

## 混沌伪随机序列的谱熵复杂性分析\*

孙克辉<sup>1)2)</sup> 贺少波<sup>1)†</sup> 何毅<sup>1)</sup> 尹林子<sup>1)</sup>

1) (中南大学物理与电子学院, 长沙 410083)

2) (新疆大学物理科学与技术学院, 乌鲁木齐 830046)

(2012年2月27日收到; 2012年7月17日收到修改稿)

为了准确分析混沌伪随机序列的结构复杂性, 采用谱熵算法对 Logistic 映射、Gaussian 映射和 TD-ERCS 系统产生的混沌伪随机序列复杂度进行了分析. 谱熵算法具有参数少、对序列长度  $N$  (惟一参数) 和伪随机进制数  $K$  鲁棒性好的特点. 采用窗口滑动法分析了混沌伪随机序列的复杂度演变特性, 计算了离散混沌系统不同初值和不同系统参数条件下的复杂度. 研究表明, 谱熵算法能有效地分析混沌伪随机序列的结构复杂性; 在这三个混沌系统中, TD-ERCS 系统为广域高复杂度混沌系统, 复杂度性能最好; 不同窗口和不同初值条件下的混沌系统复杂度在较小范围内波动. 为混沌序列在信息安全中的应用提供了理论和实验依据.

**关键词:** 结构复杂性, 谱熵算法, Logistic 映射, Gaussian 映射

**PACS:** 05.45.Tp, 05.45.-a

**DOI:** 10.7498/aps.62.010501

## 1 引言

混沌伪随机序列由混沌系统产生的混沌时间序列量化而得到, 具有类随机性, 因而在保密通信领域有着广泛的应用前景<sup>[1,2]</sup>. 混沌伪随机序列的复杂性是指伪随机序列接近随机序列的程度, 越接近随机序列, 其复杂度越大, 因此伪随机序列复杂性是衡量保密通信系统抗干扰、抗截获能力的重要指标之一<sup>[3,4]</sup>.

混沌序列的复杂度可从行为复杂度和结构复杂度两方面进行分析. 行为复杂度是指从混沌序列本身出发, 利用一定方法度量短时间窗口内序列产生新模式概率的大小, 产生新模式概率越大则序列越复杂. 目前, 计算混沌伪随机序列行为复杂度的算法比较多, 且均以 Kolmogorov 方法<sup>[5]</sup> 和香农熵<sup>[6]</sup> 为基础, 如文献<sup>[7]</sup> 利用 Lempel-Ziv 算法<sup>[8]</sup> 计算二进制混沌伪随机序列的复杂度, 但此算法需要符号化序列, 只在一维方向上计算序列的复杂性, 且涉及序列长度  $N$  的选取问题, 具有一定局限性; 文献<sup>[9, 10]</sup> 分别利用近似熵算法 (ApEn)<sup>[11]</sup> 和模糊熵算法 (FuzzyEn)<sup>[12]</sup> 测量混沌伪随机序列复杂度,

但此类算法计算耗时大; 文献<sup>[13—15]</sup> 分别利用强度统计 (LMC) 算法<sup>[16]</sup> 和符号熵 (SymEn) 算法<sup>[17]</sup> 测量混沌序列复杂度, 这类算法计算速度快, 且结果比较准确, 但是如果选取的维数过高或者伪随机序列符号空间过大时, 计算结果会溢出, 甚至得不到结果. 结构复杂度<sup>[18]</sup> 是指通过变换域内的频率特性、能量谱特性等来分析序列的复杂程度, 序列变换域内能量谱分布越均衡, 表示原序列越接近随机信号, 即序列复杂性越大, 结合香农熵概念即可计算出相应的谱熵值. 结构复杂度对变换域能量特征进行分析, 其针对的是序列的全部而不是局部, 因而与行为复杂度算法相比, 其结果具有全局统计意义, 现有的变换方法主要有傅里叶变换和小波变换等, 算法计算速度快. 目前, 利用结构复杂度算法分析混沌伪随机序列复杂性鲜有报道, 开展这方面的研究具有重要意义.

本文采用谱熵复杂度算法对混沌伪随机序列复杂度进行分析, 内容安排为: 第 2 部分, 给出谱熵复杂度算法描述; 第 3 部分, 利用功率谱图分析了 Logistic 映射、Gaussian 映射、ERCS 系统和 TD-ERCS 系统产生的混沌伪随机序列的结构复杂

\* 国家自然科学基金 (批准号: 61161006, 61073187) 资助的课题.

† 通讯作者. E-mail: heshabo.123@163.com

性, 然后利用谱熵算法计算了混沌伪随机序列的结构复杂度, 并分析了混沌伪随机序列随时间的演化特性, 计算了不同初值和不同参数条件下的复杂度; 最后得出本文的结论.

