基于小波包能量熵的混沌序列复杂度分析

梁涤青[1,2,3],陈志刚[2,4],邓小鸿[2,5]
(1.中南大学信息科学与工程学院,湖南长沙 410083; 2.中南大学"移动医疗"教育部-中国移动联合实验室,湖南长沙 410075; 3.长沙理工大学信息化处,湖南长沙 410114; 4.中南大学软件学院,湖南长沙 410075; 5.江西理工大学应用科学学院,江西赣州 341000)

摘 要: 混沌密码学是密码学的一个新方向,混沌序列的复杂度是衡量混沌密码学安全性的重要指标.本文将小波包能量熵应用到混沌序列的复杂度分析中,首先将混沌序列进行小波包分解,然后通过小波包能量熵计算方法确定各频段能量大小,从而确定混沌序列的复杂度.通过对 Logistic、TD-ERCS 和 Henon 产生的混沌序列进行比较分析,结果表明,小波包能量熵具有全局统计特性,无需引入新参数进行相空间重构.另外,计算方法简单,且不依赖于混沌序列的采样长度与初始值,能有效衡量混沌序列的复杂度.

关键词: 小波包分解; 小波熵; 混沌序列; 混沌加密; 复杂度
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2015)10-1971-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.10.014

Analysis of Chaotic Sequence Complexity Based on Wavelet Packet Energy Entropy

LIANG Di-qing[1,2,3], CHEN Zhi-gang[2,4], DENG Xiao-hong[2,5]
(1. *College of Information Science and Engineering, Central South University, Changsha, Hunan* 410083, *China*;
2. "*Mobile Health*" *Ministry of Education-China Mobile Joint Laboratory, Central South University, Changsha, Hunan* 410075, *China*;
3. *Information Department, Changsha University of Science and Technology, Changsha, Hunan* 410114, *China*;
4. *College of Software, Central South University, Changsha, Hunan* 410075, *China*;
5. *College of Applied Science, Jiangxi University of Science and Technology, Ganzhou, Jiangxi*, 341000, *China*)

Abstract: Chaotic cryptography is a new direction of cryptography, and chaotic sequence complexity is an important index to measure the security of chaotic cryptography. The wavelet packet energy entropy is discussed in this paper to analyze the complexity of chaotic sequence. Firstly, chaotic sequences are decomposed by wavelet packet, and then each frequency band's energy can be computed with wavelet energy entropy calculation method. Thus the complexity of chaotic sequences is finally determined. Comparing the chaotic sequences generated by Logistic, TD-ERCS and Henon, we can discover that the wavelet packet energy entropy has the global statistical property, which doesn't require new parameters for phase space reconstruction. In addition, its calculation method is simple and it does not rely on the chaotic sequence's sampling length and initial values, which can effectively measure the complexity of chaotic sequences.

Key words: wavelet packet decomposition; wavelet entropy; chaotic sequence; chaos encryption; complexity

1 引言

混沌系统的随机性、遍历性及对初始值敏感等特性与密码学中的混乱与扩散原则相似,能较好地应用于密码学中,形成密码学的新方向——混沌密码学[1~4].混沌序列由混沌系统产生,其复杂度越高,所产生的混沌密码安全性越好[5,6],研究混沌序列复杂度对混沌密码学有极其重要的意义.为表述事物复杂程度,研究者们一直在寻找有效的方法.到目前为止,复杂度的定义有多种,大多以 Kolmogorov 提出的测度熵为基础[7].ApEn、PermutEn、SymEn 等方法的计算结果依赖于选取的混沌序列,选取序列长度也会对结果产生大的影响[8~11].以上方法计算复杂度之前,需将混沌序列进行符号化和粗粒化处理,方法选取带有经验性,会影响混沌序列复杂

收稿日期:2015-01-08;修回日期:2015-05-19;责任编辑:马兰英
基金项目:国家自然科学基金(No.61272494,No.61350011)

度的精度与稳定性.文献[12]提出的模糊熵计算方法需要引入参数对序列进行相空间重构,参数的选取带有经验性质,计算结果不具有普适性.

结构复杂度分析方法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度.变换域内各频谱中能量谱分布越均衡,复杂度越大[13].变换域内频率与能量特性具有全局统计特性,因此结构复杂度分析方法具有全局性.目前,利用结构复杂度分析混沌序列的研究尚不多.孙克辉等人[14]提出小波熵与谱熵等测试方法,首先对混沌序列进行傅立叶变换得出序列的功率分布情况,然后结合信息熵计算出功率谱熵.该类方法的谱熵计算受到采样混沌序列长度的影响而不稳定,同时采用傅立叶变换获取功率谱的方法不适用于平稳信号.文献[15]中小波熵分析法首先对序列进行小波变换重构,然后对各重构分支进行傅立叶变换获得功率谱熵,最后利用功率谱熵进行小波熵的计算.该方法的实质还是利用功率谱分析混沌序列复杂度,同样不适用于平稳信号复杂度分析.并且,小波变换基础上得到的功率谱熵方法无法有效区分长周期与混沌序列.

