

广义二维多项式混沌映射及其在信息传输中的应用

闫文浩¹, 姜子敬¹, 黄欣¹, 朱淑娟², 丁群¹

(1.黑龙江大学工程学院, 黑龙江 哈尔滨 150080; 2.澳大利亚弗林德斯大学科学与工程学院, 通斯利 SA 5042)

摘要: 现有混沌映射在工程应用中存在许多缺陷, 如混沌参数范围不连续、弱混沌、混沌序列输出不均匀和动力学退化等。基于此, 提出了一种广义二维多项式混沌映射, 通过设定不同控制参数和多项式最高次数, 得到一系列特定 Lyapunov 指数的二维多项式混沌映射。为避免该映射第二个状态方程的输出塌陷为一个固定值, 引入了一个不随时间变化的随机扰动变量。然后, 通过具体的数值实验验证了该映射的有效性, 动力分析表明该映射具有复杂的动力学行为。最后, 将该映射应用于信息传输技术, 相较于其他混沌映射, 该映射可以取得更小的误码率, 表明该混沌映射更适用于混沌信息传输。

关键词: Lyapunov 指数; 动力学退化; 混沌映射; 信息传输

中图分类号: TN918

文献标志码: A

DOI: 10.11959/j.issn.1000-436x.2022168

Generalized 2D polynomial chaotic map and its application in information transmission

YAN Wenhao¹, JIANG Zijing¹, HUANG Xin¹, ZHU Shujuan², DING Qun¹

1.College of Electronic Engineering, Heilongjiang University, Harbin 150080, China

2.College of Science and Engineering, Flinders University, Tonsley SA 5042, Australia

Abstract: Existing chaotic systems have many defects in engineering applications, such as discontinuous chaotic parameter range, weak chaos, uneven output of chaotic sequences and dynamic degradation. Therefore, a generalized 2D polynomial chaotic mapping model was proposed. By setting different control parameters and the highest degree of polynomial, a series of 2D robust chaotic maps with specific Lyapunov exponent could be obtained. In order to avoid the output of the second state equation collapsing to a fixed value, a random disturbance variable which did not change with time was introduced. Finally, a numerical example was given to verify the effectiveness of the proposed model, and the dynamic analysis showed that the mapping has complex dynamic behavior. Finally, the system was applied to information transmission technology. Compared with other chaotic maps, the system can achieve lower bit error rate, which indicates that the chaotic map is more suitable for chaotic information transmission.

Keywords: Lyapunov exponent, dynamic degradation, chaotic map, secure communication

0 引言

非线性动力系统在许多研究领域都受到越来越多的关注^[1-2]。混沌映射是一种典型的非线性映射, 其具有初值敏感性、内禀随机性、遍历性、拓

扑传递性和正的 Lyapunov 指数等优良特性^[3-5]。这些特性使混沌映射更适用于密码学、信号处理、神经网络等领域^[6-9]。

现有混沌映射在工程应用中存在许多缺点。1) 由于经典混沌映射结构比较简单, 随着计算机计算

收稿日期: 2022-05-25; 修回日期: 2022-08-25

通信作者: 丁群, qunding@aliyun.com

基金项目: 国家自然科学基金资助项目 (No.61471158); 黑龙江省自然科学基金优秀青年基金资助项目 (No.YQ2020F012)

Foundation Items: The National Natural Science Foundation of China (No.61471158), The Natural Science Foundation of Heilongjiang Province for Distinguished Young Scholars (No.YQ2020F012)

能力的提升,混沌映射的控制参数,甚至整个序列都可以被估计出来。2) 这些混沌映射都存在弱混沌现象,即控制参数发生微小的变化,就会造成混沌现象的消失。3) 由于动力学退化的问题,这些混沌映射会产生严重的安全缺陷,从而影响基于混沌的应用^[10-11]。

为了改善混沌映射的动力学特性,许多新的混沌映射被提出。新的混沌映射大致分为两类,第一类是基于现有混沌映射提出的改进混沌映射,文献[12]提出了离散忆阻器模型耦合一维混沌映射,得到了新的二维混沌映射,文献[13]提出了将3个不同的一维映射嵌套生成分段函数,文献[14-15]将2个一维混沌耦合生成二维混沌映射;第二类是基于线性函数或非线性函数构建新的混沌映射,文献[16]基于“周期三蕴含混沌”提出了新的二维混沌映射并研究了该映射的动力学特性,文献[17]提出了三维超混沌映射并基于该混沌映射提出了一个混沌传输方案,文献[18]基于三维分段映射提出了一个图像加密方案。上述研究都比较特殊,没有一种广义的表达式,不具有一般性。文献[19]根据相似矩阵的观点,提出了一个高维离散混沌映射,但该映射只针对高维混沌映射,不适用于二维混沌映射。文献[20]根据 Lyapunov 指数的定义反向构造了一个二维多项式混沌映射,基于这种构造方法,映射中的一个方程必为线性映射。如果初始值和控制参数选取特殊值,那么映射的维数就会降低,映射所产生序列的复杂度不能满足要求。为此,本文提出一种二维多项式混沌映射,其可以产生具有稳健性和既定复杂行为的二维混沌映射。理论仿真和实验结果表明了该映射的优越性。本文的主要工作总结如下。

1) 本文提出了一个广义二维多项式混沌映射,通过一个命题给出不同控制参数和多项式最高次数,得到一系列具体的二维混沌映射。

2) 理论分析结果表明,二维多项式混沌映射可以产生稳健混沌和期望的 Lyapunov 指数。

3) 为了阐述该映射的有效性,本文给出了一个具体的数值实例,特性分析表明,本文提出的混沌映射比 Hénon 映射、2D-SLM 和 2D-LSMCM 动力学特性更为复杂。

4) 本文将不同混沌映射应用于 RM-DCSK 通信方案,实验结果表明,本文映射更适合于信息传输。

1 二维混沌映射

本节介绍3种典型的二维混沌映射,并通过分岔图和相空间运动轨迹分析其动力学特性。由于现有映射只在一定的参数范围内存在混沌行为,且混沌序列的输出不均匀,本文提出了一个二维多项式混沌映射。首先,通过设计一个命题,从理论上给出了系统存在混沌行为的参数取值。然后,选择不同控制参数和多项式最高次数,得到许多具有稳健混沌和既定复杂行为的二维混沌映射。最后,通过平衡点分析研究了该映射的稳定性。

1.1 现有二维混沌映射

Hénon 映射作为经典的二维离散混沌映射,其数学表达式为

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \quad (1)$$

其中, x_n 和 y_n 为映射的状态变量, a 和 b 为映射的控制参数。当参数 $a = 1.4, b = 0.3$ 时,映射为混沌状态。近年来,许多学者也提出了改进的二维混沌映射,文献[14]以一维 Logistic 映射和 Sine 映射为基础,提出了一种新的二维混沌映射(2D-SLM, two dimensional sine-logistic map),其数学表达式为

$$\begin{cases} x_{n+1} = a(\sin(\pi y_n) + b)x_n(1 - x_n) \\ y_{n+1} = a(\sin(\pi x_{n+1}) + b)y_n(1 - y_n) \end{cases} \quad (2)$$