## 2 谱熵复杂度算法描述

谱熵 (spectral entropy, SE)<sup>[19]</sup> 采用傅里叶变换, 通过傅里叶变换域内能量分布, 结合香农熵得出相应谱熵值, 其算法流程如下.

**第 1 步** 去直流. 对长度为  $N$  的混沌伪随机序列  $\{x(n), n = 0, 1, 2, \dots, N-1\}$  采用下式去掉直流部分, 使得频谱能更有效地体现信号能量信息.

$$x(n) = x(n) - \bar{x}, \quad (1)$$

其中,  $\bar{x} = \frac{1}{N} \sum_{n=0}^{N-1} x(n)$ .

**第 2 步** 对序列  $x(n)$  进行离散傅里叶变换

$$X(k) = \sum_{n=0}^{N-1} x(n) e^{-j\frac{2\pi}{N}nk} = \sum_{n=0}^{N-1} x(n) W_N^{nk}, \quad (2)$$

其中  $k = 0, 1, 2, \dots, N-1$ .

**第 3 步** 计算相对功率谱. 对于变换后的  $X(k)$  序列取前面一半进行计算, 依据 Paserval 定理, 计算其某一个频率点的功率谱值为

$$p(k) = \frac{1}{N} |X(k)|^2, \quad (3)$$

其中,  $k = 0, 1, 2, \dots, N/2-1$ , 则序列的总功率可定义为

$$p_{\text{tot}} = \frac{1}{N} \sum_{k=0}^{N/2-1} |X(k)|^2, \quad (4)$$

则序列的相对功率谱概率  $P_k$  为

$$P_k = \frac{p(k)}{p_{\text{tot}}} = \frac{\frac{1}{N} |X(k)|^2}{\frac{1}{N} \sum_{k=0}^{N/2-1} |X(k)|^2} = \frac{|X(k)|^2}{\sum_{k=0}^{N/2-1} |X(k)|^2}, \quad (5)$$

易知,  $\sum_{k=0}^{N/2-1} P_k = 1$ .

**第 4 步** 计算谱熵. 利用相对功率谱密度  $P_k$ , 结合香农熵概念, 求得信号的谱熵  $se$  为<sup>[20]</sup>

$$se = - \sum_{k=0}^{N/2-1} P_k \ln P_k, \quad (6)$$

式中, 如果  $P_k$  为 0, 则定义  $P_k \ln P_k$  为 0. 可以证明, 谱熵的大小收敛于  $\ln(N/2)$ , 为了便于对比分析, 将

谱熵归一化, 得到归一化的谱熵 SE 为

$$SE(N) = \frac{se}{\ln(N/2)}. \quad (7)$$

可见, 当序列功率谱分布越不均衡时, 序列频谱结构越简单, 信号中具有明显的振荡规律, 得到的 SE 测度值越小, 即复杂度越小, 否则复杂度越大. 从算法定义可以看出, 谱熵算法参数少, 只有序列长度  $N$  一个.

## 3 混沌伪随机序列结构复杂性分析

目前, 离散混沌系统在混沌保密通信、混沌密码学等领域中有着广泛应用, 其中 Logistic 映射是被研究和用最广泛的离散混沌系统, Gaussian 映射是一维离散混沌系统, TD-ERCS 系统为一类二维离散混沌系统, 具有丰富的动力学特性.

### 3.1 混沌伪随机序列产生

#### 3.1.1 Logistic 映射

$$x_{n+1} = \mu x_n (1 - x_n), \quad (8)$$

其中, 参数  $\mu \in (0, 4]$ ,  $x_n \in (0, 1)$ , 当  $3.5699 \dots \leq \mu \leq 4$  时, 系统处于混沌状态.

#### 3.1.2 Gaussian 映射<sup>[21]</sup>

$$x_{n+1} = e^{-bx_n^2} + c, \quad (9)$$

当参数  $b = 7.5, c = -0.6$  时, 系统为混沌态.

#### 3.1.3 TD-ERCS 系统<sup>[22]</sup>

$$\begin{cases} x_n = -\frac{2k_{n-1}y_{n-1} + x_{n-1}(u^2 - k_{n-1}^2)}{u^2 + k_{n-1}^2}, \\ k_n = \frac{2k'_n - k_{n-1} + k_{n-1}k_{n-1}^2}{1 + 2k_{n-1}k'_n - k_n^2} \quad n = 1, 2, 3, \dots, \\ k'_{n-m} = -\frac{x_{n-m}u^2}{y_{n-m}} \quad (m \leq n), \\ y_n = k_{n-1}(x_n - x_{n-1}) + y_{n-1}, \end{cases} \quad (10)$$

式中, 系统参数  $u \in (0, 1]$ , 变量  $|x_n| \leq 1, |y_n| \leq 1, m$  为整数, 代表切延迟大小,  $k'_{n-m}$  为延迟  $m$  后椭圆切线的斜率.  $k_0$  可由入射角  $\alpha$  确定, 方法如下.

