

基于切延迟的椭圆反射腔离散混沌系统及其性能研究^{*}

盛利元 孙克辉 李传兵

(中南大学物理科学与技术学院, 长沙 410083)

(2003 年 11 月 21 日收到, 2003 年 12 月 30 日收到修改稿)

根据椭圆反射腔物理模型, 提出了一种改变系统演化轨道的切延迟操作方法, 导出了基于该方法的一类离散混沌映射系统. 实验表明, 这类离散混沌系统最大 Lyapunov 指数恒大于零, 状态变量等概率分布且与参数和初值无关, 全域零相关性. 切延迟 1 单位时存在一个稳定不变的方形吸引子, 切延迟大于 1 单位时走向各态遍历. 这类离散混沌系统可以产生两个独立的伪随机序列, 其特殊性质和复杂的动力学行为极具密码学应用价值.

关键词: 混沌, 切延迟, Lyapunov 指数, TD-ERCS, 吸引子

PACC: 0545

1. 引言

十多年来, 混沌理论用于信息加密成为研究热点^[1-8]. 信息加密对混沌系统有特殊的要求. 首先混沌系统应是满映射的. 若是一条连续的相轨线, 相点的任意小邻域都会隐含系统的演化趋势, 将降低算法的安全性. 第二是系统应具有全域混沌特性. 即混沌系统在参数值域和初始值域内都是混沌的, 以降低密码系统的弱密钥率. 第三是系统具有全域零相关性, 以抵抗密码相关性分析. 第四是系统具有巨大的参数和初值空间, 以抵抗穷举密钥攻击. 找到一个理想的混沌系统是混沌系统能够成功用于加密技术的关键. 目前所研究的一些典型混沌系统^[2-8], 并不完全具有这些理想特性, 所以至今还没有成功应用的实例. 但无论如何, 混沌系统以其对初始条件的敏感性和内秉随机性, 喻示着在信息技术领域将有良好的应用前景.

作者试图寻找一种理想的混沌映射系统. 本文通过建立一个椭圆反射腔物理模型, 提出了一种切延迟操作方法, 基于该方法导出了一类新的离散混沌映射系统, 称为切延迟椭圆反射腔混沌映射系统. 初步研究表明, 该类离散混沌系统当切延迟 1 个单位时存在一个方形吸引子, 切延迟大于 1 个单位时呈现各态遍历性, 状态变量等概率分布且与参数和

初值无关, 全域混沌性和全域零相关性. 这是一类新的混沌系统, 可用来产生两个独立的伪随机数序列, 其特殊性质和复杂的动力学行为极具密码学应用价值. 本文定义模型和切延迟操作, 并给出映射关系; 给出主要实验结果和有限度的讨论.

2. 切延迟椭圆反射腔模型

2.1. 椭圆反射腔映射系统

2.1.1. 物理模型

设归一化标准椭圆

$$x^2 + \frac{y^2}{\mu^2} = 1, \quad (1)$$

其中 μ 为椭圆压缩因子. 如图 1 所示, 一射线 l_0 从椭圆的初始位置 $M_0(x_0, y_0)$ 射入, 相对于 M_0 点的切线夹角为 α ($0 < \alpha < \pi$), 入射到椭圆上 $M_1(x_1, y_1)$ 点, 经 $M_1(x_1, y_1)$ 反射成 l_1 , l_1 入射到 $M_2(x_2, y_2)$, 经反射成 l_2 , 如此继续, 系统演化得到一个点序列

$$M = \{M_i(x_i, y_i) | i = 0, 1, 2, \dots\} \quad (2)$$

和一个射线序列

$$L = \{l_i | i = 0, 1, 2, \dots\}. \quad (3)$$

定义 1 称 (1) 式及其点序列 (2) 和射线序列 (3) 所组成的系统为椭圆反射腔映射系统 (ellipse

^{*} 湖南省自然科学基金 (批准号 01JJY2110) 资助的课题.

reflecting cavity map system (ERCS).