其中, x_n 和 y_n 为映射的状态变量, a 和 b 为映射的控制参数。当参数 $a = 1, b = 3$ 时,映射为混沌状态。文献[15]同样以一维 Logistic 映射和 Sine 映射为基础,提出了另一种新的二维混沌映射(2D-LSMCM, two dimensional logistic-sine-modulated-coupling map),其数学表达式为

$$\begin{cases} x_{n+1} = (\sin(4a\pi y_n(1 - y_n)) + b)x_n(1 - x_n) \\ y_{n+1} = (\sin(4a\pi x_{n+1}(1 - x_{n+1})) + b)y_n(1 - y_n) \end{cases} \quad (3)$$

其中, x_n 和 y_n 为映射的状态变量, a 和 b 为映射的控制参数。当参数 $a = 0.75, b = 3$ 时,映射为混沌状态。对于一个混沌映射,其分岔图刻画了不同参数情况下的运动轨迹。通过分岔图可以直观地衡量混沌映射在不同控制参数下的遍历性和非周期性。图1的前两列展示了3个混沌映射的2个状态变量 x_n 和 y_n 随控制参数 b 变化的分岔图(控制参数 a 固定),

可以看出 3 个映射的分岔图只有在很小的区域内才表现出混沌状态，并且出现了周期窗。若控制参数发生偏差，映射就有可能从混沌态退化为周期运动。图 1 的最后一列描绘了 3 个映射在固定参数下的相空间运动轨迹，可以看出 Hénon 映射的输出序列只分布在二维平面的一小块区域，而其他映射的输出序列也分布在特定区域。这说明 3 个映射的输出序列分布不具有均匀性，会使混沌映射在图像加密、信息传输、信息安全领域受到影响。

1.2 广义二维多项式混沌映射

为了增强混沌映射的动力学特性，本文提出了一种二维多项式混沌映射。其数学表达式为

$$\begin{cases} x_{n+1} = (ax_n + by_n^\gamma) \bmod \beta \\ y_{n+1} = (cy_n + r_n) \bmod \beta \end{cases} \quad (4)$$

其中， x_n 和 y_n 是映射的状态变量， a, b, c, r 是映射

的控制参数， γ 是多项式最高次数， β 是取模系数。为防止状态变量 y_n 塌陷为一个固定值，本文将 r_n 取为随机扰动量。下面，通过一个命题来讨论该映射何时处于混沌状态。

1.3 混沌行为证明

Lyapunov 指数是用来证明一个映射是否为混沌最有效的手段。本文采用 Lyapunov 指数来判别所构造的映射。

定义 1^[21] 若一个二维映射是全局有界的，且至少有一个正的 Lyapunov 指数，则该映射处于混沌状态；若具有 2 个正的 Lyapunov 指数，则处于超混沌状态。

一个二维离散动力学映射的 2 个 Lyapunov 指数计算表达式为

$$LE_i = \lim_{k \rightarrow \infty} \frac{1}{k} \ln \lambda_i(\Phi_k), \quad i = 1, 2 \quad (5)$$

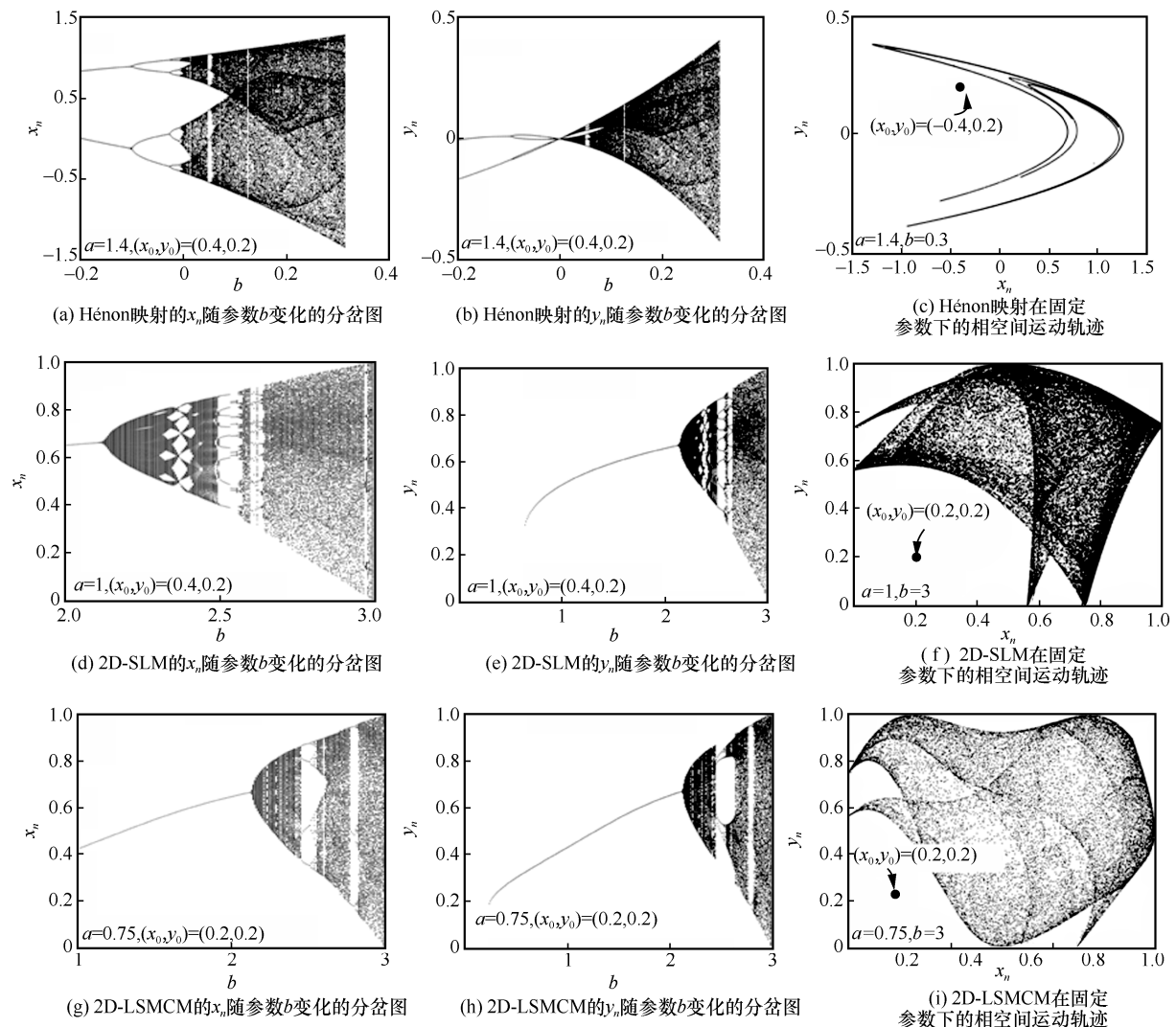


图 1 二维混沌映射的分岔图和运动轨迹

其中, $\lambda_i(\Phi_k)$ 是矩阵 Φ_k 的第 i 个特征值, Φ_k 的表达式为

$$\Phi_k = \prod_{i=0}^{k-1} J(x(i), y(i)) \quad (6)$$

其中, $J(\bullet)$ 是系统第 i 次迭代时的 Jacobian 矩阵。

命题 1 若式(4)的控制参数 $|a| > 1$ 或 $|b| > 1$, 则该映射是混沌的。若 $|a| > 1$ 且 $|b| > 1$, 则该映射是超混沌的。

