计算机科学
COMPUTER SCIENCE

基于m序列和球腔体的二维动态耦合映像格系统及其特性

马英杰, 田彦, 赵耿, 杨亚涛, 覃晶滢, 洪辉

引用本文

马英杰, 田彦, 赵耿, 杨亚涛, 覃晶滢, 洪辉. 基于m序列和球腔体的二维动态耦合映像格系统及其特性[J]. 计算机科学, 2025, 52(4): 381-391.

MA Yingjie, TIAN Yan, ZHAO Geng, YANG Yatao, QIN Jingying, HONG Hui. Two-dimensional Dynamic Coupled Mapping Lattice System Based on m-sequence and Spherical Cavity and Its Characteristics [J]. Computer Science, 2025, 52(4): 381-391.

相似文章推荐（请使用火狐或 IE 浏览器查看文章）

Similar articles recommended (Please use Firefox or IE to view the article)

大模型驱动多智能体的军事需求生成框架

Large Language Models Driven Framework for Multi-agent Military Requirement Generation

计算机科学, 2025, 52(1): 65-71. https://doi.org/10.11896/jsjkx.240800022

“五位一体”通信原理课程智慧教学模式研究与实践

Research and Practice on “Five in One” Smart Teaching Model in the Course of CommunicationPrinciple

计算机科学, 2024, 51(10): 129-134. https://doi.org/10.11896/jsjkx.240300007

基于可逆元胞自动机加密的扩展码索引调制方案

Extended Code Index Modulation Scheme Based on Reversible Elementary Cellular Automata Encryption

计算机科学, 2024, 51(6): 416-422. https://doi.org/10.11896/jsjkx.230300067

基于扰动时空混沌的三维OFDM星座加密方案

Three-dimensional OFDM Constellation Encryption Scheme Based on Perturbed Spatiotemporal Chaos

计算机科学, 2024, 51(5): 390-399. https://doi.org/10.11896/jsjkx.230200169

基于抗退化混沌系统和初等元胞自动机的动态S盒设计

Design of Dynamic S-box Based on Anti-degradation Chaotic System and Elementary Cellular Automata

计算机科学, 2023, 50(11): 333-339. https://doi.org/10.11896/jsjkx.220900026

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240100008

基于 m 序列和球腔体的二维动态耦合映像格系统及其特性

马英杰[1]　田　彦[2]　赵　耿[2]　杨亚涛[1]　覃晶滢[1]　洪　辉[2]
1 北京电子科技学院电子与通信工程系　北京 100070
2 北京电子科技学院网络空间安全系　北京 100070
(myj@besti.edu.cn)

摘　要　为解决现有时空混沌系统中动力学复杂性较低和生成序列之间相关度较高的问题,提出了一种基于 m 序列和球腔体的二维动态耦合映像格系统。利用改进的 m 序列来构建迭代矩阵,用于确定每个格点在迭代过程中耦合对象的索引和扰动符号,采用球腔体构造的分段混沌映射对混沌序列引入强度可控的扰动。通过分岔图、回归映射、Lyapunov 指数和 K 熵评估系统的动力学特性,并对生成序列的相关性、均匀性、随机性以及系统的计算复杂度进行测试与验证。仿真实验与对比分析表明,该系统呈现出丰富的非线性动力学行为和优越的性能指标,包括周期倍增和分叉现象,在数据加密、图像加密和 S 盒生成领域具有潜在的应用前景。

关键词:混沌系统;二维耦合映像格;m 序列;动力学特性;球腔体
中图分类号　TN918

Two-dimensional Dynamic Coupled Mapping Lattice System Based on m-sequence and Spherical Cavity and Its Characteristics

MA Yingjie[1],TIAN Yan[2],ZHAO Geng[2],YANG Yatao[1],QIN Jingying[1] and HONG Hui[2]
1 Department of Electronic and Communication Engineering,Beijing Electronic Science and Technology Institute,Beijing 100070,China
2 Department of Cyberspace Security,Beijing Electronic Science and Technology Institute,Beijing 100070,China

Abstract　In order to solve the problems of low dynamic complexity and high correlation between generated sequences in existing spatiotemporal chaotic systems,two-dimensional dynamic coupled map lattices system based on m-sequences and spherical cavity is proposed. The improved m-sequence is used to construct an iterative matrix,which is used to determine the index and perturbation symbol of the coupled objects of each lattice in the iterative process. The piecewise chaotic mapping constructed through a spherical cavity introduces controllable perturbations to the chaotic sequence. The dynamic characteristics of the system are evaluated by bifurcation diagram,regression mapping,Lyapunov exponent and K-entropy,while the correlation,uniformity,randomness of the generated sequence and the computational complexity of the system are tested and verified. Simulation experiments and comparative analysis show that the system exhibits rich nonlinear dynamical behavior and superior performance metrics,including period doubling and bifurcation phenomena,with potential applications in data encryption,image encryption,and S-box generation.