小波包分解是对小波分析的进一步扩展与改善,小波包可对小波分析不能细分的高频部分进行更精细的划分,且能对分析信号自适应选择相应频带,提高时频分辨率,有效显示信号的时频特征,弥补小波分析在特征提取方面的不足.由于小波包分析同时适用于平稳信号与非平稳信号,已经被广泛应用于人体生物信号分析、机器故障诊断和语言分析等领域[16,17].本文采取小波包能量熵分析混沌系统复杂度,直接利用序列小波包变换后的系数来评估能量谱,从全局来评估其产生的混沌序列的复杂度,为混沌密码学选取安全的混沌系统提供理论基础.

2 离散混沌映射

(1)Logistic 系统

该系统是最简单的一维混沌系统,其序列产生如式(1)所示.其中 x_{n+1}为 x_n,后一个序列值为前驱的序列值的迭代结果,Logistic 具有较好的初值敏感性.

$$x_{n+1}=\mu x_n(1-x_n)\ n=1,2,3,\cdots \tag{1}$$

其中 $\mu\in(0,4]$,$x_n\in(0,1)$,当 $\mu\in(3.5699456,4]$时,系统处于混沌状态.

(2)Henon 系统

Henon 系统于 1976 年由 Henon 提出,是高维映射中最简单的非线性映射[18].当参数 a、b 改变时,该系统可演变为 Logistic 系统.

$$\begin{cases}x_{n+1}=1-ax_n^2+y_n\\ y_{n+1}=bx_n\end{cases},\ n=1,2,3,\cdots \tag{2}$$

当 $a\in[1.07,1.4]$且 $b=0.3$ 时,系统处于混沌状态.

(3)TD-ERCS 系统

2004 年,盛利元等人[19]提出基于切延迟的椭圆反射腔离散混沌系统(Tangent Delay-Eclipse Reflecting Cavity Map System)-TD-ERCS 系统.该系统混沌特性明显且具有很好的计算性能,因此被许多文献用做研究对象.

$$\begin{cases}x_n=-\dfrac{2k_{n-1}y_{n-1}+x_{n-1}(\mu^2-k_{n-1}^2)}{\mu^2+k_{n-1}^2}\\ k_n=-\dfrac{2k'_n-k_{n-1}+k_{n-1}k'^2_{n-1}}{1+2k_nk'_n-k'^2_n}\\ k'_{n-m}=-\dfrac{x_{n-m}}{y_{n-m}}\mu^2\\ y_n=k_{n-1}(x_n-x_{n-1})+y_{n-1}\end{cases},\ \begin{matrix}n=1,2,3,\cdots\\ m\leqslant n\end{matrix} \tag{3}$$

其中系统参数 $\mu\in(0,1]$,变量 $|x_n|\leqslant 1$,$|y_n|\leqslant 1$,m 为整数,代表切延迟大小,k_n 表示反射线斜率,k'_{n-m}为延迟后椭圆切线斜率.k_0 可由入射角 α 确定:

由系统初始值 x_0 及参数 μ 计算出及斜率 k'_0:

$$y_0=\mu\sqrt{1-x_0^2} \tag{4}$$

$$k'_0=-\frac{x_0}{y_0}\mu^2 \tag{5}$$

利用三角函数关系,求得

$$k_0=\frac{\tan\alpha+k'_0}{1-k'_0\tan\alpha} \tag{6}$$

当四元组(μ,x_0,α,m)确定后,TD-ERCS 系统特性确定.其中 $\mu\in(0,1]$,$x_0\in[-1,1]$,$\alpha\in(0,\pi)$,$m=0,1,2,3,\cdots$.x_0 与 α 构成初始值,μ 与 m 构成控制参数空间.当 $m=0$ 时,系统处于周期状态;$m\geqslant 1$ 时,系统处于混沌状态;$m\geqslant 2$ 时,系统达到混乱状态,其产生的混沌序列类随机性最强.

3 谱熵与小波包能量熵

3.1 谱熵

谱熵(Spectral Entropy,SE)是基于傅里叶变换的结构复杂度分析法,结合香农信息熵定义可对混沌序列进行复杂度定量分析.谱熵的计算方法描述如下[14]:

(1)去直流.对长度为 N 的混沌伪随机序列$\{x_n\}$去掉直流部分,公式如下:

$$\begin{cases}\bar{x}=\dfrac{1}{N}\sum\limits_{n=0}^{N-1}x_n\\ x_n=x_n-\bar{x}\end{cases} \tag{7}$$

(2)对序列$\{x_n\}$离散傅立叶变换得系数序列:

$$X(k)=\sum_{n=0}^{N-1}x_n e^{-j\frac{2\pi}{N}nk} \tag{8}$$

其中 $X(k)$为傅立叶变换后得到的傅立叶系数,$k=0,1,2,\cdots,N-1$.