首先, 由系统初始值  $x_0$  及系统参数  $u$  计算出  $y_0$  及斜率  $k'_0$

$$y_0 = u\sqrt{1 - x_0^2}, \quad (11)$$

$$k'_0 = -\frac{x_0}{y_0}u^2. \quad (12)$$

然后利用三角函数关系, 求得

$$k_0 = \frac{\tan \alpha + k'_0}{1 - k'_0 \tan \alpha}, \quad (13)$$

其中, 参数  $(u, x_0, \alpha, m)$  为系统种子参数, 确定了系统种子参数, 系统特性也就随之确定, 且有  $u \in (0, 1], x_0 \in (-1, 1], \alpha \in (0, \pi), m = 0, 1, 2, \dots$ . 当  $m = 0$  时系统为 ERCS 系统, 系统处于周期状态; 当  $m \geq 1$  时, 系统为 TD-ERCS 系统, 处于混沌状态, 且当  $m \geq 2$  时, 系统相空间为“混乱态”, 所以在下面的分析中 TD-ERCS 系统参数  $m$  取 2. 对 (10) 式进行迭代就能得到一组混沌序列  $\{x_n, k_n\}$ .

本文采用如下判决公式对已产生的混沌序列进行量化, 首先将序列归一化到  $[0, 1]$ , 若

$$\sin^2\left(\frac{j\pi}{2K}\right) \leq x(n) \leq \sin^2\left(\frac{(j+1)\pi}{2K}\right),$$

则

$$X(n) = j, \quad (14)$$

其中  $j = 0, 1, 2, \dots, K-1$ , 即可得到  $K$  进制混沌伪随机序列  $\{X(n), n = 0, 1, 2, \dots, N-1\}$  [9].

### 3.2 混沌伪随机序列的谱熵复杂度

#### 3.2.1 功率谱分析

对 Logistic 映射 ( $\mu = 3.8, x_0 = 0.43$ ), Gaussian 映射 ( $b = 7.5, c = -0.6, x_0 = 0.4$ ), ERCS 系统 (0.7123, 0.7654, 0.9876, 0) 和 TD-ERCS 系统 (0.7123, 0.7654, 0.9876, 2) 产生的序列, 舍去前面 1000 个数据点, 取序列长度  $N$  为 1000, 进行 8 进制伪随机化, 并进行快速傅里叶变换, 从功率谱分布情况分析混沌系统的结构复杂性大小, 不同系统的功率谱如图 1 所示.

从图 1 可知, 由于 ERCS 系统是周期系统, 其伪随机序列功率谱能量比较集中, 复杂度最小; Logistic 映射和 Gaussian 映射的能谱分布比较均衡, 两者复杂性明显比 ERCS 系统的大, 但两者之间哪个更大从图中不能直接判断; TD-ERCS ( $m = 2$ ) 功率谱分布更为均衡, 显然其复杂度是四个系统中最大的. 从图 1 可见, 利用功率谱图分析只能区分混沌系统和周期系统, 混沌系统之间复杂度大小关系可初步判断. 为了得到准确的数值结果, 则需要采用谱熵算法进行计算分析.