Keywords　Chaotic system,Two-dimensional coupled map lattices,m-sequence,Dynamic characteristics,Spherical cavity

1　引言

混沌是一种不确定的行为,无法根据给定的初始条件确定其系统的未来状态。混沌系统由于具有拓扑混乱性、不可预测性、遍历性、初值敏感性以及伪随机性等动力学特性,在通信、加密、混沌计算等领域有重要的研究意义。混沌系统的动力学特性能够为密码学应用提供更高的安全性、抗攻击性和随机性,因此在流密码[1]、图像加密[2-5]、随机数生成[6]以及动态 S 盒[7-8]的生成等领域得到广泛应用。然而,在有限精度的数字系统中实现混沌系统时,常常会出现数值扩散、伪周期性、系统偏移以及弱随机性等动力学退化行为[9],导致密钥空间减小、密钥泄露风险增加,从而危及数字混沌系统的安全性。为了应对这一挑战,研究者们提出了多种解决方案。Liu 等[10]通过构建新的超 Chen 混沌系统,引入周期性的交叉影响,将多个混沌系统级联耦合来解决这个问题。这种方法有效地增加了系统的复杂性和鲁棒性,增强了系统的非线性

到稿日期:2024-01-02　返修日期:2024-05-23
基金项目:中央高校基本科研业务费(328202258,3282024060);国家自然科学基金(62441208)
This work was supported by the Fundamental Research Funds for the Central Universities(328202258,3282023054) and National Natural Science Foundation of China(62441208).
通信作者:田彦(ty19991103@163.com)

特性，但使得系统的计算复杂度大幅度增加，系统的分析、建模和控制变得更加困难。Flores 等[11]提出了使用更高运算精度的数字系统来扩展其状态空间。该方法有助于保持混沌系统的稳定性和准确性，同时减少动力学退化现象，但需要更多的位数和更复杂的运算，导致混沌系统的成本和周期难以控制。Lai 等[12]提出了一种新的超混沌系统，利用忆阻器的非线性和可塑性构建超增强混沌映射，通过导入两个一维超混沌映射来提高 Lyapunov 指数，解决了常见超混沌系统的不连续混沌范围问题。Ning 等[13]发现添加扰动可以明显降低混沌系统的动力学退化，通过对系统变量进行扰动，相比于扰动控制参数和输入，能够更有效地改善系统的动力学行为，提高系统的混沌性能和抗退化能力。

时空混沌系统[14]允许不同格点的混沌系统相互影响和扰动彼此的状态变量或输出信号，从空间耦合上增强了系统的混沌特性，逐渐成为混沌系统研究的热点领域。Kaneko 等[15]通过研究发现简单的一维离散映射格点之间的耦合就可以引发复杂的动力学行为，进而提出了耦合映像格(COUPLED Map Lattices，CML)系统。此后，越来越多的基于 CML 的时空混沌系统被引入，其中大部分是基于一维 CML[16-18]和二维 CML[19-22]的时空混沌系统。Zhao 等[16]提出了将初级元胞自动机(Cellular Automata，ECA)与伪随机耦合相结合的方法，通过调整 ECA 的参数和扰动方式，灵活地调控系统的动态行为，从而降低了格点序列之间的相关系数，有效地缓解了数字系统的动力学退化。Azam 等[17]利用 CML 的长周期和伪随机性，将其与椭圆曲线相结合，显著扩展了密钥空间，提升了系统的鲁棒性。Dong 等[18]设计的基于混合初等元胞自动机的伪随机耦合映射格系统，可以有效抵抗差分和统计攻击，增强了系统的混沌特性。以上这些研究均集中在一维时空混沌系统上。Lv 等[19]通过系统动态特性的对比分析发现，相比于一维时空混沌系统，二维时空混沌系统具有更高的复杂性和更强的数据处理能力。同时，Lai 等[23]提出的基于离散忆阻的高维超混沌系统表现出更复杂的吸引子拓扑和动态行为，在图像加密的应用中通过了相关性、信息熵等测试。因此，二维时空混沌系统在密码学领域具有更强的安全性和随机性。

Zhou 等[20]采用 PWLCM-Sin 映射作为底层映射，构建了二维混合伪随机耦合映像格系统。该系统在分叉图中没有明显的分叉行为和空白窗口，混沌系统序列值遍布整个状态空间，增强了系统的非周期性特性。然而，该系统的 K 熵密度部分值处于较低水平，并且总体大小不均匀，表明系统的复杂性和混乱度还有待进一步改善。Liu 等[21]采用分段 Logistic 映射作为底层映射来构建二维耦合映射格系统，从分岔图中的分叉现象可以看到系统的遍历性变得更加广泛。然而，相空间中的序列状态值在整个范围内的分布并不均匀，表明系统的非周期性有待改进。Ning 等[22]提出了一种基于分区初等元胞自动机的二维动态伪随机耦合映射格系统，通过元胞自动机的迭代结果确定耦合格索引坐标，系统的均匀性和随机性得到明显提升。然而，局部邻居之间的相互作用规则约束了初等元胞自动机的随机性，导致序列相对有序和可预测，安全性有待提升。