(3)取$\{X(k)\}$中前 $N/2$ 点计算每个频率点功率谱 $p(k)$与序列总功率 p_{tot},公式如下:

$$p(k)=\frac{1}{N}|X(k)|^2 \tag{9}$$

$$p_{tot}=\frac{1}{N}\sum_{k=0}^{\frac{N}{2}-1}|X(k)|^2 \tag{10}$$

(4)计算序列相对功率谱概率 P_k,公式如下:

$$P_k=\frac{p(k)}{p_{tot}} \tag{11}$$

(5)按照下式计算序列谱熵.

$$se=-\sum_{k=1}^{N/2}P_k\ln P_k \tag{12}$$

(6)将 se 归一化后得 SE.

$$SE=\frac{se}{\ln(\frac{N}{2})} \tag{13}$$

3.2 小波包熵

(1)小波包分解

混沌序列小波包分解的实质是将混沌信号通过高低通组合滤波器组,将原始混沌信号进行不断细分,直到满足一定精确程度.给定正交小波函数 $\varphi(t)$、尺度函数 $\phi(t)$,其关系满足双尺度方程:

$$\phi(t)=\sqrt{2}\sum_{k\in z}h_{0k}\phi(2t-k) \tag{14}$$

$$\varphi(t)=\sqrt{2}\sum_{k\in z}h_{1k}\varphi(2t-k) \tag{15}$$

其中 h_{0k}和h_{1k}为多分辨分析中的滤波器系数.

将二尺度方程进行推广,有如下递推关系:

$$w_{2n}(t)=\sqrt{2}\sum_{k\in z}h_{0k}w_{2n}(2t-k) \tag{16}$$

$$w_{2n+1}(t)=\sqrt{2}\sum_{k\in z}h_{1k}w_{2n}(2t-k) \tag{17}$$

其中 h_{0k}和h_{1k}为多分辨分析中的滤波器系数.当 $n=0$ 时,$w_0(t)=\phi(t)$,$w_1(t)=\varphi(t)$.函数集合$\{w_n(t)\}_{n\in z}$为由 $w_0(t)=\phi(t)$确定的小波包,该小波包含有尺度函数 $w_0(t)$和小波母函数 $w_1(t)$在内的具有联系的函数集合.

(2)小波包能量熵计算

小波包变换是一种线性变换,满足能量守恒定律.小波包系数具有能量量纲,可用于能量分析.因而根据信号的小波包系数确定各频段能量大小,结合香农熵定理,通过对混沌序列进行小波包变换,可得出每个频段的小波包能量熵.小波包能量熵越大,表示频域内能量分布越均匀,被分析的混沌序列复杂度越大,类随机性能越强.计算小波包能量熵算法如算法 1 所示.

实验过程表明混沌序列进行 3 层小波包分解后,其结果与大于 3 层的分解结果一致,而少于 3 层时,分解不够完全,变换域特征不够明显.因此本文选取小波包分解树第 3 层的所有小波包,$T=8$.

算法 1　混沌序列小波包能量熵计算

(1)初始化

　For 每个混沌系统 do

　　设置初始化参数和序列长度 N

　End for

(2)生成混沌序列

　For 每个混沌系统 do

　　生成长度为 N 的混沌序列$\{x(n),n=1,2\cdots,N\}$

　End for

(3)设置混沌序列小波包分解层数 $L=3$

(4)对$\{x(n),n=1,2\cdots,N\}$进行 3 层小波包分解,得到分解序列 $s_{i,j}$

(5)For 每个 $s_{i,j}$ do

　取 $s_{i,j}y_{i,j}(k)$做为输入源,计算每个频带能量

$$E_{i,j}=\int|s_{i,j}|^2\mathrm{d}t=\sum_{k=0}^{M-1}|y_{i,j}(k)|^2$$

　End for

(6)For 每个 $E_{i,j}$ do

　　计算每个频带的相对能量

$$e_{i,j}=\frac{E_{i,j}}{\sum_{j=0}^{2^i-1}E_{i,j}}$$

　End for

(7)计算小波包能量熵

$$we=-\sum_{k=0}^{2^j-1}e_{i,j}\ln e_{i,j}$$

(8)计算小波包个数 $T=2^L$

(9)对小波包能量熵进行归一化处理

$$WE=\frac{we}{\ln T}$$

(10)输出结果.