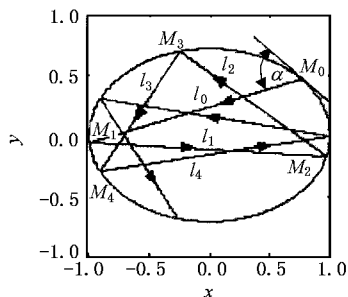


图 1 ERCS 物理模型 ($\mu = 0.7123$, $x_0 = 0.7654$, $\alpha = 0.9876$)

2.1.2. ERCS 的系统状态

显然, 点序列 (2) 由两个实数集

$$X = \{x_i \mid i = 0, 1, 2, \dots\}, \quad (4)$$

$$Y = \{y_i \mid i = 0, 1, 2, \dots\} \quad (5)$$

组成, 但由于 (1) 式的约束, 仅一个是独立的, 不妨取 X . 引入点 $M_i(x_i, y_i)$ 处反射线 l_i 的斜率 k_i 序列

$$K = \{k_i \mid i = 0, 1, 2, \dots\} \\ -\infty < k_i < +\infty, \quad (6)$$

则可由 X 和 K 描述 ERCS 的状态.

定义 2 X 和 K 为 ERCS 的两个状态参量, 它们构成相空间 (X, K) .

实验中, 为了相空间 (X, K) 简化表示, 可取 l_i 与横轴的夹角 β_i 即 k_i 的反正切表示 k_i , 以及 x_i 的象限角 θ_i 表示 x_i . 其转换式为

$$\beta_i = \arctan k_i \quad \left(-\frac{\pi}{2} < \beta_i < \frac{\pi}{2}\right), \quad (7)$$

$$\theta_i = \arccos x_i \quad (0 \leq \theta_i \leq \pi). \quad (8)$$

另外, 在不会引起混淆的情况下, 可用 M_i 简单表示椭圆上的点 $M_i(x_i, y_i)$ 或相空间的 $M_i(x_i, k_i)$.

2.1.3. 映射关系

给定系统参数 μ 及初值 x_0 与 α , ERCS 系统将演化出序列 (2) 和序列 (3), 并形成一种映射关系.

定理 1 给定系统参数 μ 及初值 x_0 和 α , ERCS 的状态存在二维映射关系

$$x_n = -\frac{2k_{n-1}y_{n-1} + x_{n-1}(\mu^2 - k_{n-1}^2)}{\mu^2 + k_{n-1}^2}, \quad (9)$$

$$k_n = \frac{2k'_n - k_{n-1} + k_{n-1}k'_n}{1 + 2k_{n-1}k'_n - k_n'^2}, \quad (10)$$

$$n = 1, 2, 3, \dots$$

其中

$$k'_n = -\frac{x_n}{y_n}\mu^2, \quad (11)$$

$$y_n = k_{n-1}(x_n - x_{n-1}) + y_{n-1}, \quad (12)$$

k'_n 为 M_n 点处椭圆切线的斜率.

该定理可由 ERCS 的几何关系不难导出, 证明从略.

k_0 可由入射角 α 确定, 方法如下: 首先由 x_0 求得 y_0 , 然后求出 M_0 点切线斜率 k'_0 , 即

$$y_0 = \mu \sqrt{1 - x_0^2}, \quad (13)$$

$$k'_0 = -\frac{x_0}{y_0}\mu^2, \quad (14)$$

再利用三角函数关系, 得

$$k_0 = \frac{\tan \alpha + k'_0}{1 - k'_0 \tan \alpha}. \quad (15)$$

显然, μ 的所有可能取值构成了系统的参量空间, x_0 和 α 的所有可能取值构成了系统的初值空间.

2.2. 切延迟椭圆反射腔映射系统

为表述方便, 用 k'_n 表示 M_n 点的切线.

定义 3 在 ERCS 中, 如果将切线 k'_{n-m} 从 M_{n-m} ($m \in \mathbb{Z}, m \leq n$) 平移到 M_n 取代切线 k'_n , 那么这种切线平移的操作称为切延迟操作 (tangent-delay operation, TD).

这里 m 是平移的迭代步长. 如果一条切线从 M_{n-1} 移到了 M_n , 我们说它延迟了 1 单位, 如果从 M_{n-2} 移到 M_n , 就说延迟了 2 单位, 一般地, 若从 M_{n-m} 移到 M_n , 则说延迟了 m 单位. 当 $m \neq 0$ 时, TD 使得 (9) 式和 (10) 式的每一步迭代都要改变 ERCS 的演化轨道, 从而将改变 ERCS 的性质.

定义 4 经切延迟操作后的 ERCS 称为切延迟椭圆反射腔映射系统 (tangent-delay ellipse reflecting cavity map system, TD-ERCS).

若切延迟为 m , 则用

$$k'_{n-m} = -\frac{x_{n-m}}{y_{n-m}}\mu^2 \quad (m \leq n) \quad (16)$$

替换 (11) 式即可. $m = 0$ 时, TD-ERCS 就是 ERCS.