为了解决上述问题，本文提出了一种新颖的基于 m 序列和球腔体的二维动态耦合映像格(Two-dimensional Dynamic Coupled Mapping Lattice，2D-DCML)系统。该系统不仅继承了上述方案的优点，而且显著增加了系统的状态空间，降低了不同格点生成序列之间的相关性，表现出更强的混沌特性。本文的主要研究贡献如下：

1)设计了拓展 m 序列(Expand m-sequence，EMS)。传统 m 序列的有限周期性特征，限制了其提供长期稳定性和高随机性的能力。EMS 通过控制混沌系统的输入参数实现自周期扩展和最优反馈多项式选择，相比于 m 序列展现出更好的伪随机性和更大的应用空间。

2)提出了一种新型的二维映像格耦合方案。该方案通过 EMS 所构造的迭代矩阵确定当前格点的耦合对象。由于 EMS 所构造的迭代矩阵具有较高的复杂性和不可预测性，因此系统中每次迭代时耦合格的选择是伪随机的。此外，由于迭代矩阵是先行生成的，因此可以预先确定耦合过程的演化路径，这样就简化了系统的实现和计算过程，从而提高了效率。

3)在球腔体的基础上，提出了一种新的混沌映射，并设计了一种新的扰动方案。首先，对球坐标方程进行变量替换，生成新的混沌映射，采用分段函数为系统添加强度可控的伪随机扰动，通过控制扰动峰值和输入参数来调节扰动模式。其次，根据迭代矩阵确定扰动符号，保证了良好的可控性和伪随机性。研究结果表明，与其他二维耦合映像格系统相比，2D-DCML 系统呈现出更丰富的动态行为和更复杂的空间结构，混沌性质得到增强，输出序列之间的相关性显著降低。

2 设计原理

2.1 二维耦合映像格系统

二维耦合映像格(Two-dimensional Coupled Map Lattices，2D-CML)[24]系统是一种时空混沌系统，它通过非线性映射规则和耦合函数描述格点之间的相互作用。2D-CML 由一个二维的格点网络组成，每个格点都受到其 4 个相邻格点的影响，其演化规则的函数表示为：

$$\begin{aligned}X_{n+1}(i,j)=(1-\varepsilon)f[x_n(i,j)]+\frac{\varepsilon}{4}\{&f[x_n(i+1,j)]+\\&f[x_n(i-1,j)]+f[x_n(i,j+1)]+\\&f[x_n(i,j-1)]\}\end{aligned}\tag{1}$$

其中，$i=1,2,3,\cdots,R$ 和 $j=1,2,3,\cdots,L$ 分别表示行索引和列索引，$n(n=1,2,3,\cdots)$是时间索引，$\varepsilon(\varepsilon\in[0,1])$是耦合系数，$x_n(i+R,j)=x_n(i,j)$和 $x_n(i,j+L)=x_n(i,j)$为周期性边界条件，Logistic 映射函数 $f(x)$的数学表达为：

$$f(x)=\mu x(1-x)\tag{2}$$

其中，函数自变量 $x(x\in(0,1))$，系统控制参数 $\mu(\mu\in(0,4])$，当 $\mu\in[3.57,4]$时，系统的演化变得高度敏感，映射处于混沌状态[25]。

2.2 拓展 m 序列

m 序列是一种特殊的伪随机二进制序列，也被称为最大长度线性反馈移位寄存器(Linear Feedback Shift Register，LFSR)序列。由于 m 序列具有伪随机特性，因此其在音频

加密[26]、图像加密[27]等领域有着广泛的应用。通过特定的移位寄存器算法可以生成相应的 m 序列，图 1 给出了由 n 级移位寄存器构成的码序列发生器。

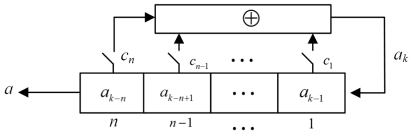


图 1　线性反馈移位寄存器

Fig. 1　Linear feedback shift register

图 1 中，$c_1, c_2, \cdots, c_n$ 均为反馈线，值为 0 则表示断开反馈线，值为 1 则表示参与反馈；反馈线的连接情况与二元域 GF(2) 上的反馈多项式 $g(x)$ 的关系如式(3)所示；$[a_{k-n}, a_{k-n+1}, \cdots, a_{k-1}]$ 为序列表示，参数 $k \geqslant n$，通过式(4)的反馈函数可以得到 a_k 的值。

$$g(x)=1+c_1x+c_2x+\cdots+c_{n-1}x^{n-1}+c_nx^n \tag{3}$$

$$a_k = c_1a_{k-1} \oplus c_2a_{k-2} \oplus \cdots \oplus c_na_{k-n} = \sum_{j=1}^{n} c_j a_{k-j} \tag{4}$$