4 实验结果分析

4.1 三类混沌映射序列复杂度对比

Logistic 映射中 $\mu=4$, $x_0=0.3$; Henon 中 $a=1.2$, $b=0.3$, $x_0=0.1$, $y_0=0.1$; TD-ERCS 中 $\mu=0.8$, $x_0=0.5$, $\alpha=2$, $m=1$,分别取三个混沌序列迭代 2000 次中的后

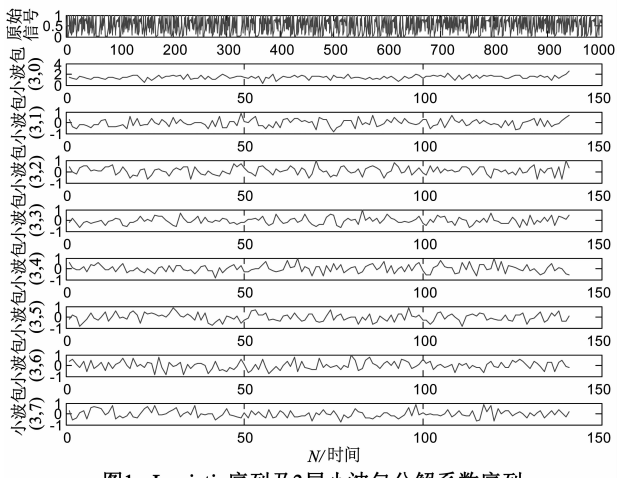


图1　Logistic序列及3层小波包分解系数序列

1000 个数据点用于实验.三类混沌序列及其小波包分解系数序列如图 1、图 2 和图 3 所示.

计算各序列的小波包能量熵,结果如表 1 所示.表中第一行数字表示各类序列小波包分解后第 3 层中的小波包次序,1 表示为混沌系统小波包分解树中第 3 层小波包中的(3,0)小波包,2 为小波包(3,1),以此类推.*WE* 为小波包能量熵,*SE* 为谱熵.从结果可知各混沌系统产生序列复杂度由强到弱依次为:Logisitc、TD-ERCS、Henon,其谱熵分别为:0.9533,0.9365,0.5960,小波包熵与谱熵趋势基本相同.从图 1、图 2、图 3 和表 1 结果来看 Logisitc 在各个频段的能量分布相比其他两类系统更均匀,因而复杂度更高.TD-ERCS 产生序列与 Logisitc 序列非常接近.

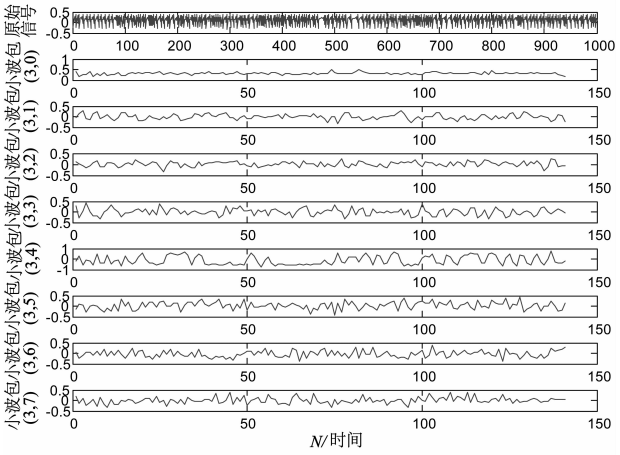


图2 Henon的y序列及3层小波包分解系数序列

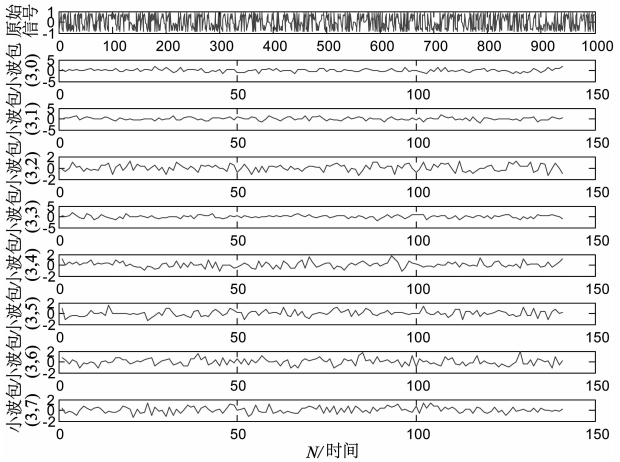


图3 TD-ERCS的x序列及3层小波包分解系数序列

表 1 三类序列小波包能量熵及谱熵

离散混沌系统	1	2	3	4	5	6	7	8	*WE*	*SE*
Logisitc	0.1175	0.1177	0.1281	0.1066	0.1288	0.1335	0.1454	0.1223	0.9987	0.9533
Henon	0.0083	0.0461	0.0364	0.0840	0.5812	0.0955	0.0798	0.0687	0.6905	0.5960
TD-ERCS	0.1476	0.1530	0.1358	0.1026	0.1053	0.1095	0.1236	0.1226	0.9882	0.9365

4.2 初值变化对小波包能量熵的影响

为分析混沌初始值对混沌序列复杂度计算结果的影响,分别对三种混沌系统谱熵、小波包能量熵受初值变化的影响进行仿真实验,实验结果如图 4 ~ 图 6 所示.