证明 式(4)第 i 次迭代的 Jacobian 矩阵为

$$J(x(i), y(i)) = \begin{pmatrix} a & g(y_i) \\ 0 & b \end{pmatrix} \quad (7)$$

其中, $g(y_i) = c\gamma y_i^{\gamma-1}$, 矩阵 Φ_k 的推导过程为

$$\begin{aligned} \Phi_k &= \prod_{i=0}^{k-1} J(x(i), y(i)) = \\ &= \begin{pmatrix} a & g(y_0) \\ 0 & b \end{pmatrix} \cdots \begin{pmatrix} a & g(y_{k-1}) \\ 0 & b \end{pmatrix} = \\ &= \begin{pmatrix} a^k & t(a, b, g(y_0), \dots, g(y_{k-1})) \\ 0 & b^k \end{pmatrix} \end{aligned} \quad (8)$$

其中, $t(a, b, g(y_0), \dots, g(y_{k-1}))$ 是由变量 $a, b, g(y)$ 表示的一个具体数值, 矩阵 Φ_k 的 2 个特征值 λ_1, λ_2 也可以容易求出, 即

$$\lambda_1 = a^k, \quad \lambda_2 = b^k \quad (9)$$

那么该映射的 2 个 Lyapunov 指数的推导过程为

$$LE_1 = \lim_{k \rightarrow \infty} \frac{1}{k} \ln \lambda_1 = \lim_{k \rightarrow \infty} \frac{1}{k} \ln(a)^k = \ln a \quad (10)$$

同理, $LE_2 = \ln b$ 。由于式(4)加入了取模运算, 因此映射的输出必定是全局有界的。若控制参数 $|a| > 1$ 或 $|b| > 1$, 则必有一个正的 Lyapunov 指数, 则该映射处于混沌状态。若控制参数 $|a| > 1$ 且 $|b| > 1$, 则 2 个 Lyapunov 指数都是正的, 则该映射处于超混沌状态。证毕。

1.4 平衡点及稳定性

平衡点是指动力学系统下一时刻的运动状态与当前时刻的状态一致, 其数学表达式为 $f(\dots f(x)\dots) = x, f(\dots f(y)\dots) = y$ 。二维混沌映射所有的平衡点都是方程式(11)的解。

$$\begin{cases} x = (ax + cy^\gamma) \bmod \beta \\ y = (by + r_n) \bmod \beta \end{cases} \quad (11)$$

通过对式(11)进行求解, 可以得到许多不同的平衡点。显然, $(0, 0)$ 是上述方程的一个解, 因为不同的参数设置, 上述方程会出现很多非零平衡点。不妨设系统的非零平衡点为 (x_s, y_s) , 混沌映射的 Jacobian 矩阵为式(7)。从式(7)可以看出, Jacobian 矩阵的 2 个特征值为 $\lambda = a, \lambda = b$, 即特征值只取决于控制参数, 而与状态变量无关。当参数 $a > 1$ 且 $b > 1$ 时, Jacobian 矩阵的 2 个特征值始终为 $|\lambda_1| > 1, |\lambda_2| > 1$ 。那么二维混沌映射模型所有非零平衡点都是不稳定的, 从而系统可以表现出混沌状态甚至超混沌状态。

2 数值实验

本节按照命题 1 给出的结论, 构造了一个具体的二维多项式混沌映射。目前, 判断混沌特性的主要方法主要有相轨迹(相图)分析法、分岔图、Lyapunov 特征指数法、分数维分析法、复杂度测度法、自功率谱谱分析法等^[22]。本文通过相图、分岔图、Lyapunov 指数、样本熵(SE, sample entropy)、关联维数(CD, correlation dimension)分析其动力学行为, 并通过与现有二维混沌映射进行对比, 以阐述该映射的优良特性。

2.1 数值实例

为了方便计算, 本文取 $\gamma = 2$, 该二维多项式混沌映射的数学表达式为

$$\begin{cases} x_{n+1} = (ax_n + cy_n^2) \bmod \beta \\ y_{n+1} = (by_n + r_n) \bmod \beta \end{cases} \quad (12)$$

由命题 1 可知, 若要使式(12)处于混沌状态, 则令 $a = 2, b = 3, c = 1.7, \beta = 1, r_n$ 是 $(0, 1)$ 范围的一个随机数。为了方便讨论, 本文将控制参数的范围取为 $a, b, c \in (1, 5)$ 。

2.2 分岔图与运动轨迹

对于一个混沌映射, 其分岔图刻画了不同参数情况下的运动轨迹。通过分岔图, 可以直观地衡量混沌映射在不同控制参数下的遍历性和非周期性。动力学系统的分岔图显示了在不同参数下系统在相空间中所经过的点, 为研究混沌的性质提供了一种直观的方法。图 2 以三维视角展示了该映射随 2 个参数变化的分岔图。从图 2 中可以看出, 状态变量 x_n 在不同的控制参数下都均匀地分布在空间。图 3 展示了映射在固定参数下的运动轨迹, 随着迭代次数的增加, 系统的输出范围为 $[0, 1)$ 。