在一个 n 级移位寄存器中，第 i 级移位寄存器的状态是由前一个时钟周期后第 $i-1$ 级移位寄存器的状态决定，状态 $S_m=(a_{m+n-1}, \cdots, a_{m+1}, a_m)$ 到 $S_{m+1}=(a_{m+n}, \cdots, a_{m+2}, a_{m+1})$ 的状态转移矩阵如式(5)所示：

$$\begin{pmatrix} a_{m+n} \\ a_{m+n-1} \\ a_{m+n-2} \\ \cdots \\ a_{m+2} \\ a_{m+1} \end{pmatrix} = \begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_{n-2} & c_n \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \times \begin{pmatrix} a_{m+n-1} \\ a_{m+n-2} \\ a_{m+n-3} \\ \cdots \\ a_{m+1} \\ a_m \end{pmatrix} \tag{5}$$

传统 m 序列的本原多项式通常是固定的，这限制了序列的变化和性能。本文方案通过引入最佳反馈多项式替换的方法，对其进行改进和拓展，构建 EMS。EMS 的长度 N 以及初态寄存器长度 K 的计算公式为：

$$N=R\times L\times Num \tag{6}$$

$$K=ceil(\log_2 N) \tag{7}$$

其中，Num 为 2D-DCML 系统的迭代次数，$ceil$ 函数表示向上取整，N 与 K 的值随变量自适应调整。

生成 EMS 的具体步骤为：1)初始化寄存器，随机生成 K 位的比特序列作为寄存器的初始状态；2)用比特序列表示随机生成的 K 个反馈多项式的系数对，计算每个比特序列的十进制值，从中选取值最大的 3 个反馈多项式作为最佳反馈多项式；3)在寄存器进行移位和异或的操作期间，切换最佳反馈多项式来计算反馈值，并更新寄存器的状态。

2.3　m 序列与 EMS 的性能分析

2.3.1　线性复杂度

伯利坎普-梅西算法(Berlekamp Massey，BM) 是一个迭代算法，它的基本思想是利用前 $n-1$ 个比特序列求出的最小线性多项式来确定前 n 个比特序列的最小线性多项式。该算法通过动态地调整线性复杂度估计和伴随多项式确定序列的最小线性复杂度。为验证 2.2 节方案生成序列的线性复杂度，表 1 列出了采用 BM 算法对线性时间内的传统 m 序列和 EMS 的分析结果。

表 1　线性复杂度

Table 1　Linear complexity

Length-N	LSFR-K	Linear complexity	
		m-sequence	EMS
10^4	13	8191	10^4
10^5	13	8191	10^5
10^5	16	65535	10^5
10^6	16	65535	10^6
10^6	19	524287	10^6
10^7	19	524287	10^7
10^7	23	8388607	10^7

从密码分析的角度考虑，要使得用线性方法对密钥序列进行重建所需的代价最小，需要构造一个级数尽可能小的 LFSR 来生成长度为 N 的序列。表 1 中，在所需序列长度 N 确定的情况下，由 BM 算法计算得到 m 序列的 LFSR-K 的最小值为 $ceil(\log_2(N+1))$。而式(7)中，$ceil(\log_2 N)$ 为 EMS 所需 LFSR-K 的最大值。在 LSFR-K 确定的情况下，m 序列的周期是固定的(2^K-1)，而 EMS 的周期长度远大于(2^K-1)。此外，本原多项式是产生最长周期的序列的关键，m 序列的本原多项式数量由欧拉函数 $\varphi(2^K-1)$ 计算得出。因此，EMS 通过最佳反馈多项式替换的方法解决了本原多项式相对较少的问题，并且达到了与混沌系统所需序列长度相等的最小线性复杂度。

2.3.2　均衡特性

在通信和密码学中，数字序列的均衡性是一个重要的特性，因为它可以确保序列在不同的情况下表现得足够随机。在 m 序列的每个周期中，1 的数量比 0 多 1 个。图 2 给出了比特“1”在不同序列长度中 1000 个等差样本下出现的频率分布曲线。在仿真过程中，图 2(a)、图 2(c)、图 2(e)分别采用表 2 中寄存器级数(14，17，20)对应的八进制反馈系数(42103，400011，4000011)，使 m 序列的频率分布达到最优，而 EMS 则由 2.2 节方案自适应生成。在图 2 中，对于 m 序列，其中“1”的最优频率分布区间为(0.35，0.5)，峰谷值相差 0.15，且 3 种不同序列长度的频率分布始终低于 0.5；对于 EMS，其中“1”的最差频率分布区间为(0.48，0.56)，峰谷值相差 0.08，特别是在 EMS-10^6 中仅相差 0.01。虽然 m 序列 0 和 1 的分布平衡与序列长度呈正比关系，但其频率分布始终小于 0.5，其初始序列段的频率分布上升幅度较大，随机性较差，不适合应用到本文所提的混沌系统中。相比之下，EMS 的频率分布始终以微小的波动幅度接近 0.5，在后续伪随机耦合中发挥着关键作用，有助于提高混沌系统的性能和安全性。