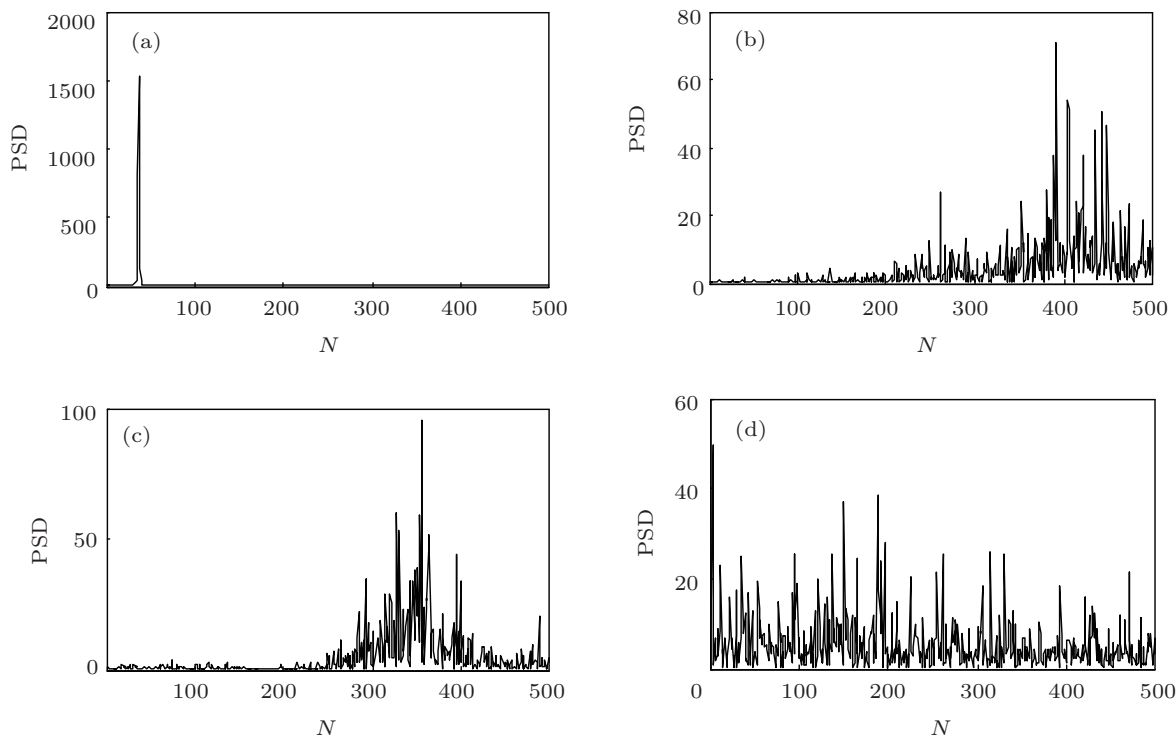


图 1 不同混沌系统伪随机序列功率谱分析 (a) ERCS 系统; (b) logistic 映射; (c) Gaussian 映射; (d) TD-ERCS 系统 ( $m = 2$ )

### 3.2.2 谱熵 (SE) 分析

为了分析混沌伪随机序列结构复杂度变化规律, 采用谱熵算法对 Logistic 映射、Gaussian 映射、ERCS 系统和 TD-ERCS 系统产生的伪随机序列进行谱熵复杂度分析, 分别计算了不同系统产生的不同进制 ( $K$  变化) 伪随机序列和不同系统产生的 8 进制混沌伪随机序列取不同长度 ( $N$  变化) 时的谱熵复杂度, 其结果如图 2 所示. 图 2(a) 中, 不同伪随机序列复杂度由大到小分别为 TD-ERCS 系统、Logistic 映射、Gaussian 映射和 ERCS 系统, 同

时当进制数  $K$  变化时, 不同系统产生的混沌伪随机序列结构复杂度变化不大, 且随  $K$  增大而趋于稳定; 图 2(b) 中, 当序列长度  $N$  变化时, Logistic 映射、Gaussian 映射和 TD-ERCS 系统伪随机序列的复杂度基本保持不变, 而 ERCS 系统结构复杂度最小, 且当序列长度  $N$  大于 50 时都能有效测度出序列的复杂度, 即谱熵算法对序列长度  $N$  有很好的鲁棒性. 下文中不做特殊说明时, 序列长度  $N$  取 1000,  $K$  取 8.

