, Lü J H, et al. Constructing hyperchaotic systems at will[J]. International Journal of Circuit Theory and Applications, 2016, 43(12):2039 - 2056.

(下转第 335 页)

Net-level accuracy with 50x fewer parameters and <0.5MB model size[EB]. arXiv:1602.07360,2016.

[2] Szegedy C, Liu W, Jia Y Q, et al. Going deeper with convolutions[EB]. arXiv:1409.4842,2014.

[3] Ioffe S, Szegedy C. Batch normalization: Accelerating deep network training by reducing internal covariate shift[EB]. arXiv:1502.03167,2015.

[4] Szegedy C, Vanhoucke V, Ioffe S, et al. Rethinking the inception architecture for computer vision[EB]. arXiv:1512.00567,2015.

[5] Chollet F. Xception:Deep learning with depthwise separable convolutions[EB]. arXiv:1610.02357,2016.

[6] Zhang X Y, Zhou X Y, Lin M X, et al. ShuffleNet:An extremely efficient convolutional neural network for mobile devices[EB]. arXiv:1707.01083,2017.

[7] Hu J, Shen L, Albanie S, et al. Squeeze-and-excitation networks[EB]. arXiv:1709.01507,2017.

[8] Howard A G, Zhu M L, Chen B, et al. MobileNets:Efficient convolutional neural networks for mobile vision applications[EB]. arXiv:1704.04861,2017.

[9] Sandler M, Howard A, Zhu M L, et al. MobileNetV2:Inverted residuals and linear bottlenecks[EB]. arXiv:1801.04381,2018.

[10] Ma N N, Zhang X Y, Zheng H T, et al. ShuffleNet V2:Practical guidelines for efficient CNN architecture design[EB]. arXiv:1807.11164,2018.

[11] Zoph B, Vasudevan V, Shlens J, et al. Learning transferable architectures for scalable image recognition[EB]. arXiv:1707.07012, 2017.

[12] Liu C X, Zoph B, Neumann M, et al. Progressive neural architecture search[EB]. arXiv:1712.00559,2017.

[13] Tan M X, Chen B, Pang R M, et al. MnasNet: Platform-aware neural architecture search for mobile[EB]. arXiv:1807.11626,2018.

[14] Goodfellow I J, Shlens J, Szegedy C. Explaining and harnessing adversarial examples[EB]. arXiv:1412.6572,2014.

[15] Moosavi-Dezfooli S, Fawzi A, Frossard P. DeepFool:A simple and accurate method to fool deep neural networks[EB]. arXiv:1511.04599,2015.

[16] Papernot N, McDaniel P, Jha S, et al. The limitations of deep learning in adversarial settings[EB]. arXiv:1511.07528,2015.

[17] Carlini N, Wagner D. Towards evaluating the robustness of neural networks[EB]. arXiv:1608.04644,2016.

[18] Kingma D P, Ba J L. Adam:A method for stochastic optimization[EB]. arXiv:1412.6980,2014.

[19] Loshchilov I, Hutter F. Decoupled weight decay regularization[EB]. arXiv:1711.05101,2017.

[20] Tieleman T, Hinton G. Lecture 6.5-RMSProp: Divide the gradient by a running average of its recent magnitude[J]. COURSERA: Neural Networks for Machine Learning, 2012, 4(2):26 - 31.

[21] John D, Elad H, Yoram S. Adaptive subgradient methods for online learning and stochastic optimization[J]. Journal of Machine Learning Research,2011,12(61):2121 - 2159.

[22] Zeiler M D. ADADELTA:An adaptive learning rate method[EB]. arXiv:1212.5701,2012.

[23] Dean J, Corrado G, Monga R, et al. Large scale distributed deep networks[C]//Proceedings of the 25th International Conference on Neural Information Processing Systems. ACM, 2012:1223 - 1231.

[24] Kidambi R, Netrapalli P, Jain P, et al. On the insufficiency of existing momentum schemes for stochastic optimization[EB]. arXiv:1803.05591,2018.

[25] ImageNet 2012 DataBase[DB/OL]. [2019 - 10 - 31]. http://www.image-net.org/challenges/LSVRC/2012/nonpub-downloads.

[26] Kaggle dogs-vs-cats DataBase[DB/OL]. [2019 - 10 - 31]. https://www.kaggle.com/c/dogs-vs-cats.

[27] Pascal VOC 2012 DataBase [DB/OL]. [2019 - 10 - 31]. https://host.robots.ox.ac.uk/pascal/VOC.

[28] MicroSoft COCO DataBase[DB/OL]. [2019 - 10 - 31]. https://cocodataset.org.

(上接第 307 页)

[13] Matsumoto T. Chaos in electronic circuits[J]. Proceedings of the IEEE,1987,75(8):1033 - 1057.

[14] Lü J H, Chen G R. A new chaotic attractor coined[J]. International Journal of Bifurcation and Chaos,2002, 12(3): 659 - 661.

[15] Chen S K, Yu S M, Lü J H, et al. Design and FPGA-based realization of a chaotic secure video communication system[J]. IEEE Transactions on Circuits and Systems for Video Technology,2018,28(9):2359 - 2371.

[16] Mamat M, Vaidyanathan S, Sambas A, et al. A novel double-convection chaotic attractor, its adaptive control and circuit simulation[J]. IOP Conference Series: Materials Science and Engineering,2018,332:012033.

[17] Vanecek A, Celikovsky S. Control systems: From linear analysis to synthesis of chaos[J]. Automatica, 1998, 34(11):1479 - 1480.

[18] Yu S M, Chen G R. Anti-control of continuous-time dynamical systems[J]. Communications in Nonlinear Science and Numerical Simulation,2012,17(6):2617 - 2627.