表 2　m 序列的部分反馈系数

Table 2　Partial feedback coefficients for m-sequence

LSFR-K	Maximum cycle length	Feedback coefficients(Oct)
10	1023(>10^3)	2011，2033，2157，2443，2745
14	16383(>10^4)	42103，51761，55753，60153
17	131071(>10^5)	400011，411335，444257
20	1048575(>10^6)	4000011，4001051，4004515

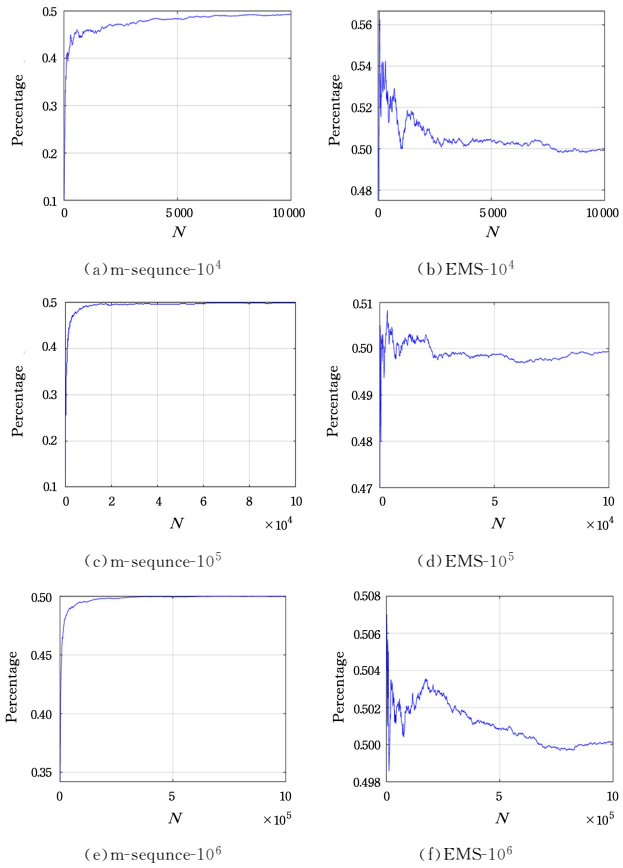


图 2 频率分布

Fig. 2 Frequency distribution

2.3.3 分布特征和自相关函数

自相关函数是衡量时间序列数据中自身相关性的重要工具，它反映了时间序列中每个时刻与之前某个时刻的相关程度，数学表示如下：

$$\rho_x(t_1,t_2)=\frac{E[x(t_1)x(t_2)]}{R_x(0)} \tag{8}$$

其中，$R_x(0)$表示序列在滞后为 0 时的函数值，通常为 1。为了比较 m 序列和 EMS 的分布特征和自相关函数的差异，采用表 2 中寄存器级数 10 对应的八进制反馈系数(2011)，使 m 序列的自相关函数达到最优值，结果如图 3 所示。

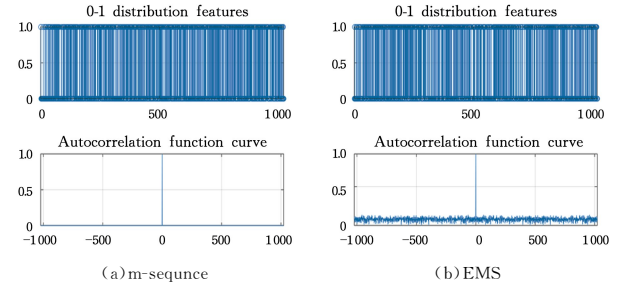


图 3 分布特征和自相关函数

Fig. 3 Distribution characteristics and autocorrelation functions

可以看出，两个序列的 0-1 分布特征没有明显差异，在零点处的自相关函数值皆为 1，m 序列在其余时间点的自相关函数值为 0。EMS 在其余时间点的自相关函数值区间为[−0.0987, 0.0890]，这意味着序列中的数据点之间的相关性近乎于 0，即序列中的一个数据点的取值与另一个数据点的取值之间没有明显的线性关系。因此，EMS 在本文所提时空混沌系统的应用中具有良好的性能和可靠性。

2.4 新型混沌映射

球腔体表示球表面空间组成的区域。根据球坐标方程，其数学表达式为：

$$\begin{cases} X=r\times\sin\varphi\cos\theta \\ Y=r\times\sin\varphi\sin\theta \\ Z=r\times\cos\varphi \end{cases} \tag{9}$$