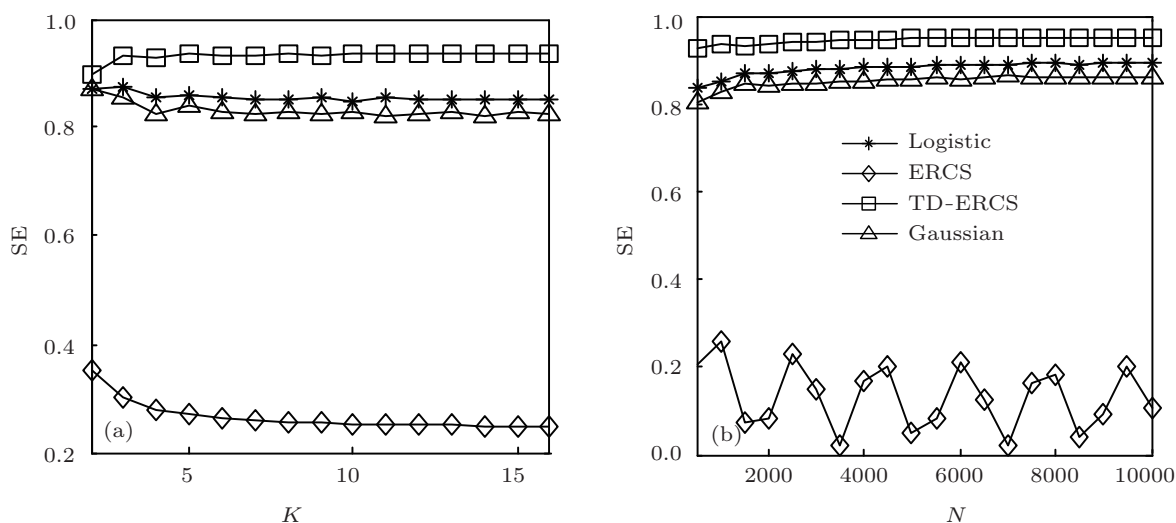


图 2 不同混沌系统伪随机序列 SE 复杂度 (a) 进制数  $K$  变化; (b) 序列长度  $N$  变化

### 3.2.3 复杂度的时间演变特征

复杂度的时间演变特征可用来分析混沌系统产生的伪随机序列随时间演变的稳定性, 本文采用滑动窗口法分析不同混沌伪随机序列 SE 复杂度, 其变化特征如图 3 所示, 系统参数和初值与前面相同, 产生的序列长度  $N = 10000$ , 窗口长度  $L = 1000$ , 滑动步长  $M = 100$ . 由图可见, Logistic 映射 ( $\mu = 3.8$ ) 复杂度波动范围为 0.840—0.855, Gaussian 映射复杂度波动范围为 0.780—0.840; Logistic 映射参数  $\mu$  为 4.0 时结构复杂度明显大于参数  $\mu$  为 3.8 时的复杂度; Gaussian 映射的复杂度是最小的, 其波动范围也最大, Logistic 映射 ( $\mu = 4.0$ ) 和 TD-ERCS 系统的复杂度波动范围更小, 可见复杂性大的系统产生的序列随时间演变时复杂性稳定; 在某一些窗口 Logistic 映射 ( $\mu = 4.0$ ) 复杂度大于 TD-ERCS 系统的复杂度, 而在另一些窗口 Logistic 映射 ( $\mu = 4.0$ ) 复杂度比 TD-ERCS 系统小, 即从系统结构复杂度演变特性来看, TD-ERCS 系统和 Logistic 映射 ( $\mu = 4.0$ ) 的复杂度相当.

### 3.2.4 初值对复杂度影响

下面研究不同初始条件下系统产生的伪随机序列复杂度, 为实际应用提供初值选取参考依据. 图 4 为 Logistic 映射、Gaussian 映射和 TD-ERCS 系统产生的伪随机序列结构复杂度随初始条件改变的变化情况, 其中  $x_0$  从 0.1 到 0.9 等间隔取 50 个点, 舍去迭代序列的前面 1000 个点. 由图 4 可见, 初始条件不同, 系统的复杂度是不同的, 即本文从复杂性角度反映出混沌系统对初始条件的敏感性; 对于同一系统, 初始条件改变, 复杂度变化不是很大, 如 Logistic 映射复杂度变化区域在 0.920 到 0.940 之间; 复杂度大的系统, 复杂度波动性小, 即对初值选取的要求小; Gaussian 映射复杂度最小, TD-ERCS 系统和 Logistic 映射复杂度大致在 0.93 附近波动, 两者复杂性相当.

### 3.2.5 系统参数变化对复杂度影响

系统参数是影响系统状态的最主要因素之一, 为了进一步分析系统的复杂性, 下面考察各系统随

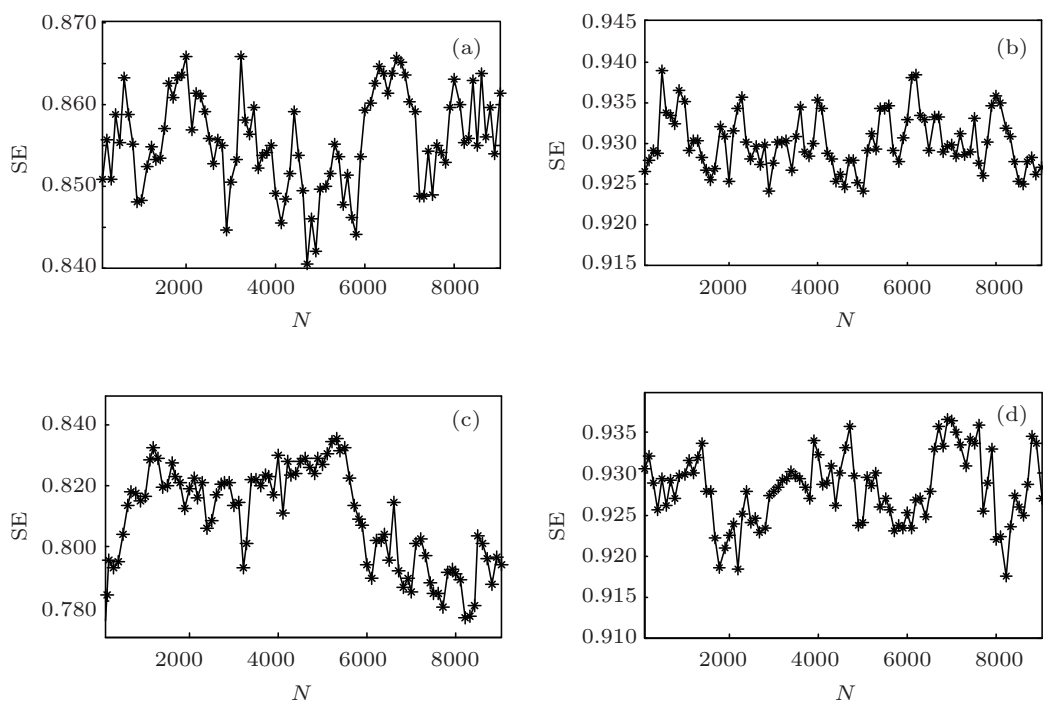


图3 不同混沌系统伪随机序列  $SE$  复杂度演变特征 (a) Logistic ( $\mu = 3.8$ ); (b) Logistic ( $\mu = 4.0$ ); (c) Gaussian; (d) TD-ERCS

