文章编号: 1000−8152(2010)05−0597−05

参数扰动超混沌系统输出真随机信号

于　波[1], 胡国四[2,3], 蒋式勤[3]

(1. 烟台大学 工程实训中心, 山东 烟台 264005; 2. 烟台大学 光电信息科学技术学院, 山东 烟台 264005;
3. 同济大学 电子与信息工程学院, 上海 201804)

摘要: 通过分析一个四翼三正Lyapunov指数超混沌系统的基本特性, 获知了3个可调参数对系统动力学特性的影响, 得到最佳可施加扰动的参数选择方案, 构造出一个新的参数扰动超混沌系统. 利用嵌入式系统中的AD转换器, 将其悬空, 得到一个能够采集真随机电路噪声的电路. 将此电路噪声数据做适当变比后, 作为参数扰动量加入超混沌系统中, 使得超混沌系统的输出不再是一个伪随机序列, 而是一个真随机信号.

关键词: 超混沌; 真随机信号; AD转换

中图分类号: O415.5　　**文献标识码**: A

True random signal generated by hyperchaotic system with parameter perturbation

YU Bo[1], HU Guo-si[2,3], JIANG Shi-qin[3]

(1. Engineering Training Center, Yantai University, Yantai Shandong 264005, China;
2. Department of Optics and Electronics, Yantai University, Yantai Shandong 264005, China;
3. School of Electronics and Information Engineering, Tongji University, Shanghai 201804, China)

Abstract: By analyzing the basic characteristics of a four-wing hyperchaotic system with three positive Lyapunov exponents, we find out the influences of three adjustable parameters to the dynamics of system, and determine the best perturbed parameter for generating a new hyperchaotic system by parameter perturbation. A new circuit noise sample circuitry is constructed by using a floating AD input in an embedded system. After amplitude-scale transformation, and the circuit noise data is added to the hyperchaotic system as a parameter perturbation, the output signal of this system will be a true random signal rather than the pseudo one.

Key words: hyperchaos; true random signal; AD converter

1　引言(Introduction)

高质量随机数在信息安全中具有重要的应用. 因为密码被广泛应用于信息系统中, 以实现系统信息的保密性、完整性、可用性、可控性和不可否认性, 因而随机数在密码学中扮演着极其重要的角色. 如何产生高质量的随机数已经成为密码学乃至信息安全领域的一个重要研究方向.

生成随机数的方法繁多, 从产生机理来说, 可分为数学方法和物理方法两种.

数学方法一般为基于纯计算机算法的随机序列产生方法[1~3], 或者利用混沌系统的输出信号, 将之通过一种普适算法[4]转换为均匀随机序列. 这种方法产生的数据随机程度较高, 但由于混沌系统本质上是确定性的, 计算过程中受计算机计算精度(字长)的影响, 计算结果最后必然转化为极长周期序列. 所以通过计算机计算出的混沌序列只是一种伪随机信号.

相比于伪随机数发生器的研究而言, 真随机数发生器的研究还相当初步. 利用物理方法可以产生真随机数, 如调用系统函数[5~7]获取随机信息或使用专门的硬件电路[8~10]. 但在嵌入式单片机系统中, 由于系统规模很小, 可能并没有适合的系统函数可以调用, 为产生随机数而专门设计一个随机信号发生电路则成本太高.

本文提出一种新的单片式真随机信号器的设计方法:

1) 利用单片机的AD输入端, 将其悬空, 则可以从该输入端采集到电路噪声数据, 此噪声数据受单

收稿日期: 2009−01−19; 收修改稿日期: 2009−06−26.
基金项目: 山东省自然科学基金资助项目(ZR2009GQ003); 国家自然科学基金资助项目(60771030); 上海市科学发展基金资助项目(054407061).

片机AD转换位数的影响, 随机程度不高, 但属于真随机信号;

2) 设计一个参数扰动混沌系统, 将随机程度不高的电路噪声采集信号做适当变比后, 作为该系统的参数扰动量输入; 然后利用单片机计算出系统的输出数据序列;

3) 计算所得数据序列通过普适算法[4]转换为均匀随机序列;

4) 随机序列可以通过单片机的I/O口输出或用DA器件转化为模拟量输出.