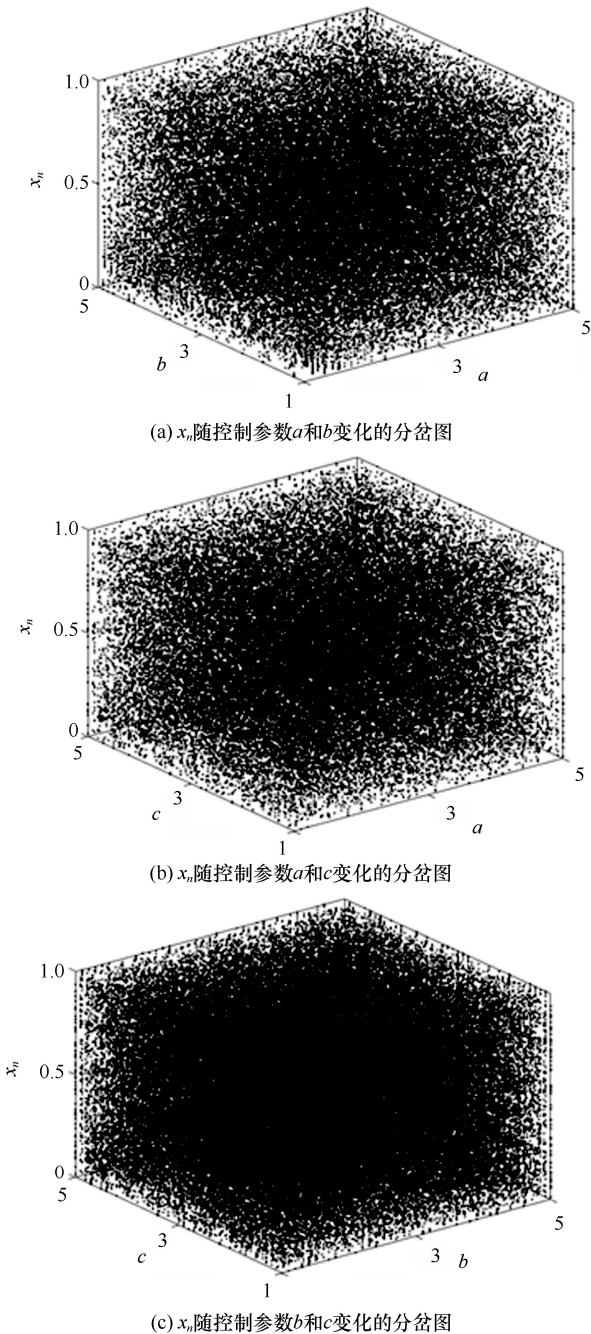


图 2 映射随 2 个参数变化的分岔图

2.3 Lyapunov 指数

在非线性动力学理论中, Lyapunov 指数可有效地描述映射随时间演化时映射对初值的敏感性。对初始条件的敏感性是混沌的一个重要特征, 即相空间中的 2 个轨道彼此接近, 随着时间的推移, 它们会以指数形式分离。若 Lyapunov 指数为负, 表明系统的相体积在运动方向上是收缩的, 即该方向的运动是稳定的; 若 Lyapunov 指数为正, 表明系统的相体积在某个方向上是不

断膨胀和折叠的, 导致吸引子中本来邻近的轨迹变得越来越不相关, 从而使初始状态不确定的映射随时间演化时, 其行为变得不可预测, 即初值敏感性。此时, 映射的运动状态是混沌的。Lyapunov 指数的计算在前文已做过叙述, 本节不做赘述。该映射随控制参数变化的 Lyapunov 指数谱如图 4 所示。从图 4(a)和图 4(b)可以看出, Hénon 映射和 2D-SLM 只有在极小参数范围内有正的 Lyapunov 指数; 从图 4(c)可以看出, 系统在 $(1, 5]$ 参数范围内都有正的 Lyapunov 指数, 与前面给出的理论分析一致。如果映射的控制参数发生微小变化, 前 2 个映射会出现弱混沌, 甚至退化为周期行为, 而本文映射仍然保持混沌状态。其次, 映射在 $(1, 5]$ 参数范围内具有 2 个正的 Lyapunov 指数, 因此映射在 $(1, 5]$ 范围内处于超混沌状态, 相较于前 2 个映射, 本文映射展示了稳健超混沌行为和更复杂的动力学特性。

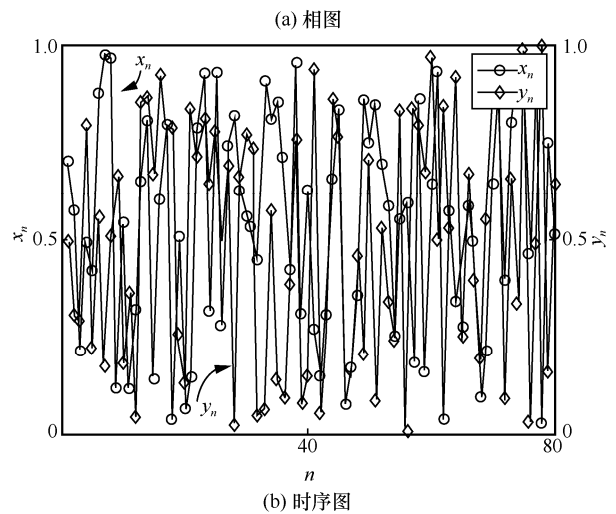
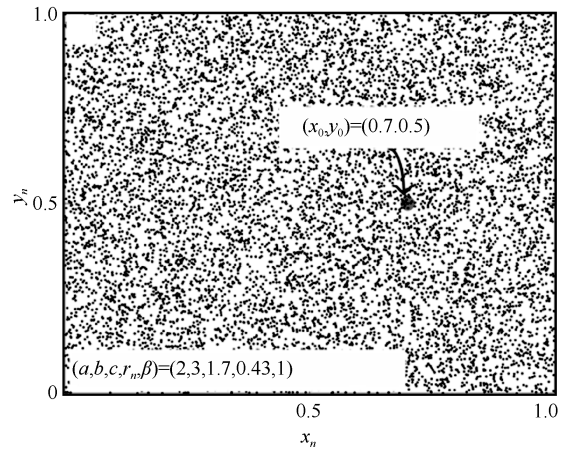