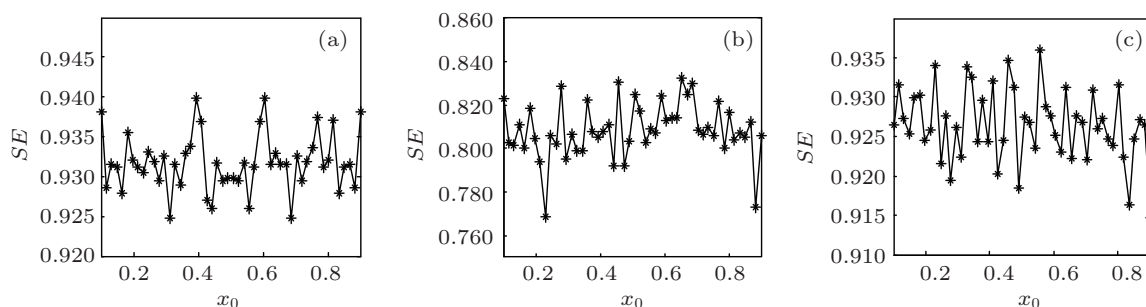


图4 初值对不同混沌系统伪随机序列  $SE$  复杂度的影响 (a) Logistic ( $\mu = 4.0$ ); (b) Gaussian; (c) TD-ERCS

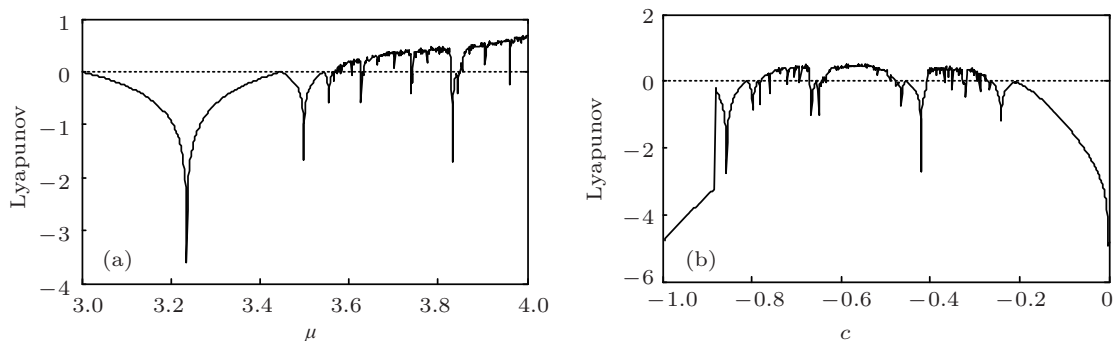


图5 Logistic 和 Gaussian 的 Lyapunov 指数图 (a) Logistic 映射; (b) Gaussian 映射 ( $b = 7.5$ )

参数变化时复杂性变化情况. Logistic 映射和 Gaussian 映射的 Lyapunov 指数如图 5 所示, 不同混沌系统伪随机序列 SE 复杂度随参数变化的情况如图 6 所示. 对比 Logistic 映射 SE 复杂度曲线和 Lyapunov 指数图, 可见当系统处于周期态时, SE 复杂度很小, 甚至为 0, 当系统处于混沌态时复杂度大,  $\mu$  接近 4 时复杂度大于 0.9. 所以对于 Logistic 系统, 在实际使用中,  $\mu$  应取接近 4 的值; 对比 Gaussian 映射 SE 复杂度曲线和 Lyapunov 指数图, 可知当系统处于混沌态时, SE 复杂度处于 0.6 到 0.9 之间, SE 算法检测出了系统的长、短周期窗口. 图 6(c)

中, 当  $m \geq 1$  时, 系统的复杂度大于 0.9, 且改变切延迟参数复杂性改变不大. 图 6(d) 中, 当  $u > 0.4$  时, 系统复杂度大于 0.9, 随着  $u$  值增大, 系统复杂性增大. 对比三个系统, Gaussian 映射复杂性最小, 但其处于混沌态时, 复杂度与 Logistic 系统  $\mu$  处于 3.8 左右时的复杂度相当, 即 Gaussian 可以满足实际使用要求, TD-ERCS 系统复杂度在  $m \geq 1$  和  $u > 0.4$  时复杂度大于 0.9, 可见其高复杂度区域范围大于 Logistic 映射, 使得其在实际使用中参数选取更为灵活, 密钥空间更大.