从图 4 中可以看出,正常情况下($\mu x_0 = 1$ 与 $\mu x_0 = \mu - 1$ 都不成立的条件下),x_0 变化时 Logistic 小波包能量熵在(0.9943,0.9987)之间浮动,其变化幅度在 5‰以内,表明 Logistic 系统复杂度高,受初始值影响的程度非常小.谱熵受初值变化的影响较大,在(0.9342,0.9581)之间起伏,变化幅度超过 20‰.小波包能量熵的稳定性能优于谱熵.

从图 5 中可以看出,在初始值变化时 Henon 小波包熵与谱熵都受到明显影响,说明该系统产生混沌序列的受初始值影响大,稳定性较差.与 Logistic 相比,Henon 产生的离散混沌序列复杂度与随机性能差.小波包能量熵相比谱熵,测度值波动幅度较小.

从图 6 中可知,D-ERCS 小波包熵在(0.9920,0.9969)之间波动,幅度在 5‰以内.谱熵波动范围为(0.9302,0.9413),幅度超过 11‰.

综合图 4、图 5 和图 6 可知,小波包熵受初值影响较小,Logisitc 与 TD-ERCS 的稳定性好,Henon 稳定性差.复杂度较低的混沌系统,受初值影响大于复杂度高的混沌系统.在选取混沌系统应用于信息安全时,尽量选用复杂度高的混沌系统.而 Logisitc 的稳定性能最好,小

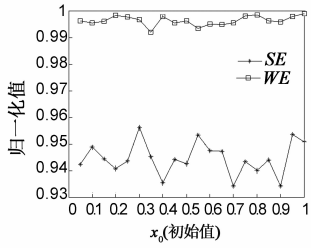


图4 Logistic谱熵、小波包熵受x_0变化的影响
(μ=3.999,N=2000)

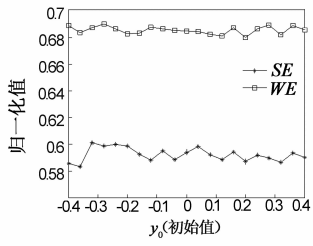


图5 Henon谱熵、小波包熵受y_0变化的影响
(a=1.2,b=0.3,x_0=0.1,N=2000)

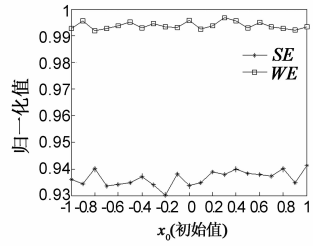


图6 TD-ERCS谱熵、小波包熵受x_0变化的影响
(μ=0.8,a=2,m=1,N=2000)

波包熵最大浮动范围在 5‰以内,迭代计算简单,产生的序列复杂度大而稳定,其应用前景优于其他两类混沌映射.三种混沌系统的小波包熵总体波动幅度远小于各自谱熵,尤其在复杂度特性不强的混沌系统测量中,谱熵的波动幅度大大超过小波包熵.因此,小波包熵对初始值变化的鲁棒性强于谱熵.

图 7 给出了参数 μ 变化时,Logisitc 小波包熵在特殊情况下受初值的影响.研究表明 $\mu x_0 = 1$ 或 $\mu x_0 = \mu - 1$ 时,Logistic 陷入不定点[20].$\mu = 4$ 时,Logistic 分别取 $x_0 = 0.25$ 与 $x_0 = 0.75$ 时,分别满足不定点条件.由于有限精度效应,Logistic 映射迭代值超出浮点数表示的最小值,因此图 7 中无法标示.小波包熵成功预测出 Logistic 不定点,验证小波包熵对序列复杂度分析的有效性.谱熵在上述特殊情况下,依然波动平缓.

4.3　序列选取长度变化对小波包能量熵的影响

混沌序列长度对小波包能量熵和谱熵的影响实验结果如表 2 和表 3 所示.