图 3 映射在固定参数下的运动轨迹

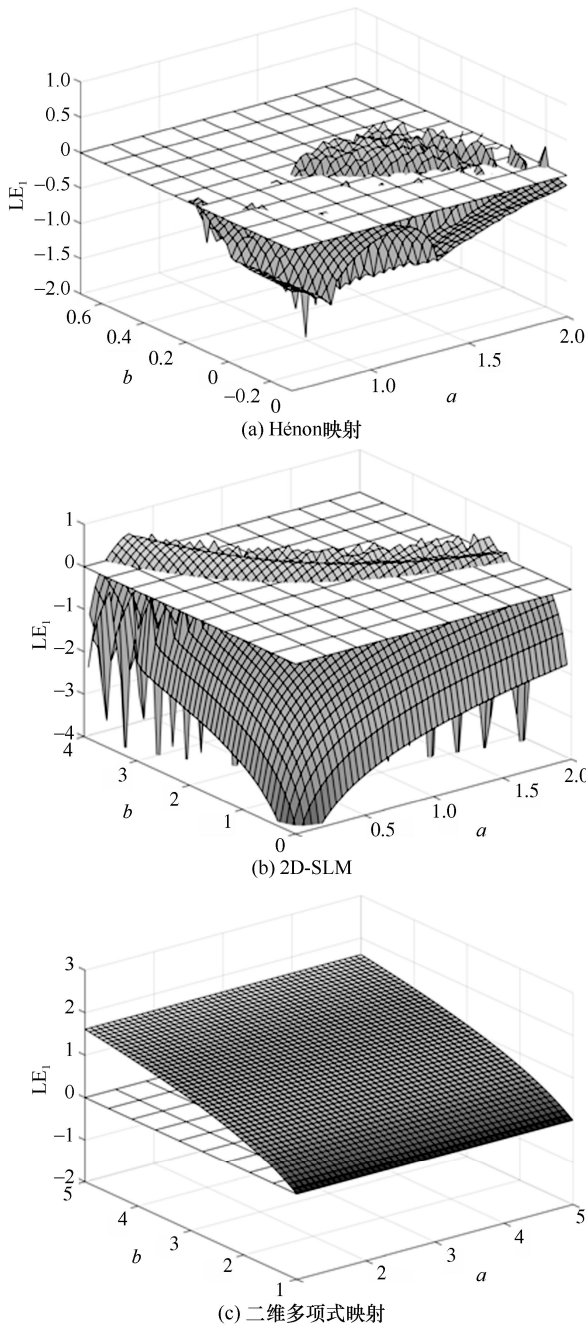


图 4 映射随 2 个参数变化的 Lyapunov 指数谱

2.4 样本熵

样本熵是基于近似熵提出的一种新的生物时间序列复杂度的分析算法^[23-24]。该算法取消了近似熵中的自匹配，使其计算更为简单，计算时间大大缩短，计算的条件概率也更加精确。该算法在计算上采用去除与自身模板比较的方式，扩大了与阈值相比较的偏差值，可以更加准确地估计新数据出现的概率，降低了近似熵的误差，是时间序列复杂度量化更加精确的一种算法。近似熵值越接近 0，时间序列的自相似性越强，产生新数据的概率越小，

复杂度越低；近似熵值越大，映射的复杂度越高。图 5 展示了不同映射随参数变化的近似熵值。从图 5(a)和图 5(b)可以看出，2 个映射在特定范围内可以取得正的近似熵值，且近似熵值都介于 (0, 1)；从图 5(c)可以看出，二维多项式映射的近似熵值在整个区间都是正的，且近似熵值也大于前 2 个映射。这说明了该映射产生的混沌序列具有很高的复杂度，可应用于图像加密、信息处理和信息传输等领域。

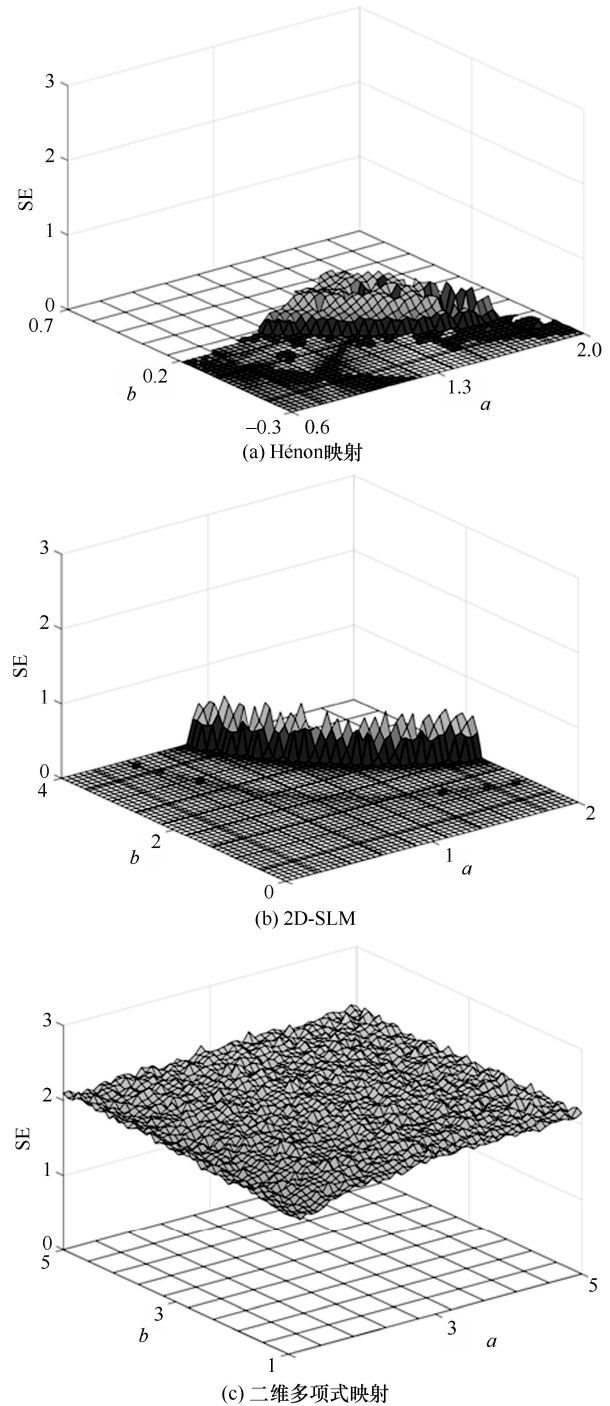


图 5 映射随 2 个参数变化的近似熵值

2.5 关联维数

作为分形维数的一种，关联维数研究的是时间序列所占据空间维数^[25]。时间序列的关联维数的表达式为

$$d = \lim_{r \rightarrow 0} \lim_{N \rightarrow \infty} \frac{\log C_m(r)}{\log r} \quad (13)$$

其中， m 表示序列的嵌入维数， r 表示嵌入空间球的半径， $C_m(r)$ 表示关联函数，其表达式为

$$C_m(r) = \lim_{N \rightarrow \infty} \frac{1}{N(N-1)} \sum_{i \neq j} \theta(r - |x_i - x_j|) \quad (14)$$

其中， $\theta(x)$ 表示阶跃函数， $|\cdot|$ 表示欧氏空间中 X_i 与 X_j 之间的距离， N 表示相空间中点的个数。如果一个非线性映射其输出序列的关联维数大于 0，则表明该非线性映射具有混沌行为。数值越接近映射的维数，映射的混沌行为越复杂。表 1 展示了 4 个混沌映射在给定参数下的关联维数。相较于其他映射，二维多项式混沌映射的关联维数大于其他 3 个系统，表明二维多项式混沌映射产生的时间序列具有更高空间维数。

表 1 4 个混沌映射在给定参数的下的关联维数

映射	初始值 (x_0, y_0)	参数 (a, b)	CD
Hénon 映射	(0.4, 0.3)	(1.4, 0.3)	1.359 9
2D-SLM	(0.4, 0.3)	(1, 3)	1.546 2
LSMCL	(0.4, 0.3)	(0.75 3)	1.491 4
本文映射	(0.4, 0.3)	(49, 49)	1.990 8

2.6 随机性测试

为了证明混沌输出序列的伪随机性，本文通过 NIST SP 800-22 进行测试。对于 NIST 套件中的 15 项测试，其显著性水平设置为 1%。当 $P > 0.01$ 时，该二进制序列就被认为是随机的，且其置信度为 99%，否则被认为是非随机的。在本文测试中，给定初始值和控制参数，由于混沌序列的输出都介于 $[0, 1)$ ，本文采用等式 $B = \lfloor d_i \alpha \rfloor \bmod \beta$ ，将十值序列转化为二值序列。其中， $\lfloor \cdot \rfloor$ 是向下取整函数， d_i 是混沌输出序列， α 是一个很大的数来影响序列的数值， β 是一个整数。设 $\alpha = 10^8, \beta = 256$ ，可以得到 8 bit 的二进制序列。然后对 2 个混沌序列进行 NIST 测试，测试结果如表 2 所示。在表 2 中，所有测试均测试成功，表明所提映射产生的混沌序列具有很强的随机性。