其中，r 表示点到原点的距离，θ 表示点在 xy 平面上的极角，φ 表示点与正 z 轴之间的夹角。在球腔体方程中，将 φ 和 θ 替换为 $2\pi\sin(x_n(c_1,c_2))$和 $2\pi\sin(x_n(c_2,c_1)/(R+L))$，得到新的混沌映射：

$$\begin{cases} X(n)=r\times\sin(2\pi\sin(x_n(c_1,c_2)))\times \\ \qquad\cos(\pi\sin(x_n(c_2,c_1)/(R+L))) \\ Y(n)=r\times\sin(2\pi\sin(x_n(c_1,c_2)))\times \\ \qquad\sin(\pi\sin(x_n(c_2,c_1)/(R+L))) \\ Z(n)=r\times\cos(2\pi\sin(x_n(c_1,c_2))) \end{cases} \tag{10}$$

$$\begin{cases} c_1=1+Num \bmod R \\ c_2=1+L-c_1 \end{cases} \tag{11}$$

其中，$r\in(0,1)$表示扰动峰值，Num 表示迭代次数，x_n表示所提系统的混沌序列值。设 $Num=20\,000$，$r=0.5$，$R=L=10$，球腔体与所提混沌映射吸引子相图如图 4 所示。

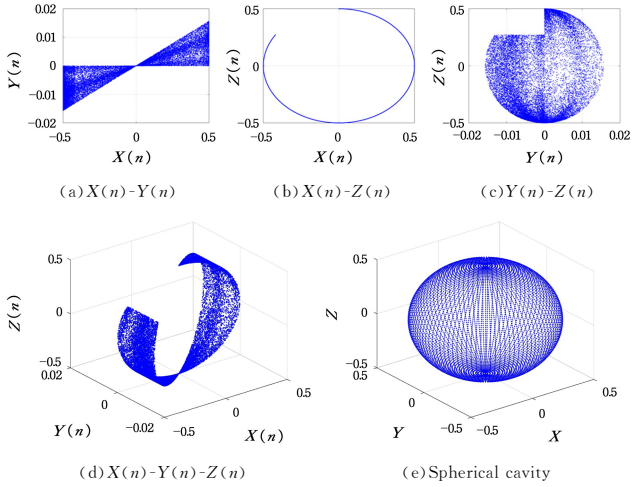


图 4 吸引子相图

Fig. 4 Attractor phase diagram

图 4(e)为球腔体吸引子相图，图 4(a)－图 4(d)分别代表相图在 3 个不同平面的投影和三维坐标轴吸引子相图。从图中可以观察到，$(X(n),Z(n))\in[-0.5,0.5]$，$Y(n)\in[-0.02,0.02]$，新型混沌映射的吸引子在球腔体表面的分布并不均匀，这并非没有益处。由于不适度的扰动可能会超出系统的调节能力，导致系统失去控制，因此，我们利用吸引子的不均匀分布，构造出强扰动和弱扰动两种扰动强度，并根据式(19)的条件判断，使系统呈现符合期望的状态，提高对系统的控制能力。

3 系统设计

基于 EMS 和二维耦合映像格，本方案提出的 2D-DCML

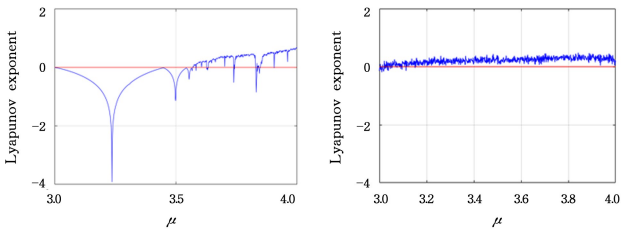
系统表达式为：

$$X_{n+1}(i,j)=\{(1-\varepsilon)f[x_n(i,j)]+\frac{\varepsilon}{4}\{f[x_n(i,a)]+f[x_n(i,b)+f[x_n(c,j)]+f[x_n(d,j)]\}\} \bmod 1 \tag{12}$$

$$\boldsymbol{X}_{n+1}=(\boldsymbol{X}_{n+1}+P_n\boldsymbol{\delta}_n) \bmod 1 \tag{13}$$

其中，n 表示系统的时间索引；$\varepsilon\in(0,1)$ 表示系统的耦合强度；$f(x)$ 作为系统的底层映射，是一维 Logistic 函数；a,b,c,d 分别表示 4 个耦合对象的纵坐标和横坐标；$i\in[1,R]$ 和 $j\in[1,L]$ 表示系统的空间索引，通常设 $R=L$；P_n 是扰动数值；$\boldsymbol{\delta}_n$ 表示第 n 次迭代时格点的扰动符号矩阵。式(12)中 $X_{n+1}(i,j)$ 表示格点值的计算，式(13)中 $\boldsymbol{X}_{n+1}$ 表示整体二维耦合映像格的计算。

为了得到所提系统的量化性能，设参数 $\varepsilon=0.9$，$R=L=10$，$f(x)$ 初始值为 0.05，对格点(6,6)输出序列的 Lyapunov 指数进行测试与比较。图 5 中的结果显示，2D-DCML 系统中所占参数空间中 95.9%的 Lyapunov 指数为正，远高于 Logistic 映射系统中的 40.5%，表明 2D-DCML 具有更复杂的轨道和混沌序列。