由于混沌系统具有极端初值敏感性, 真随机的电路噪声作为参数扰动影响了混沌系统的演化轨迹, 等效为随时更改系统的任意时刻初值, 导致两个相同的参数扰动混沌系统即使是从同一个初值出发, 其混沌轨迹也会在一段时间后以指数速度分离(如果是超混沌系统, 则在任何一点处均具有多个分离方向), 输出数据的随机程度很高. 如果需要高速输出随机信号, 则只需要将单片机换成自带AD转换器的能进行高速运算的DSP芯片即可.

2 参数扰动超混沌系统的设计(Design of the hyperchaotic system with parameter perturbation)

为了使得目标真随机序列具有更好的随机性, 可以采用能产生更复杂拓扑结构和具有更多正Lyapunov指数吸引子的超混沌系统. 因为超混沌系统具有两个或两个以上正Lyapunov指数(正Lyapunov指数表示了系统轨迹分离方向, 多个正Lyapunov指数代表系统轨迹具有多个分离方向), 因而微弱差别的初值信号在超混沌系统中会出现更快的分离现象, 系统轨迹更不可预测, 随机性越好.

目前, 能产生超混沌特性吸引子的系统屡见报道, 其反控制方法涉及状态反馈[11]、近似时滞状态反馈[12~14]等. 但这些超混沌系统产生的吸引子只有两个翼, 结构较简单. 为了增加吸引子结构复杂性, 文献[15~17]采用一种坐标变换方法将一类Lorenz系统族的双翼超混沌吸引子转换为具有四翼复杂拓扑结构的超混沌吸引子.

在此选用具有四翼三正Lyapunov指数的超混沌系统[15]为随机信号发生的数学计算部分:

$$\begin{cases} \dot{x} = 10(y-x)+u, \\ \dot{y} = 28x - y - xw^2 - v, \\ \dot{w} = k_1 wxy - k_2 w + k_3 x, \\ \dot{u} = -xw^2 + 2u, \\ \dot{v} = 8y. \end{cases} \tag{1}$$

其中: k_1, k_2, k_3为系统控制参数. 当$k_1 = 1, k_2 = 4, k_3 = 1.2$时可以产生如图1所示的四翼三正Lyapunov指数超混沌吸引子.

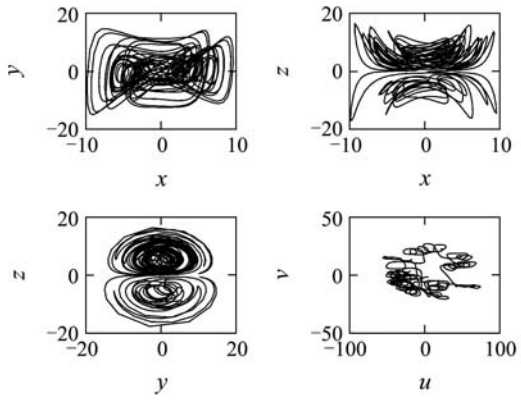


图 1 四翼超混沌吸引子相图

Fig. 1 Phase portraits of four-wing hyperchaotic attractor

可以将扰动量加入该系统的k_1, k_2或k_3参数中, 为了防止加入的扰动量影响系统的动力学特性, 导致超混沌特性的丢失, 需要分别分析参数k_1, k_2和k_3的变化对系统产生的影响. 由于系统的Lyapunov指数谱和该系统的Jacobian矩阵的特征值有关, 从对系统在任意点(x, y, w, u, v)处的Jacobian矩阵开始探讨:

$$J = \begin{pmatrix} -10 & 10 & 0 & 1 & 0 \\ 28-w^2 & -1 & 2xw & 0 & -1 \\ k_3+k_1wy & k_1wx & -k_2+k_1xy & 0 & 0 \\ -w^2 & 0 & -2xw & 2 & 0 \\ 0 & 8 & 0 & 0 & 0 \end{pmatrix}. \tag{2}$$

当$k_3 = 0$时, 原点$S_0(0,0,0,0,0)$是系统的唯一平衡点. 当$k_3 \neq 0$时, 除了原点S_0外, 系统还有两个平衡点. 由于系统轨迹主要在原点S_0附近演化, 所以在原点S_0处的Jacobian矩阵特性能反映该系统的主要特性.