表 2 混沌序列的 NIST 测试结果

测试序号	测试项目	P 值		结果
		x 序列	y 序列	
1	频率	0.554 320	0.326 810	通过
2	组内频数	0.834 570	0.577 802	通过
3	游程	0.547 600	0.197 506	通过
4	组内最长游程	0.801 265	0.792 351	通过
5	二元矩阵秩	0.972 745	0.267 811	通过
6	离散傅里叶变换	0.035 687	0.948 721	通过
7	非重叠模板匹配	0.235 874	0.478 512	通过
8	重叠模板匹配	0.497 832	0.089 451	通过
9	通用统计	0.935 647	0.058 974	通过
10	线性复杂度	0.798 145	0.278 945	通过
11	串行	0.754 612	0.845 971	通过
12	近似熵	0.616 784	0.089 451	通过
13	累积和	0.168 745	0.944 513	通过
14	随机偏离	0.654 123	0.087 945	通过
15	随机偏离变量	0.565 209	0.058 799	通过

3 混沌映射在信息传输中的应用

由于混沌映射的不可预测性以及遍历性，因此其被广泛用于网络传输数据。利用混沌映射产生的序列进行数据传输时，其输出的分布对传输误码性能有很大的影响^[26-29]。由于本文构造的二维多项式混沌映射的输出较为均匀地分布在整个取值空间上，因此使该混沌映射在安全通信中可以表现出较高的性能。本节使用参考调制差分混沌移位键控 (RM-DCSK, reference-modulated differential chaos shift keying)^[30]来演示本文所提混沌映射在信息传输中的性能。

3.1 RM-DCSK 通信方案

RM-DCSK 通信方案由发送端和接收端两部分组成。发送端首先利用混沌序列对信息比特位进行编码，生成传输信号，然后将传输信号发送给接收端。接收端对接收信号进行解码，从而恢复出信息比特位。

1) 发送端。传输信号的结构如图 6 所示， b_{2k} 是第 $2k$ 个信息比特位， X_k 是一条长度为 M 的混沌序列，表达式为 $X_k = \{x_i | 2kM < i \leq (2k+1)M\}$ ， M 为扩频指数。RM-DCSK 通信方案的发送端结构如图 7 所示。首先，将系统的第一个时隙设置为参考时隙，混沌信号 x_i 作为信息载波在第一个时隙内传输比特信息 b_{2k} ，而第二个时隙是两部分之和，前一部分是将上一个时隙传输的信息 $b_{2k}x_{i-M}$ 作为信息载波，

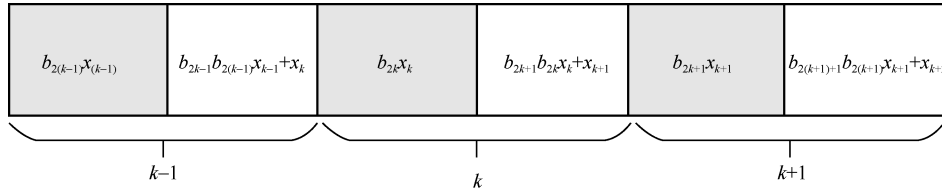


图 6 传输信号的结构

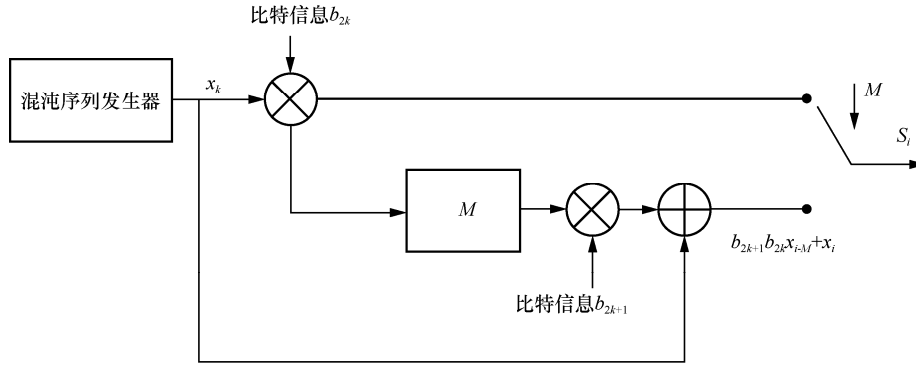


图 7 RM-DCSK 通信方案的发送端结构

然后在第二个时隙内传输比特信息 b_{2k+1} ，而后一部分是本时隙的混沌序列，即 x_i 。则第 k 帧的传输信号 s_i 的表达式为

$$s_i = \begin{cases} b_{2k}x_i, & 2kM < i \leq (2k+1)M \\ b_{2k+1}b_{2k}x_{i-M} + x_i, & (2k+1)M < i \leq 2(k+1)M \end{cases} \quad (15)$$

其中，混沌样点 x_i 满足

$$x_{(2k+1)M+m} = x_{2(k+1)M+m}, \forall k \in \{0, \pm 1, \dots\} \quad (16)$$

2) 接收端。当接收端从发送端接收到传输信号时，可以利用相关器恢复原始信息比特位。RM-DCSK 通信方案在解调时主要利用了混沌延迟特点和非相干技术，接收端结构如图 8 所示。由于信号在不同网络中传输时可能会受到噪声的干扰，因此接收到的信号与原始信号有所不同。本文主要以加性白高斯噪声 (AWGN, additive white Gaussian noise) 信道模型作为主要通信传输媒介，信道中的干扰以加性白高斯噪声 ξ_i 为主，且 $E(\xi_i) = 0$, $\text{Var}(\xi_i) = \frac{N_0}{2}$ 。则接收到的信号 r_i 为

$$r_i = s_i + \xi_i \quad (17)$$

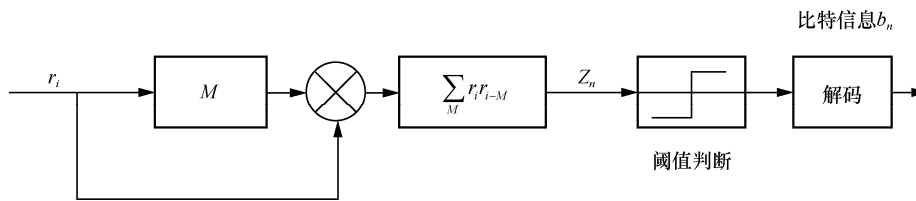


图 8 RM-DCSK 方案的接收端结构

相关器 Z_n 为

$$Z_n = \sum_{i=nM+1}^{(n+1)M} r_i r_{i-M} \quad (18)$$

恢复出信息比特位 b_{2k} 的相关器 Z_{2k} 为

$$Z_{2k} = \sum_{i=2kM+1}^{(2k+1)M} (s_i + \xi_i)(s_{i-M} + \xi_{i-M}) = \sum_{i=2kM+1}^{(2k+1)M} (b_{2k}x_i + \xi_i)(b_{2k-1}b_{2(k-1)}x_{i-2M} + x_{i-M} + \xi_{i-M}) \quad (19)$$