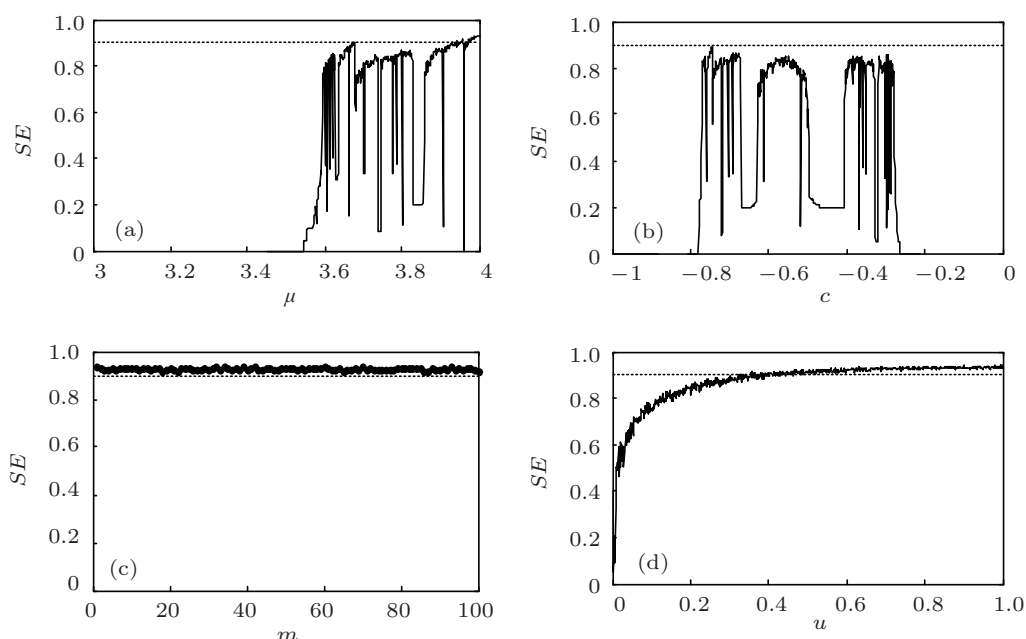


图 6 不同混沌系统伪随机序列 SE 复杂度随参数变化情曲线 (a) Logistic 映射; (b) Gaussian 映射 ( $b = 7.5$ ); (c) TD-ERCS(0.7123, 0.7654, 0.9876,  $m$  变化); (d) TD-ERCS ( $u$  变化, 0.7654, 0.9876, 2)

### 4 结论

采用基于傅里叶变换的谱熵复杂度算法分析了混沌伪随机序列的复杂度. 谱熵算法物理概念清晰, 计算速度快, 实时性好, 但也有本身的缺点. 首先, 基于傅里叶变换的功率谱在短时间窗口内可能会降低频率分辨率, 且会引起旁瓣泄漏; 另外, 基于傅里叶变换的功率谱估计难以适应平稳时间信号, 此时可以采用其他变换方法, 如小波变换. 采用滑动窗口法、改变初始条件和改变系统参数等分析方法, 对 Logistic 映射、Gaussian 映射和 TD-ERCS 系统产生的混沌伪随机序列谱熵复杂度进行了分析, 并得出以下结论.

1) 利用功率谱图只能区分伪随机序列的周期

态和混沌态, 并大致分析其复杂性; 采用谱熵算法则可准确分析混沌伪随机序列的复杂度, 且该算法对序列长度  $N$  和伪随机序列进制数  $K$  有很好的鲁棒性.

2) Gaussian 映射结构复杂度与 Logistic 映射 ( $\mu = 3.8$ ) 复杂度相当, 复杂度稍小; TD-ERCS 的结构复杂度与 Logistic 映射 ( $\mu = 4.0$ ) 复杂度相当, 且当参数  $m$  大于等于 1,  $u$  大于 0.4 时, 结构复杂度恒大于 0.9, 即 TD-ERCS 是一类广域高复杂度系统, 比 Logistic 系统参数选取自由度大 (密钥空间更大), 所以从复杂度的角度来看, TD-ERCS 系统是进行保密通信比较理想的模型.

3) 对系统伪随机序列复杂度的演变特征和不同初始条件下复杂度分析结果表明, 谱熵复杂度能

保持相对稳定性,在一定范围内波动,且复杂度大的系统波动范围相对较小,可见复杂度也反映了混

沌系统丰富的动力学特性.