(a) Logistic　　(b) 2D-DCML

图 5　Lyapunov 指数

Fig. 5　Lyapunov exponent

3.1　耦合格索引方式

首先，将 EMS 按行序排列，构造 n 个与耦合映像格空间维度相同的矩阵 $\boldsymbol{M}_n$，使得系统在第 n 次迭代时的二维耦合映像格可与 $\boldsymbol{M}_n$ 相匹配。耦合对象的索引偏移量 $left$，$right$，up，$down$ 的计算式为：

$$\begin{cases} left=[bin2dec(M_n(i,:))] \bmod j \\ right=[bin2dec(M_n(i,:))] \bmod (L-j+1) \\ up=[bin2dec(M_n(:,j))] \bmod i \\ down=[bin2dec(M_n(:,j))] \bmod (L-i+1) \end{cases} \tag{14}$$

其中，$M_n(i,:)$ 与 $M_n(:,j)$ 分别代表 $\boldsymbol{M}_n$ 的第 i 行和第 j 列的比特值，通过函数 $bin2dec$ 进行十进制转化。利用模运算限制其偏移量，防止出现越界行为。可以看出，单个维度的比特值得到两个偏移量，降低了系统的时间复杂度。具体耦合格点的索引坐标计算式为：

$$a=\begin{cases} L, & left=0 \\ j-left, & \text{else} \end{cases} \tag{15}$$

$$b=\begin{cases} 1, & right=0 \\ j+right, & \text{else} \end{cases} \tag{16}$$

$$c=\begin{cases} L, & up=0 \\ i-up, & \text{else} \end{cases} \tag{17}$$

$$d=\begin{cases} 1, & down=0 \\ i+down, & \text{else} \end{cases} \tag{18}$$

其中，以 $left$，$right$，up，$down$ 是否为 0 作为判断条件来避免耦合格点坐标回位，使得耦合对象的索引值 a,b,c,d 在区间 $[1,R]$ 中动态变化。图 6 给出了耦合格点在迭代中动态演化路径的具体实例：$R=L=10$，$M_n(5,:)$ 为 1100001101，对应的十进制数是 781，$M_n(:,7)$ 为 1011111110，对应的十进制数是 766。因此，由 $x_n(i,j)(i=5,j=7)$ 确定的左偏移量 $left$ 为 4，右偏移量 $right$ 为 1，上偏移量 up 为 1，下偏移量 $down$ 为 3。最终可得出 4 个耦合对象格点的索引值 a 为 $j-4$，b 为 $j+1$，c 为 $i=1$，d 为 $i+3$。这种设计打破了耦合格的索引值的规律性，有利于能量在整个系统中的快速传递，扩大了混沌现象的范围。

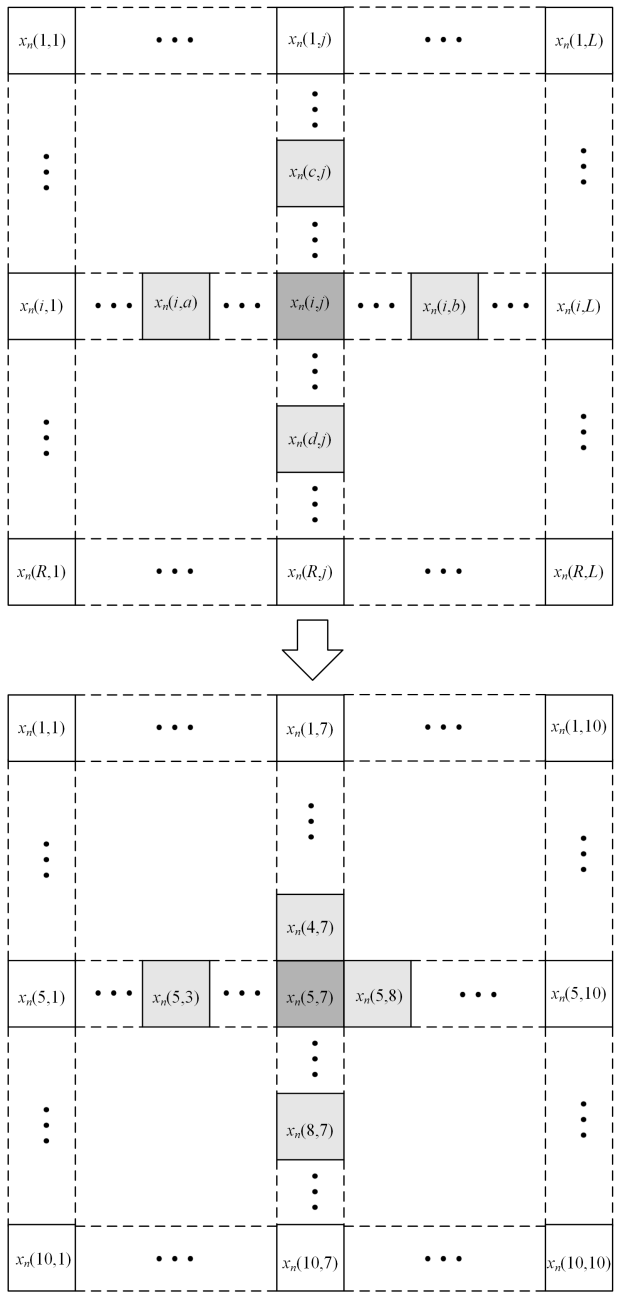


图 6　耦合方案

Fig. 6　Coupling scheme

3.2　动态扰动方案

二维耦合映像格系统的扰动方式是由扰动值 P_n 与扰动符号 $\boldsymbol{\delta}_n$ 确定的，P_n 决定扰动的大小，$\boldsymbol{\delta}_n$ 用于在迭代过程中衰