从式(16)得到 $x_{i-M} = x_i$ ，则式(19)可以整理为

$$Z_{2k} = \sum_{i=2kM+1}^{(2k+1)M} (b_{2k}x_i + \xi_i)(b_{2k-1}b_{2(k-1)}x_{i-2M} + x_i + \xi_{i-M}) = b_{2k} \sum_{i=2kM+1}^{(2k+1)M} x_i^2 + \sum_{i=2kM+1}^{(2k+1)M} A_i \quad (20)$$

其中

$$A_i = b_{2k}b_{2k-1}b_{2(k-1)}x_i x_{i-2M} + b_{2k}x_i \xi_{i-M} + b_{2k-1}b_{2(k-1)}x_{i-2M} \xi_i + x_i \xi_i + \xi_i \xi_{i-M} \quad (21)$$

式(20)中， $b_{2k} \sum_{i=2kM+1}^{(2k+1)M} x_i^2$ 是主体判别的信号，其

数值的正负是恢复信号信息的基础； $\sum_{i=2kM+1}^{(2k+1)M} A_i$ 是干扰信号，且噪声的能量远小于有用信息的能量。因此，相关器 Z_{2k} 的正负主要由比特信息 b_{2k} 所决定。相关器 Z_{2k+1} 也可以相似地恢复出比特信息 b_{2k+1} 。最后，根据判决门限解调出比特信息 b_n ，即

$$\hat{b}_n = f(Z_n) = \begin{cases} 1, & Z_n > 0 \\ -1, & Z_n \leq 0 \end{cases} \quad (22)$$

3.2 仿真实验

为了证明本文构造的混沌映射在 RM-DCSK 中的优良特性，本文对比了现有的 4 种二维离散混沌映射，如经典的 Hénon 混沌映射、2D-SLM、2D-LSMCM、文献[19]混沌映射。在不同的扩频指数 M 及不同等级噪声的 AWGN 信道模型中，本文使用以上混沌序列发生器进行了 RM-DCSK 通信方案的仿真。每次实验传输数据是一个随机生成的 1×10^5 bit 长度的二进制序列。通过计算接收到的数据与原始数据之间的误码率 (BER, bit error ratio) 来验证其抗噪声能力。第一组研究针对不同扩频指数下的误码率。对于每个混沌映射，实验设置如下。

- 1) 选取 5 种混沌映射中的 x_n 序列对信息比特进行编码。
- 2) 设置 AWGN 通道的噪声强度为 26 dB，在不同的扩频指数 $M = \{10, 20, \dots, 100\}$ 下，计算 RM-DCSK 通信方案的误码率。
- 3) 在不同初始值下重复步骤 1) 和步骤 2) 10 次。
- 4) 计算这 10 次实验误码率的平均值。

第二组研究针对不同噪声等级下的误码率。对于每个混沌映射，实验设置如下。

- 1) 选取 5 种混沌映射中的 x_n 序列对信息比特进行编码。
- 2) 设置 AWGN 通道的扩频指数 $M = 80$ ，在不同的噪声等级 $\text{SNR} = \{0, 1, \dots, 30\}$ 下，计算 RM-DCSK 通信方案的误码率。
- 3) 在不同初始值下重复步骤 1) 和步骤 2) 10 次。
- 4) 计算这 10 次实验误码率的平均值。

从图 9 中可以看出，在不同扩频指数 M 下，RM-DCSK 通信采用本文提出的二维多项式混沌映射总能比其他混沌映射获得更小的误码率。从图 10 中可以看出，当信噪比较小时，使用不同混沌映射的 RM-DCSK 通信方案可以获得几乎相同的误码率。但随着信噪比的增加，使用本文提出的二维多

项式混沌映射比使用其他混沌映射可获得更小的误码率。这说明二维多项式混沌映射相较于其他混沌映射更适用于信息传输。

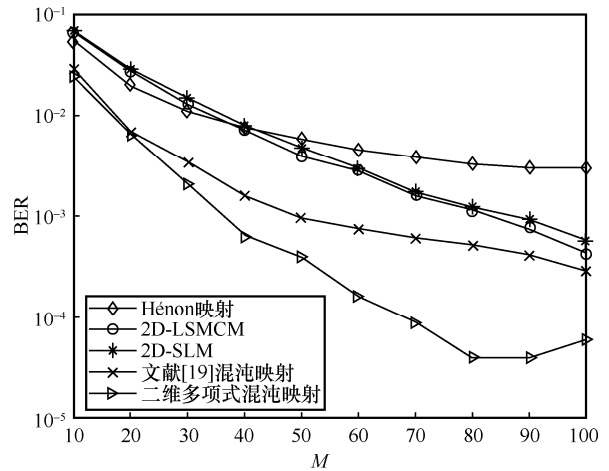


图 9 不同扩频指数下 RM-DCSK 方案的误码率

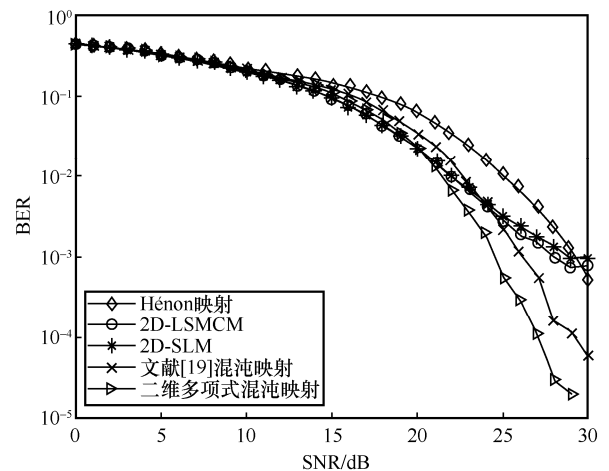


图 10 不同噪声等级下 RM-DCSK 方案的误码率

4 结束语

为了解决离散混沌映射存在着混沌范围不连续、输出分布不完整等缺陷，本文提出了广义二维多项式混沌映射，并通过理论分析与实验仿真证实了该映射的有效性，最后将 5 种二维混沌映射应用于 RM-DCSK 通信方案中。相较于其他混沌映射，本文提出的二维多项式混沌映射可以获得更小的误码率，说明了该映射更适用于信息传输。在后续工作中，本文将基于局域网，利用现场可编程门阵列硬件平台搭建通信方案模型，RM-DCSK 通信方案可以为加密端和解密端发送密钥。

参考文献:

- [1] VAIDYANATHAN S, VOLOS C. Advances and applications in chaotic systems[M]. Berlin: Springer International Publishing, 2016.
- [2] BURT P M S, DE MORAIS G J H. Efficient computation of bilinear approximations and Volterra models of nonlinear systems[J]. IEEE Transactions on Signal Processing, 2018, 66(3): 804-816.
- [3] 黄润生, 黄浩. 混沌及其应用: 第二版[M]. 武汉: 武汉大学出版社, 2005.
- [4] HUANG R S, HUANG H. Chaos and its application[M]. 2nd ed. Wuhan: Wuhan University Press, 2005.
- [5] HIRSCH M W, SMALE S, DEVANEY R L. Differential equations, dynamical systems, and an introduction to chaos[M]. Amsterdam: Elsevier, 2013.
- [6] SCHUSTER H G, JUST W. Deterministic chaos[M]. Berlin: Wiley-VCH, 2005.
- [7] GUREVICH A, COHEN K, ZHAO Q. Sequential anomaly detection under a nonlinear system cost[J]. IEEE Transactions on Signal Processing, 2019, 67(14): 3689-3703.
- [8] WANG Z P, WU H N. On fuzzy sampled-data control of chaotic systems via a time-dependent Lyapunov functional approach[J]. IEEE Transactions on Cybernetics, 2015, 45(4): 819-829.
- [9] JANAKIRAMAN S, THENMOZHI K, RAYAPPAN J B B, et al. Lightweight chaotic image encryption algorithm for real-time embedded system: implementation and analysis on 32-bit microcontroller[J]. Microprocessors and Microsystems, 2018, 56: 1-12.
- [10] CAO Z L, WANG L D. A secure video watermarking technique based on hyperchaotic Lorenz system[J]. Multimedia Tools and Applications, 2019, 78(18): 26089-26109.
- [11] HUA Z Y, ZHOU Y C. Dynamic parameter-control chaotic system[J]. IEEE Transactions on Cybernetics, 2016, 46(12): 3330-3341.
- [12] LIU L F, LIU B C, HU H P, et al. Reducing the dynamical degradation by Bi-coupling digital chaotic maps[J]. International Journal of Bifurcation and Chaos, 2018, 28(5): 1850059.
- [13] LI H Z, HUA Z Y, BAO H, et al. Two-dimensional memristive hyperchaotic maps and application in secure communication[J]. IEEE Transactions on Industrial Electronics, 2021, 68(10): 9931-9940.
- [14] ZHOU Y C, BAO L, CHEN C L P. Image encryption using a new parametric switching chaotic system[J]. Signal Processing, 2013, 93(11): 3039-3052.
- [15] HUA Z Y, ZHOU Y C, PUN C M, et al. 2D sine logistic modulation map for image encryption[J]. Information Sciences, 2015, 297: 80-94.
- [16] ZHU H G, ZHAO Y R, SONG Y J. 2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption[J]. IEEE Access, 2019, 7: 14081-14098.
- [17] WANG C F, DING Q. A class of quadratic polynomial chaotic maps and their fixed points analysis[J]. Entropy (Basel, Switzerland), 2019, 21(7): 658.
- [18] LI W S, YAN W H, ZHANG R X, et al. A new 3D discrete hyperchaotic system and its application in secure transmission[J]. International Journal of Bifurcation and Chaos, 2019, 29(14): 1950206.
- [19] LIU C Y, DING Q. A color image encryption scheme based on a novel 3D chaotic mapping[J]. Complexity, 2020, 2020: 3837209.
- [20] WANG C F, FAN C L, DING Q. Constructing discrete chaotic systems with positive Lyapunov exponents[J]. International Journal of Bifurcation and Chaos, 2018, 28(7): 1850084.
- [21] HUA Z Y, CHEN Y Y, BAO H, et al. Two-dimensional parametric polynomial chaotic system[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52(7): 4402-4414.
- [22] WOLF A, SWIFT J B, SWINNEY H L, et al. Determining Lyapunov exponents from a time series[J]. Physica D: Nonlinear Phenomena, 1985, 16(3): 285-317.
- [23] 孙克辉. 混沌信息传输原理与技术[M]. 北京: 清华大学出版社, 2015.
- [24] SUN K H. Principle and technology of chaotic secure communication[M]. Beijing: Tsinghua University Press, 2015.
- [25] LAKE D E, RICHMAN J S, GRIFFIN M P, et al. Sample entropy analysis of neonatal heart rate variability[J]. American Journal of Physiology Regulatory, Integrative and Comparative Physiology, 2002, 283(3): 789-797.
- [26] RAMDANI S, SEIGLE B, LAGARDE J, et al. On the use of sample entropy to analyze human postural sway data[J]. Medical Engineering & Physics, 2009, 31(8): 1023-1031.
- [27] LACASA L, GÓMEZ-GARDEÑES J. Correlation dimension of complex networks[J]. Physical Review Letters, 2013, 110(16): 168703.
- [28] 于娜, 丁群, 陈红. 异结构系统混沌同步及其在信息传输中的应用[J]. 通信学报, 2007, 28(10): 73-78.
- [29] YU N, DING Q, CHEN H. Synchronization of different structure chaotic systems and the application in secure communication[J]. Journal on Communications, 2007, 28(10): 73-78.
- [30] 朱勇, 王佳楠, 丁群. 新型的 CD-DCSK 混沌键控信息传输系统[J]. 通信学报, 2012, 33(5): 169-176.
- [31] ZHU Y, WANG J N, DING Q. New kind of CD-DCSK chaos shift keying secure communication system[J]. Journal on Communications, 2012, 33(5): 169-176.
- [32] LI G Z, ZHANG B. A novel weak signal detection method via chaotic synchronization using chua's circuit[J]. IEEE Transactions on Industrial Electronics, 2017, 64(3): 2255-2265.
- [33] ZHANG X X, XU J. An extended synchronization method to identify slowly time-varying parameters in nonlinear systems[J]. IEEE Transactions on Signal Processing, 2018, 66(2): 438-448.
- [34] YANG H, JIANG G P. Reference-modulated DCSK: a novel chaotic-communication scheme[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2013, 60(4): 232-236.

[作者简介]



闫文浩(1995-), 男, 陕西渭南人, 黑龙江大学博士生, 主要研究方向为混沌映射动力学分析、混沌同步及混沌信息传输。

姜子敬(1994-), 男, 黑龙江哈尔滨人, 黑龙江大学博士生, 主要研究方向为网络信息安全及硬件加密侧信道分析。

黄欣(1992-), 女, 黑龙江哈尔滨人, 黑龙江大学博士生, 主要研究方向为图像加密及网络信息安全。

朱淑娟(1965-), 女, 博士, 澳大利亚佛林德大学科学与工程学院研究员, 主要研究方向为智能计算、数据挖掘、数字水印及信息隐藏。

丁群(1957-), 女, 黑龙江哈尔滨人, 博士, 黑龙江大学教授、博士生导师, 主要研究方向为混沌加密算法与系统集成、混沌信息传输和网络信息安全等。