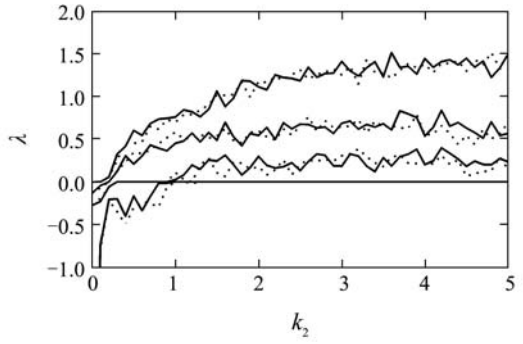
该系统在原点$S_0(0,0,0,0,0)$处的Jacobian矩阵为

$$J_0 = \begin{pmatrix} -10 & 10 & 0 & 1 & 0 \\ 28 & -1 & 0 & 0 & -1 \\ k_3 & 0 & -k_2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 8 & 0 & 0 & 0 \end{pmatrix}. \tag{3}$$

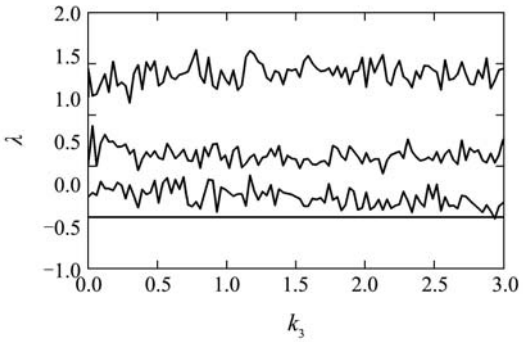
特征多项式为:

$$\begin{aligned} f(\lambda) = (\lambda-2)[&8(\lambda+10)(\lambda+k_2) + \\ &\lambda(\lambda+10)(\lambda+1)(\lambda+k_2) - \\ &280\lambda(\lambda+k_2)] = 0, \end{aligned} \tag{4}$$

显然在该特征多项式中没有出现参数k_1和k_3, 也既特征值不包含参数k_1和k_3, 意味着参数k_1和k_3对系统的超混沌特性影响几乎可以忽略.



(a) $k_3 = 0$



(b) $k_1 = 1, k_2 = 4$

图 2　Lyapunov指数谱

Fig. 2　Spectrum of Lyapunov exponents

在此分别设置参数$k_1 = 1$和2, 计算系统的Lyapunov指数谱随参数k_2的变化(取$k_3 = 0$), 如图2(a)所示. 图2(a)中实线为$k_1 = 1$时的Lyapunov指数谱, 虚线为$k_1 = 2$时的Lyapunov指数谱, 显然两者的前3个正指数变化趋势几乎相同, 也即参数k_1的不同取值对Lyapunov指数谱没有影响, 但参数k_2的值变化对Lyapunov指数谱有决定性影响. 选$k_1 = 1, k_2 = 4$计算系统的Lyapunov指数谱随参数k_3的变化, 如图2(b)所示. 随着参数k_3的递增, Lyapunov指数谱基本保持不变. 计算实验也验证了k_1和k_3对超混沌特性几乎不产生影响.

显然如果将扰动加入参数k_2中可能会更改系统的超混沌特性, 该方案不可取. 从文献[6]中知道参数k_3的主要作用是将上下两个对称的吸引子连接起来构成一个四翼吸引子, 所以对参数k_3施加的扰动可能会破坏吸引子的拓扑结构.

综上所述, 将扰动施加在参数k_1上是最合适的, 新系统为:

$$\begin{cases} \dot{x} = 10(y - x) + u, \\ \dot{y} = 28x - y - xw^2 - v, \\ \dot{w} = (k_1 + p)wxy - k_2 w + k_3 x, \\ \dot{u} = -xw^2 + 2u, \\ \dot{v} = 8y. \end{cases} \tag{5}$$

其中p为参数的随机扰动量, 如果将p取自真随机信号, 如电路噪声, 则等效于施加一个微小的随机量在变量w 上, 随机更改系统变量的当前值, 系统的输出将是一个真随机信号, 而不再是伪随机信号.

3　电路噪声采集电路(Circuit noise detecting circuitry)

在目前的嵌入式单片机系统中, 普遍都配置有AD转换器. 在不增加任何电路成本的前提下, 将嵌入式单片机系统的一个AD输入端悬空, 则可以从该端采集到电路的随机噪声数据. 为了防止现场冲击损坏AD口, 以STC12C5412AD单片机为例, 需要在输入端加如图3(a)所示的电压钳位电路.