- 
- [1] Zhou Q, Hu Y, Liao X F 2009 *Acta Phys. Sin.* **58** 4477 (in Chinese) [周庆, 胡月, 廖晓峰 2009 物理学报 **58** 4477]
- [2] Li J B, Zeng Y C, Chen S B, Chen J S 2011 *Acta Phys. Sin.* **60** 060508 (in Chinese) [李家标, 曾以成, 陈仕必, 陈家胜 2011 物理学报 **60** 060508]
- [3] Li Z, Cai J P, Chang Y L 2009 *IEEE Trans. Commun.* **57** 812
- [4] Li Z, Cai J P, Lu X F, Si J B 2009 *Communications*, 2009. *ICC* 09. *IEEE International Conference on* (6) p1-5
- [5] Kolmogorov A N 1965 *Prob. Inform. Trans.* **35** 1546
- [6] Shannon C E 1948 *Bell System Technical Journal* **27** 397
- [7] Liu N S 2011 *Commun. Nonlinear Sci. Numer. Simulat.* **16** 761
- [8] Lempel A, Ziv J 1976 *IEEE Trans.* **IT-22** 75
- [9] Sun K H, Tan G Q, Sheng L Y 2008 *Acta Phys. Sin.* **57** 3359 (in Chinese) [孙克辉, 谈国强, 盛利元 2008 物理学报 **57** 3359]
- [10] Chen X J, Li Z, Bai B M 2011 *J. Electron. Inform. Technol.* **33** 1198 (in Chinese) [陈小军, 李赞, 白宝明 2011 电子与信息学报 **33** 1198]
- [11] Pincus S M 1995 *Chaos* **5** 110
- [12] Chen W T, Wang Z, Xie H, Yu W X 2007 *IEEE Trans. Neural Sys. Rehabil. Eng.* **15** 266
- [13] Sun K H, He S B, Sheng L Y 2011 *Acta Phys. Sin.* **60** 020505 (in Chinese) [孙克辉, 贺少波, 盛利元 2011 物理学报 **60** 020505]
- [14] Luo S J, Qiu S S, Chen X 2010 *J. South China Univ. Technol.* **38** 18 (in Chinese) [罗松江, 丘水生, 陈旭 2010 华南理工大学学报 **38** 18]
- [15] Xiao F H, Yan G R, Han Y H 2004 *Acta Phys. Sin.* **53** 2877 (in Chinese) [肖方红, 阎桂荣, 韩宇航 2004 物理学报 **53** 2877]
- [16] Larrondo H A, González C M, Martin M T 2005 *Physica A* **356** 133
- [17] Rajeev K A, Subba R J, Ramakrishna R 2002 *Chaos, Solitons and Fractals* **14** 633
- [18] Abdulnasir Y, Mehmet A, Mustafa P 2009 *Exp. Syst. Appl.* **36** 7390
- [19] Phillip P A, Chiu F L, Nick S J 2009 *Phys. Rev. E* **79** 011915
- [20] Malihe S, Serajeddin K, Reza B 2009 *Artif. Intell. Med.* **47** 263
- [21] Vinod P 2006 *Electron. J. Theor. Phys.* **3** 29
- [22] Sheng L Y, Wen J, Cao L L, Xiao Y Y 2007 *Acta Phys. Sin.* **56** 78 (in Chinese) [盛利元, 闻姜, 曹莉凌, 肖燕予 2007 物理学报 **56** 78]

# Complexity analysis of chaotic pseudo-random sequences based on spectral entropy algorithm\*

Sun Ke-Hui<sup>1)2)</sup> He Shao-Bo<sup>1)†</sup> He Yi<sup>1)</sup> Yin Lin-Zi<sup>1)</sup>

1) (*School of Physics and Electronics, Central South University, Changsha 410083, China*)

2) (*School of Physics Science and Technology, Xinjiang University, Urumqi 830046, China*)

(Received 27 February 2012; revised manuscript received 17 July 2012)

## Abstract

To analyze the complexity of chaotic pseudo-random sequences accurately, spectral entropy (SE) algorithm is used to analyze chaotic pseudo-random sequences generated by Logistic map, Gaussian map or TD-ERCS system. The SE algorithm has few parameters, and has high robustness with the sequence length  $N$  (the only parameter) and the pseudo-random binary number  $K$ . Using sliding window method, the evolution features are analyzed, and complexity of discrete chaotic systems with different initial conditions and system parameters are calculated. The results show that SE algorithm is effective for analyzing the complexity of the chaotic pseudo-random sequences, and TD-ERCS is a high complexity system with wide parameter range, and has the best complex performance among the three chaotic systems. The complexity of the same chaotic system with different initial values fluctuates within a small range. It provides a theoretical and experimental basis for the applications of chaotic sequences in the field of information security.

**Keywords:** structure complexity, spectral entropy, Logistic map, Gaussian map

**PACS:** 05.45.Tp, 05.45.-a

**DOI:** 10.7498/aps.62.010501

---

\* Project supported by National Natural Science Foundation of China (Grant Nos. 61161006, 61073187).

† Corresponding author. E-mail: hshaobo\_123@163.com