3. 实验与结果分析

主要以切延迟 $m = 1$ 为例, 分析 TD-ERCS 的混沌性质. 所有实验都是在 MATLAB6.5 上完成的.

3.1. 系统演化轨迹与演化进程仿真

图 2 给出了 TD-ERCS 分别在 $m = 0, m = 1$ 和 m

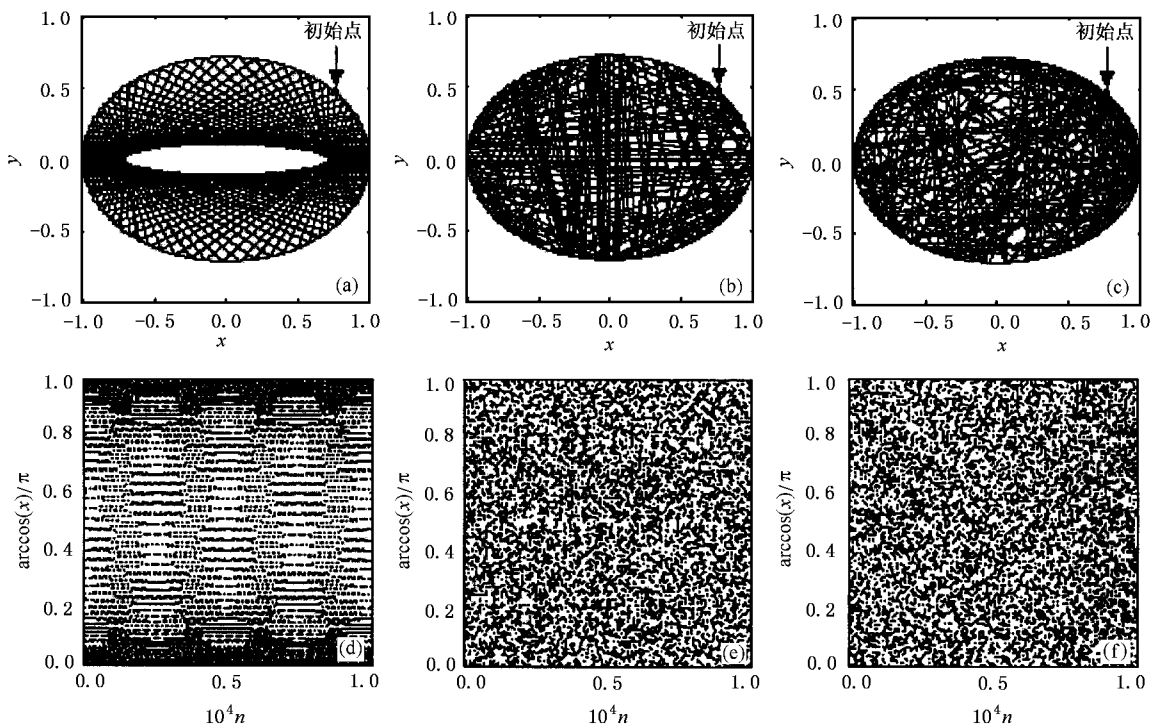


图2 TD-ERCS 的演化轨迹和演化进程,其中 $\mu = 0.7123$, $x_0 = 0.7654$, $\alpha = 0.9876$ 。(a)(b)(c)为不同切延迟下射线在椭圆反射腔内的演化轨迹(d)(e)(f)为对应的 x 随迭代次数 n 的演化进程((a)(d) $m = 0$ (b)(e) $m = 1$ (c)(f) $m = 2$)

$= 2$ 时射线的演化轨迹和 x 值的演化进程(系统的参数和初值相同,迭代 200 步后开始取值,其中演化轨迹图取 250 个值,演化进程图取 10000 个值)。显然, $m = 0$ 时,系统演化是周期性的,当 $m = 1$ 和 $m = 2$ 时,系统演化的周期性消失,且混乱程度随 m 值增加。仿真实验还表明,ERCS 不存在平庸的过渡过程,即系统从初始点开始就进入到它预期的演化周期轨道。

3.2. 相点的概率分布

3.2.1. x_i 的概率密度曲线

用 $\mu(x_i)$ 表示 TD-ERCS 中 x_i 的概率密度。

定理 2 如果 $\mu = 1$, $m \geq 1$ 则有

$$\mu(x_i) = \frac{1}{\pi \sqrt{1 - x_i^2}} \quad (-1 \leq x_i \leq 1). \tag{17}$$