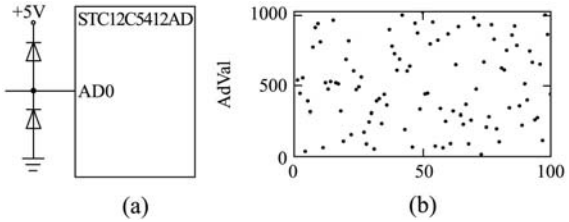


图 3　电路噪声采集电路和噪声数据序列

Fig. 3　Circuit noise sample circuitry and noise data series

采集一段悬空AD输入数据, 并上传给计算机显示, 如图3(b)所示, 显然该信号符合随机的特点. 当然受AD转换器转换分辨率影响, 数据只有1024种取值可能性, 而且随机程度不是很高, 在某些时候会出现短时间内重复相同值的现象, 所以不能将此数据序列直接作为真随机信号使用.

4　电路实现结果(Results of circuit implementation)

采用自带AD转换器的STC12C5412AD单片机设计单片式真随机信号发生器, 该单片机的AD转换器为十位, 采集到的AD转换值AdVal范围为0 ∼ 1023的整型值. 取参数扰动量$p = (\mathrm{AdVal} - 512)/512 * 0.01$, 将单片机计算得到的混沌序列上传后, 得到如图4所示相图. 从图4中可以看出, 其拓扑结构和图1相同, 计算该序列的Lyapunov指数谱为$(1.4328, 0.6474, 0.1643, 0, -11.0116)$, 仍然具有3个正Lyapunov指数. 也即该参数扰动超混沌系统保留了原系统的超混沌特性和四翼拓扑结构.

设定相同的混沌计算初值, 然后分别计算两次,

得到如图5所示的混沌数据序列1(实线)和序列2(虚线), 从图中可以看出, 即使选择相同的初值, 但由于系统被施加了参数扰动, 其两次输出数据将以指数速度分离, 也即不具有伪随机信号在相同初值出发轨迹必然相同的特点, 其输出信号已经是真随机信号.

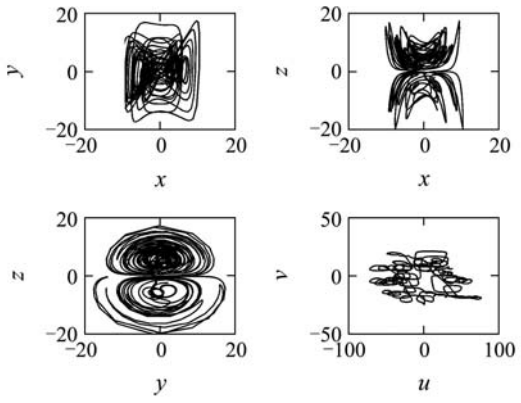


图 4 参数扰动四翼超混沌吸引子相图

Fig. 4 Phase portraits of four-wing hyperchaotic attractor with parameter perturbation

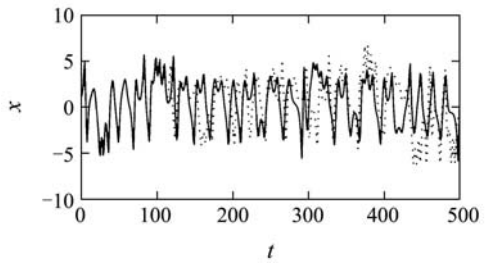


图 5 同初值真随机数据序列

Fig. 5 True random data series with same initial value

5 真随机序列的随机性分析(Randomness analysis of true random sequences)

利用普适算法[4]将系统(5)产生的序列转换为随机二值序列, 分别对其进行频率测试、游程测试和近似熵测试, 定量的分析序列的复杂性, 并将其和Logistic序列的复杂性进行比较.

5.1 频率测试(The frequency test)

频率测试是评估整个序列中所含0和1的个数基本接近的程度, 笔者期望随机序列中0和1的个数相等. 在此用平衡度表示:

$$E = \frac{|N_1 - N_0|}{N}, \tag{6}$$

其中: N_0和N_1表示序列中0和1的个数, N表示序列长度. 平衡度E越小, 均衡性越好. 表1的计算结果表明, 系统(5)产生的二值序列的均衡性远优于Logistic序列. 由于系统(5)输出的为真随机序列, 所以即使从同一初值出发, 计算得到的两个序列1和2, 其平衡度大小也有微小变化.

表 1 二值序列中0,1平衡度比较

Table 1 The balance degree comparison of 0 and 1 in binary sequences

N	500	1000	2000
Logistic序列	0.058	0.050	0.054
系统(5)序列1	0.030	0.012	0.009
系统(5)序列2	0.028	0.014	0.005

5.2 游程测试(The runs test)

序列中出现同样码元串的长度称为游程长度. 显然, 短游程长度的码元串应该占优势. 长度为i的游程出现概率为2^{-i}. 表2给出了2000点Logistic序列和系统(5)序列的游程分布比重平均值.