表 2 中 N 代表所取序列的长度.各系统中其他有关参数:Logistic 系统中 $\mu = 4$, $x_0 = 0.3$;Henon 中 $a = 1.2$, $b = 0.3$, $x_0 = 0.1$, $y_0 = 0.1$;TD-ERCS 中 $x_0 = 0.5$, $m = 1$, $\mu = 0.8$, $\alpha = 2$.混沌系统历经各态,局部特征与全局特性具有无限相似性,理论上在去掉初始迭代的一段序列后,长度对小波包熵影响很小.从 $N = 5000$ 开始,各序列的小波包熵趋向稳定,波动幅度在 10‰以内,验证了混沌系统分数维特征.

表 3 表明序列长度超过 5000 时,在计算机有限精度的限制下谱熵无法对序列进行复杂度计算.因此,在计算资源有限情况下,谱熵算法受限于序列长度.

表 2　各类混沌小波包熵受选取长度的影响

离散混沌系统	*WE*					
	$N = 3000$	$N = 4000$	$N = 5000$	$N = 6000$	$N = 7000$	$N = 8000$
Logistic	0.9980	0.9995	0.9997	0.9996	0.9998	0.9997
Henon	0.6681	0.6667	0.6658	0.6694	0.6684	0.6631
TD-ERCS	0.9913	0.9920	0.9938	0.9947	0.9943	0.9937

表 3　各类混沌谱熵受选取长度的影响

离散混沌系统	*SE*					
	$N = 3000$	$N = 4000$	$N = 5000$	$N = 6000$	$N = 7000$	$N = 8000$
Logistic	0.9469	0.9498	0.9508	内存不足	内存不足	内存不足
Henon	0.5907	0.5940	0.5940	内存不足	内存不足	内存不足
TD-ERCS	0.9407	0.9411	0.9446	内存不足	内存不足	内存不足

4.4　控制参数变化对混沌系统的影响

混沌系统控制参数对混沌系统的影响实验结果如图 8 ~ 图 11 所示.

从图 8 中得出,在区间(3,4)中存在不稳定的伪混沌序列,参数对 Logistic 特性起到决定作用.当 $\mu \in (3.82,3.85)$时,存在无数稳定周期点,因此其小波包熵突然降低.但谱熵在此区间波动较为平缓,不能准确测量出 Logistic 的特征变化.当 Logistic 应用于信息安全时,为提高基于 Logistic 安全方案的性能,应避免选取上述区间的数值作为关键参数.

从图 9 中得出,Henon 系统中当参数 $a > 1.32$ 后,其小波包熵波动较小,趋于稳定.相比其他两类混沌系统,Henon 系统小波包熵受参数影响不如其他两类混沌敏感,谱熵波动趋势与小波包熵基本一致.由于归一化范围影响,谱熵在一定值域范围内波动幅度大.

从图 10 中可知:小波包熵与谱熵受 μ 的影响一致.小波包熵曲线变化平滑,谱熵在(0.2,0.9)范围内处于同一水平,对控制参数的变化不如小波包熵敏感.小波包熵对参数值变化的敏感度证明该方法的有效性与可靠性,参考价值大于谱熵.

图 10 与图 11 表明:TD-ERCS 序列复杂度受 μ 的影响程度明显高于受 m 变化带来的影响.在选用 TD-ERCS 时,应特别关注 μ,选取接近 1 的数值效果比较好.当 m 变化时,小波包熵受影响程度在 1% 以内,能

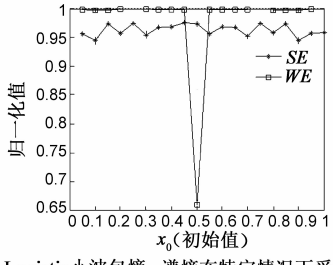


图7　Logistic小波包熵、谱熵在特定情况下受x_0变化的影响（μ=4，N=2000）

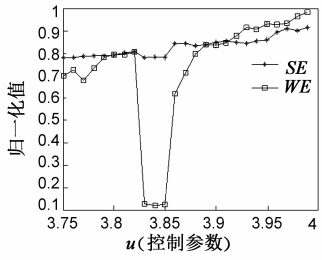


图8　Logistic受μ变化的影响（x_0=0.3,N=5000）

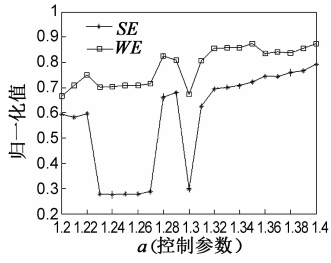


图9　Henon受a变化的影响（y_0=0.1,x_0=0.1,b=0.3,N=5000）

有效区分序列复杂度.

小波包熵对三类混沌系统的参数变化非常敏感,波动幅度明显,符合混沌系统由参数决定其局部与全局混沌特性的原理.