证明 为了简洁,略去下标变量。当 $\mu = 1$ 时,TD-ERCS 成为 TD-CRCS(tangent-delay circle reflecting cavity map system)。在 $m \geq 1$ 条件下,假定 TD-CRCS 是混沌的,那么点 $M(x, y)$ 的出现是随机的。由于圆对称性,点 $M(x, y)$ 在圆弧上任意位置出现的概率应该是相等的。就是说,若让 p_s 表示圆弧上任意点出现的概率密度,则有

$$p_s = \frac{1}{2\pi}, \tag{18}$$

这里,圆的半径等于 1。

设 ds 为对应 dx 的一段圆弧,则由微分几何关系知

$$ds = \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx, \tag{19}$$

且 x 在 dx 内出现的概率等于点 $M(x, y)$ 在上下两段圆弧 ds 内出现的概率,即

$$\mu(x)dx = 2p_s ds. \tag{20}$$

将(19)式代入(20)式得

$$\mu(x)dx = 2p_s \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx. \tag{21}$$

消去 dx ,并将(1)式和(18)式代入,便可得到(17)式。

证毕。

该证明假设 x_i 为随机变量,正确与否应通过实验来检验。如果实验与(17)式吻合,则假设成立,将是 TD-ERCS 混沌性的一个有力证据。

x_i 的象限角 θ_i 同时也是圆上 M_i 的中心角,用 $\mu(\theta_i)$ 表示 θ_i 出现的概率,显然有如下推论。

推论 象限角 θ_i 具有等概率密度,即

$$p(\theta_i) = \frac{1}{2\pi} \quad i = 0, 1, 2, \dots \quad (22)$$

3.2.2. k_i 的概率密度曲线

可由 β_i 的概率密度 $p(\beta_i)$ 等价表示.

定理 3 如果 $\mu = 1, m \geq 1$ 则有

$$p(\beta_i) = \frac{1}{\pi}. \quad (23)$$

该定理同样可由圆对称性导出(证明略).

3.2.3. 实验结果

概率密度测试实验结果如图 3 所示. 实验中, 迭代 40 万次, 分成 200 个盒计数, x_i 和 k_i 的均方差分别为 0.2378% 和 0.2421%. 实验结果不仅与理论式 (17) (22) 和 (23) 完全吻合, 而且还展示了 TD-ERCS 的两个理论上应进一步解释的重要特性:

1) 虽然 (17) (22) 和 (23) 式是在参数 $\mu = 1$ 的条件下导出的理论曲线, 但在 $0.1 < \mu \leq 1$ 范围内, TD-ERCS 仍然保持着这种分布, 与初值无关; 在 $0.001 < \mu \leq 0.1$ 范围内, 实验曲线有变形; 当 $\mu < 0.001$ 后分布无规律. 这说明 TD-ERCS 状态参量的概率密度与参数 μ 和初值无关, 具有全域稳定的分布特性.

2) (17) 式与 Logistic 映射在满映射时的概率密度函数形式完全相同^[9], 是否暗示这两种混沌系统之间存在着某种联系? 实验表明, Logistic 映射的概率密度函数与系统参数有关.

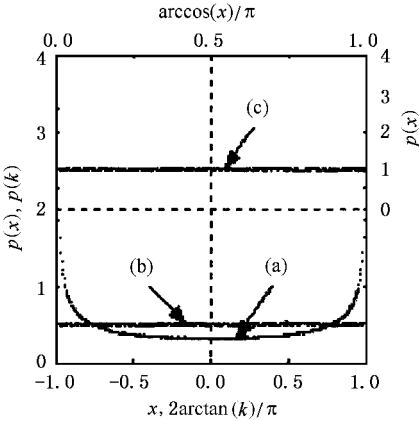


图 3 TD-ERCS 系统状态参量的概率密度, 其中, $\mu = 0.7123, x_0 = 0.7654, \alpha = 0.9876$. (a) 对应 (17) 式的 x 概率密度实验曲线; (b) 对应 (23) 式的 $\arctan(k)$ 概率密度实验曲线; (c) 对应 (22) 式的 $\arccos(x)$ 概率密度实验曲线

3.3. Lyapunov 指数

Lyapunov 指数大于零是系统处于混沌状态的充

分条件. 作者在系统参数 μ 的定义域内计算了 TD-ERCS 在 $m = 1$ 时的最大 Lyapunov 指数. 采用 Lyapunov 指数工程在线计算方法^[10, 11], 由下式可算出系统最大 Lyapunov 指数, 用 LE_1 表示, 即

$$LE_1 = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^n \ln \frac{d_i}{d_0}. \quad (24)$$

依据 (24) 式计算 LE_1 随系统参数 μ 变化的结果如图 4 所示. 曲线形态似飞翔的大雁, 故称之为大雁图. 其中 $n = 400000, d_0 = 10^{-8}, \mu = 1$ 处有最大值 $LE_1 = 0.91$ (也是极大值); $\mu = 0.5$ 处有极小值 $LE_1 = 0.33$; 由此可见, 在 μ 的定义域内 LE_1 均大于零, 表明 TD-ERCS 是全域混沌的.