表 2 游程分布比重平均值

Table 2 The average value of runs distribution proportion

游程类别	1-游程	2-游程	3-游程	4-游程
Logistic序列	0.560	0.240	0.080	0.050
系统(5)序列1	0.490	0.249	0.124	0.068
系统(5)序列2	0.488	0.247	0.127	0.061
理论值	0.500	0.250	0.125	0.0625

从表2的结果中可以看出, 系统(5)产生的真随机序列其游程分布比重平均值比Logistic序列的游程分布平均值更接近理论值.

5.3 近似熵测试((The approximate entropy test)

近似熵算法(ApEn)从多维空间来讨论序列的复杂性, 利用边缘条件概率的统计方法统计序列的随机程度, 用相邻轨道的变化程度体现整个序列的复杂性. 计算近似熵时, 必须先确定两个参数: 嵌入维数p和分辨率参数r, 一般取$p = 2, r = 0.1 - 0.25$ SD(SD是原始序列$x_i(i = 1, 2, \cdots, N)$的标准偏差). 对于任意的p, K进制序列满足

$$0 \leqslant \lim_{0 \to \infty} \mathrm{ApEn}(p, r, N) \leqslant \ln K, \tag{7}$$

所以对于八进制序列, ApEn的最大值为2.079. 分别计算Logistic序列和系统(5)序列的ApEn值, 见表3.

表 3 八进制混沌伪随机序列的ApEn

Table 3 ApEn of octal chaotic sequence

p	1	2	3	4
Logistic序列	0.694	0.692	0.691	0.691
系统(5)序列1	1.985	1.854	1.602	1.320
系统(5)序列2	1.973	1.798	1.531	1.270

从表3可以看到, 系统(5)产生的真随机序列其ApEn值远远大于Logistic序列的ApEn值, 反映了系统(5)产生的序列更趋近于理想随机信号.

6 结论(Conclusion)

本文首先分析了四翼三正Lyapunov指数超混沌系统的3个可调参数对系统动力学特性的影响, 并得到最佳可施加扰动的参数选择方案, 在此基础上构造了一个新的参数扰动超混沌系统. 利用嵌入式系统中普遍存在的AD转换器, 在不增加硬件成本的前提下, 设计了一个十分简单的采集电路噪声的真随机信号发生电路. 将此电路噪声数据做适当变比后, 作为参数扰动量加入超混沌系统中, 使得超混沌系统的输出不再是一个伪随机序列, 而是一个真随机信号.

设计的单片式真随机信号发生电路简单可靠, 如果需要高速的随机信号发生器, 则只需要将单片机替换为能进行高速数据运算的带AD转换器的DSP芯片即可. 相信该电路在保密通信或信息加密领域将发挥重要作用.

参考文献(References):

[1] 刘国良, 高小鹏. Freeswan IKE 伪随机数算法效率分析及改进[J]. 计算机工程, 2005, 31(16): 83 – 85.
(LIU Guoliang, GAO Xiaopeng. Efficiency analysis and improvement to Freeswan IKE random algorithm[J]. *Computer Engineering*, 2005, 31(16): 83 – 85.)

[2] 王新成, 孙宏. 高速伪随机数发生器的设计与实现[J]. 计算机工程与应用, 2004, 40(11): 20 – 23.
(WANG Xincheng, SUN Hong. Research & design on high-performance pseudo-random number generator[J]. *Computer Engineering and Applicaitons*, 2004, 40(11): 20 – 23.)

[3] 王许书, 王新辉, 夏宏. Montgomery方法及其在伪随机数发生器中的应用[J]. 计算机工程与应用, 2001, 37(11): 52 – 53.
(WANG Xushu, WANG Xinhui, XIA Hong. Montgomery method and its application in pseudo－random number generation[J]. *Computer Engineering and Applicaitons*, 2001, 37(11): 52 – 53.)

[4] 盛利元, 肖燕予, 盛喆. 将混沌序列变换成均匀伪随机序列的普适算法[J]. 物理学报, 2008, 57(7): 4007 – 4013.
(SHENG Liyuan, XIAO Yanyu, SHENG Zhe. A universal algorithm for transforming chaotic sequences into uniform pseudo-random sequences[J]. *Acta Physica Sinica*, 2008, 57(7): 4007 – 4013.)