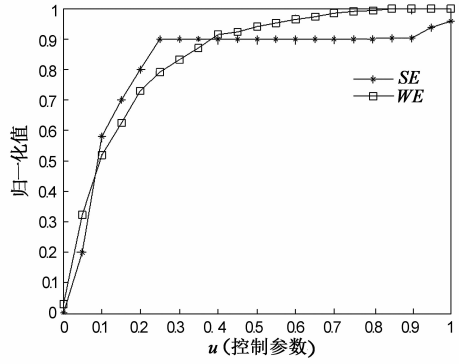


图10 TD-ERCS小波包熵受μ变化的影响
(x_0=0.5,a=2,m=1,N=5000)

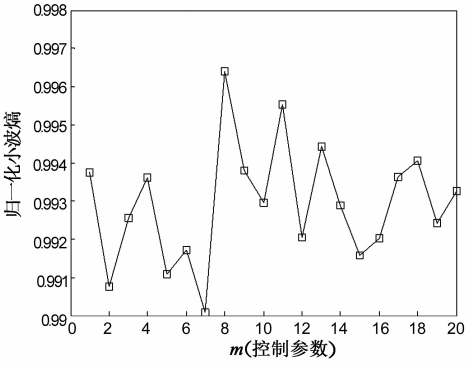


图11 TD-ERCS小波包熵受 m变化的影响
(x_0=0.5,a=2,μ=0.8,N=5000)

4.5 谱熵与小波包熵计算时间对比

复杂度计算时间指在获取序列的前提下,对混沌序序列进行熵的计算所需要的时间.谱熵计算时间主要由如下及部分组成:傅立叶变换、计算相对功率、求谱熵及归一化.小波包熵计算时间主要由如下部分组成:小波包分解、各小波包频段能量计算、小波包能量熵计算及其归一化.对图 4、图 5 与图 6 获取数据点所需时间进行两种熵的计算对比分析,具体数值如表 4 所示,时间单位为秒.

表 4 小波包熵与谱熵运算时间对比(时间单位:秒)

离散混沌系统	*WE*			*SE*		
	图 4	图 5	图 6	图 4	图 5	图 6
Logistic	0.405	0.401	0.410	73.936	73.857	72.997
Henon	0.453	0.458	0.461	75.669	74.348	75.663
TD-ERCS	0.478	0.483	0.481	81.772	83.857	85.937

从表 4 可知:谱熵计算效率远远低于小波包熵,在特殊环境下如移动终端设备中进行混沌系统选取时,计算资源珍贵,效率是一个关键的指标.因此,选用小波包熵进行混沌序列复杂度计算具有高效、快速优势.

5 结论

由于混沌系统的天然特性,在密码学中具有很好应用前景,混沌序列复杂度是衡量混沌加密性能的重要参考.本文采用小波包能量熵对混沌序列复杂度进行分析,实验结果证明小波包能量熵在分析复杂度时具有优势:(1)小波包能量熵基于能量分布衡量信号系统复杂度,不论信号是否平稳,都可很好地区分长周期与混沌系统;(2)无需进行符号化或相空间重构,不依赖被测试混沌序列长度、初始值及参数,效率较高;(3)从全局衡量混沌序列的复杂性,确保选取的混沌系统产生的序列具有很好的随机性.下一步将重点研究小波包能量熵在混沌密码分析预测模型中的应用,为混沌密码学提供安全分析基础.

参考文献

[1] Kocarev L. Chaos-based cryptography: A brief overview[J]. IEEE Circuits and Systems Magazine, 2001, 1(3): 6 – 21.

[2] 文昌辞,王沁,刘向宏,等.基于仿射和复合混沌的图像加密新算法[J].计算机研究与发展,2013,50(2):319 – 324.
Wen Chang-ci, Wang Qin, Liu Xiang-hong, et al. An encryption algorithm for image based on affine and composed chaos [J]. Journal of Computer Research and Development, 2013, 50(2): 319 – 324. (in Chinese)

[3] Zhang Y S, Xiao Di, Shu Yong-lu, et al. A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations [J]. Signal Processing: Image Communication, 2013, 28(3): 292 – 300.

[4] 邓晓衡,廖春龙,朱从旭,等.像素位置与比特双重置乱的图像混沌加密算法[J].通信学报,2014,35(3):216 – 223.
Deng Xiao-heng, Liao Chun-long, Zhu Cong-xu, et al. Image encryption algorithms based on chaos through dual scrambling of pixel position and bit[J]. Journal of Communications, 2014, 35(3): 216 – 223. (in Chinese)

[5] Lempel A, Ziv J. On the complexity of finite sequences[J]. IEEE Transactions on Information Theory, 1976, 22(1): 75 – 81.