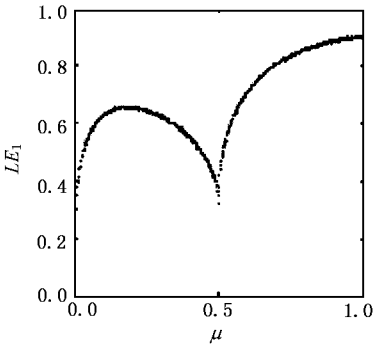


图 4 Lyapunov 指数大雁图 其中 $x_0 = 0.7654, \alpha = 0.9876$

3.4. 方形吸引子与各态遍历性

$m = 1$ 时, TD-ERCS 存在一个方形吸引子, 如图 5 所示. 迭代初期, 相点不在吸引子上, 随着迭代次数的增加, 相点最终将落在这个吸引子上. 实验还表明, 在 $0 < \mu < 1$ 的范围内, 方形吸引子的位置不变, 与初值无关. 方形吸引子给出了 θ 和 β 之间的简单线性关系. $\mu = 1$ 时, 吸引子位置与初值有关, 所有相点都在吸引子上.

吸引子存在这一事实表明, $m = 1$ 的 TD-ERPS 不具有各态遍历性, 相点的随机性最终只在一维上有意义.

$m = 2$ 时, 吸引子消失, 相点均匀地分列到整个相空间, 如图 6 所示. 由此我们观察到了随着切延迟单位数 m 的增加, TD-ERPS 从吸引子走向各态遍历, 它标志着系统混乱度的增加. 图 2 给出的演化轨迹和演化进程也能印证这一性质. $m = 2$ 时, 表明 θ 和 β 之间的约束被消除, 系统状态呈各态遍历性, 系

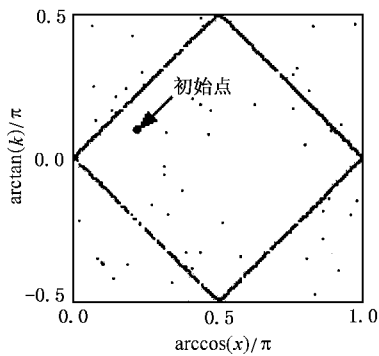


图5 $m = 1$ 时 TD-ERCS 的方形吸引子 其中 $\mu = 0.8123$, $x_0 = 0.7654$, $\alpha = 0.9876$, 取前 1500 个迭代点

统状态的随机性在整个相空间上都具有意义. 在数据加密技术中, 这样的系统可以构造两个独立的随机数字发生器.

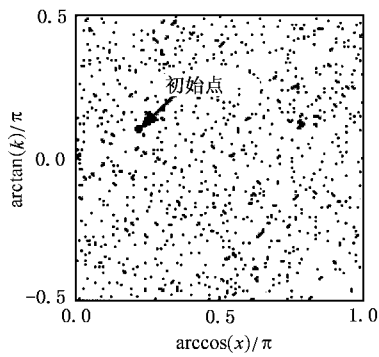


图6 $m = 2$ 时 TD-ERCS 的各态遍历性 其中 $\mu = 0.8123$, $x_0 = 0.7654$, $\alpha = 0.9876$, 取前 1500 个迭代点

3.5. 相关性分析

对初值的敏感性必然表现出两个初值非常相近的迭代演化序列之间的零相关性. 这里只讨论互相关系数. 我们计算了 TD-ERPS 和 Logistic 映射系统在系统参数 μ 的定义域内的互相关系数曲线, 由此可看出两者在相关性上的巨大差别. 计算结果如图 7 所示. 取两互相关演化序列的初始值差为 $d_0 = 10^{-16}$, 迭代 1280×20000 次求得的 1280 个相关系数作图. TD-ERPS 的相关系数在参数 μ 的定义域内均匀并接近零, 具有全域零相关性, 其平均值为