[5] 周庆, 胡月, 廖晓峰. 基于鼠标轨迹和混沌系统的真随机数产生器研究[J]. 物理学报, 2008, 57(9): 5413 – 5418.
(ZHOU Qing, HU Yue, LIAO Xiaofeng. Ture random number generators based on mouse movement and chaos systems[J]. *Acta Physica Sinica*, 2008, 57(9): 5413 – 5418.)

[6] 梁金千, 张跃. 在计算机上产生真随机数的探讨[J]. 计算机工程, 2003, 29(15): 176 – 177.
(LIANG Jinqian, ZHANG Yue. Discussion of generating the real random number in the computer[J]. *Computer Engineering*, 2003, 29(15): 176 – 177.)

[7] 黄枫, 申洪. 基于Inter RNG的真随机数生成器研究[J]. 第一军医大学学报, 2004, 24(9): 1091 – 1095.
(HUANG Feng, SHEN Hong. Intel random number generator-based true random number generator[J]. *Journal of First Military Medical University*, 2004, 24(9): 1091 – 1095.)

[8] 王云峰, 沈海斌, 严晓浪. 混沌随机数发生器的设计[J]. 半导体学报, 2005, 26(12): 2433 – 2439.
(WANG Yunfeng, SHEN Haibin, YAN Xiaolang. Design of a Chaotic Random Number Generator[J]. *Chinese Journal of Semiconductors*, 2005, 26(12): 2433 – 2439.)

[9] 王莱, 刘松强. 真随机数发生器的设计和实现[J]. 核电子学与探测技术, 1998, 18(6): 452 – 455.
(WANG Lai, LIU Songqiang. A true random number generator by sampling thermal noise source[J]. *Nuclear Electronics & Detection Technology*, 1998, 18(6): 452 – 455.)

[10] 俞俊, 沈海斌, 严晓浪. 基于混沌的高速真随机数发生器的设计与实现[J]. 半导体学报, 2004, 25(8): 1013 – 1018.
(YU Jun, SHEN Haibin, YAN Xiaolang. Implementation of chaos-based high-speed truly random number generator[J]. *Chinese Journal of Semiconductors*, 2004, 25(8): 1013 – 1018.)

[11] HU G S. Generating hyper-chaotic attractors with three positive lyapunov exponents via state feedback control[J]. *International Journal of Bifurcation and Chaos*, 2009, 19(2): 651 – 660.

[12] HU G S, JIANG S Q. Generating hyperchaotic attractors via approximate time delayed state feedback[J]. *International Journal of Bifurcation and Chaos*, 2008, 18(11): 3485 – 3494.

[13] HU G S. Hyperchaos of higher order and its circuit implementation[J]. *International Journal of Circuit Theory and Applications*, 2009, DOI: 10.1002/cta.613.

[14] 蒋式勤, 胡国四, 董家鸣, 等. 时滞反馈Lorenz系统的混沌特性及其电路实现[J]. 控制理论与应用, 2009, 26(8): 911 – 914.
(JIANG Shiqin, HU Guosi, DONG Jiaming, et al. Chaotic characteristic and circuit implementation in time-delay feedback Lorenz system[J]. *Control Theory & Applications*, 2009, 26(8): 911 – 914.)

[15] 胡国四. 一类具有四翼吸引子的超混沌系统[J]. 物理学报, 2009, 58(6)：3734 – 3741.
(HU Guosi. A family of hyperchaotic system with four-wing attractors[J]. *Acta Physica Sinica*, 2009, 58(6): 3734 – 3741.)

[16] HU G S, YU B. A hyperchaotic system with a four-wing attractor[J]. *International Journal of Modern Physics C*, 2009, 20(2): 323 – 335.

[17] 胡国四. 超混沌吸引子的翼倍增方案[J]. 物理学报, 2009, 58(12): 8139 – 8145.
(HU Guosi. Scheme for doubling the number of wings in hyperchaotic attractors[J]. *Acta Physica Sinica*, 2009, 58(12): 8139 – 8145.)

作者简介:

于　波　(1975—), 女, 硕士研究生, 实验员, 研究方向为混沌反控制技术及其保密通信, E-mail: fishwave75@163.com;

胡国四　(1974—), 男, 博士研究生, 讲师, 研究方向为混沌反控制技术及其保密通信, E-mail: 8051cpu@gmail.com;

蒋式勤　(1951—), 女, 博士生导师, 教授, 研究方向为控制理论与控制工程、生物医学信号与信息处理, E-mail: sqjiang@tongji.edu.cn.