[6] 孙克辉,贺少波,朱从旭,等.基于 C_0 算法的混沌系统复杂度特性分析[J].电子学报,2013,41(9):1765 – 1771.
Sun Ke-hui, He Shao-bo, Zhu Cong-xu, et al. Analysis of chaotic complexity characteristics based on C_0 algorithm[J]. Acta Electronica Sinica, 2013, 41(9): 1765 – 1771. (in Chinese)

[7] Kolmogorov A N. Three approaches to the definition of information[J]. International Journal of Computer Mathematics, 1968, 2(2): 157 – 168.

[8] Pincus S M. Approximate entropy as a measure of system com-

plexity[A]. Proceedings of the National Academy of Science [C]. USA. 1991,88:2297 – 2301.

[9] Band C, Pompe B. Permutation entropy: a natural complexity measure for time series[J]. Physical Review Letters, 2002, 88 (17):174102-1-174102-4.

[10] Politi A. Estimating generalized entropies from symbol sequences[J]. Physics Letters A, 1989, 136(7 – 8):374 – 378.

[11] 罗松江,丘水生,陈旭.一种混沌伪随机序列复杂度分析方法.华南理工大学学报(自然科学版),2010,38(1):18 – 21.
Luo Song-jiang, Qiu Shui-sheng, Chen Xu. A way to complexity analysis of chaotic pseudorandom sequence[J]. Journal of South China University of Technology (Natural Science Edition), 2010, 38(1):18 – 21. (in Chinese)

[12] Ullah A. Entropy, divergenceand distance measures with econometric applications[J]. Journal of Statistical Planning and Inference, 1996, 49(1):137 – 162.

[13] Inouy T, Shinosaki K, Sakanoto H. Quantification of EEG Irregularity by Use of the entropy of the Power Spectrum[J]. Electroencephalography and Clinical Neuophysial, 1991, 79 (3):204 – 210.

[14] 孙克辉,贺少波,何毅,等.混沌伪随机序列的谱熵复杂性分析[J].物理学报,2013,62(1):010501-1-010501-8.
Sun Ke-hui, He Shao-bo, He Yi. Complexity analysis of chaotic pseudo-random sequences based on spectral entropy algorithm[J]. Acta Physica Sinica, 2013, 62(1):010501-1-010501-8. (in Chinese)

[15] 董燕青,谈国强,孙克辉,等.谱熵和小波熵算法在混沌序列结构复杂性分析中的应用[J].小型微型计算机系统,2014,35(2):348 – 352.
Dong Yan-qing, Tan Guo-qiang, Sun Ke-hui, et al. Applications of spectral entropy and wavelet entropy algorithm for structure complexity analysis of chaotic sequence[J]. Journal of Chinese Computer Systems, 2014, 35(2):348 – 352. (in Chinese)

[16] Biswas A, Sahu P K, Chandra M. Admissible wavelet packet features based on human inner ear frequency response for Hindi consonant recognition[J]. Computers& Electrical Engineering, 2014, 40(4):1111 – 1122.

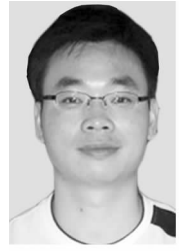
[17] Keskes H, Braham A, Zied L. Broken rotor bar diagnosis in induction machines through stationary wavelet packet transform and multiclass wavelet SVM[J]. Electric Power Systems Research, 2013, 97(2):151 – 157.

[18] Henon M. A two-dimensional mapping with a strange attractor [J]. Communications in Mathematical Physics, 1976, 50(1): 69 – 77.

[19] 盛利元,孙克辉,李传兵.基于切延迟的椭圆反射腔离散混沌系统及其性能研究[J].物理学报,2004,53(9):2871 – 2876.
Sheng Li-yuan, Sun Ke-hui, Li Chuan-bin. Study of a discrete chaotic system based on tangent delay for elliptic reflecting cavity and its properties[J]. Acta Physica Sinica, 2004, 53 (9):2871 – 2876. (in Chinese)

[20] 郑德玲,赵耿,徐国保. Logistic 映射数字流混沌奇怪吸引子及参数[J].北京科技大学学报,2002,24(3):350 – 352.
Zheng De-ling, Zhao Geng, Xu Guo-bao. Logistic mapping digital-flow chaos strange attractor and its parameter analysis [J]. Journal of University of Science and Technology Beijing, 2002, 24(3):350 – 352. (in Chinese)

作者简介



梁涤青　男,1979 年 9 月生,湖南涟源人.中南大学信息科学与工程学院博士研究生,从事混沌理论与信息安全等方面的研究.
E-mail:billldq@163.com

陈志刚　男,1964 年 5 月生,湖南益阳人.中南大学软件学院教授、博士生导师,从事分布式计算与信息安全等方面的研究.

邓小鸿　男,1982 年 2 月生,湖北天门人.2013 年获中南大学博士学位,现为江西理工大学应用科学学院副教授,从事数字水印与信息安全等方面的研究.