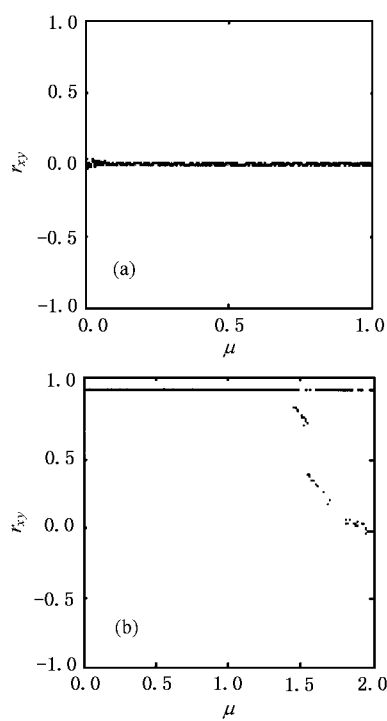


图7 互相关系数 (a) TD-ERCS , $x_0 = 0.7654$, $\alpha = 0.9876$ (b) Logistic 图 , $x_0 = 0.7654$

0.002372, 标准偏差为 0.000467, 相对标准偏差为 19.69%. Logistic 系统只在系统参数接近最大值时才具有零相关性.

因此, 如果将这两个系统用于数据加密, Logistic 系统可用的参数空间大约只有 TD-ERPS 的 1/1000.

4. 结 论

TD-ERCS 是一类全域性离散混沌系统, 全域性零相关系统, 具有稳定的概率分布, 当 $m = 1$ 时存在一个方形吸引子, 当 $m > 1$ 时系统是各态遍历的. 这些特性表明 TD-ERCS 极具密码学应用价值. 切延迟操作 TD 起了关键作用——每一步迭代都将改变 ERCS 的演化轨道, 使得非混沌的 ERCS 成为全域性混沌系统, 使得系统状态从吸引子走向各态遍历. 作者认为, TD 可能是通向混沌的一条新途径. 深入研究 TD 和 TD-ERCS 系统特性将会得到更多的有理论价值的发现.

- [1] Dachsel F and Schwarz W 2001 *IEEE Trans. CAS-I* **48** 1498
- [2] Luo W M *et al* 2000 *J. SCUT* **28**(10) 8 (in Chinese) [罗伟民等 2000 华南理工大学学报 **28**(10) 8]
- [3] Tao Y , Chua L O 1997 *IEEE Trans. CAS- I* **44** 976
- [4] Li S J *et al* 2003 *Phys. Lett. A* **307** 22
- [5] Palacios A and Juarez H 2002 *Phys. Lett. A* **303** 345
- [6] Chen G , Ueta T 1999 *Int. J. Bifurc. Chaos* **9**(7) 1465
- [7] Wong W K *et al* 2003 *Phys. Lett. A* **310** 67
- [8] Stojanoski T , Kovarev L 2001 *IEEE Trans. CAS-I* **48**(3) 281 , 382
- [9] Ulan S M and Von Neumann J 1947 *Bull. AMS* **53** 1120
- [10] Li Y T *et al* 1996 *Physics* **25** 282 (in Chinese) [李尧亭 等 1996 物理 **25** 282]
- [11] Lai J W *et al* 2000 *Acta Phys. Sin.* **49** 2328 (in Chinese) [赖建文 等 2000 物理学报 **49** 2328]

Study of a discrete chaotic system based on tangent-delay for elliptic reflecting cavity and its properties ^{*}

Sheng Li-Yuan Sun Ke-Hui Li Chuan-Bing

(School of Physics Science and Technology , Central South University , Changsha 410083 , China)

(Received 21 November 2003 ; revised manuscript received 30 December 2003)

Abstract

Based on the physical model of ellipse reflecting cavity , the tangent-delay operation is proposed to change the evolution route of the systems , and a new class of discrete chaotic map systems is deduced based on the tangent-delay operation. Simulation experiments show that the discrete chaotic systems have many special properties such as the maximum Lyapunov exponent is over zero , unchangeable equiprobability distribution and zero correlation in total field , there exists a square chaotic attractor when tangent delays one unit , and become ergodic state when tangent delays more units than one. The discrete chaotic systems can generate 2 independent pseudo-random sequences together. All of the properties suggest that the class of chaos systems possesses the potential application in encryption.

Keywords : chaos , tangent-delay , Lyapunov exponent , TD-ERCS , attractor

PACC : 0545

^{*} Project supported by the Natural Science Foundation of Hunan Province , China(Grant No.01JJY2110).