减系统内混沌序列的相关性。计算过程为：

$$P_n=\begin{cases}\varepsilon\times\sin(2\pi\sin(x_n(c_1,c_2)))\times\cos\left(\pi\sin\left(\dfrac{x_n(c_2,c_1)}{R+L}\right)\right), \\ \qquad x_n(c_1,c_2)>0.7 \\ \varepsilon\times\sin(2\pi\sin(x_n(c_1,c_2)))\times\sin\left(\pi\sin\left(\dfrac{x_n(c_2,c_1)}{R+L}\right)\right), \\ \qquad x_n(c_1,c_2)<0.3 \\ \varepsilon\times\cos(2\pi\sin(x_n(c_1,c_2))), \qquad \text{else}\end{cases} \tag{19}$$

$$\boldsymbol{\delta}_n=2(0.5-\boldsymbol{M}_n) \tag{20}$$

其中，sin 和 cos 函数的作用分别是取正弦值、余弦值，c_1 和 c_2 在式(11)中有介绍，易得 P_n 的取值范围为区间(0,ε)。x_n 的选取位置伴随变量 c_1 和 c_2 发生动态变化，导致扰动值的大小相应改变。

4 时空混沌系统性能分析

通过 EMS 构造的迭代矩阵来控制映像格的耦合模式，可以引入非线性效应，从而产生混沌系统新的动力模式。同样，利用球腔模型构建的新型混沌映射与时空混沌系统之间的相互作用，可以产生新的演化规律。利用对初始条件的敏感性，在系统中引入类球形吸引子混沌映射的扰动，可以引起系统整体状态的实质性改变，形成新的耗散机制，促进系统的能量传递和分布，从而优化系统性能。

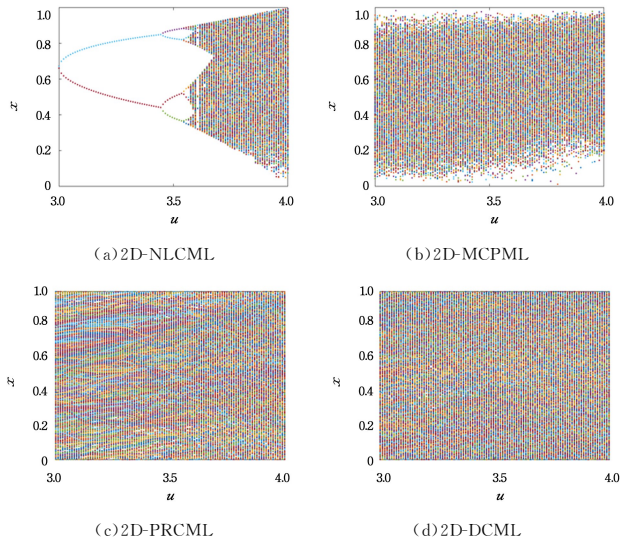
在动态特性仿真实验中，2D-DCML 系统各个参数的设定如下：系统底层映射 Logistic 的控制参数 $\mu\in[3,4]$，其初始值为 0.05；系统的耦合强度系数 $\varepsilon\in(0,1)$；系统的迭代次数 Num 设置为 10000；二维耦合映像格的空间维度 $R=L=10$。使用初始值 0.05 初始化系统的 100 个格点，通过 Logistic 函数将初始值迭代 100 次之后依次填入耦合映像格中，完成二维耦合映像格的初始化。EMS 中循环移位寄存器的长度和初始反馈多项式的数量通过式(7)计算得到 $K=20$。式(21)为从初始反馈多项式中选择的 3 个最优反馈多项式。EMS 的初始序列的位长等于 LFSR 的长度 K，随机生成的比特序列“10110010001110100100”作为初始值，完成初始化。

$$\begin{cases}g_1(x)=1+x^2+x^3+x^6+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{13}+ \\ \qquad x^{14}+x^{15}+x^{17}+x^{18}+x^{19}+x^{20} \\ g_2(x)=1+x^1+x^2+x^3+x^5+x^6+x^9+x^{11}+x^{12}+x^{13}+ \\ \qquad x^{14}+x^{15}+x^{17}+x^{19}+x^{20} \\ g_3(x)=1+x^1+x^2+x^3+x^5+x^7+x^8+x^{12}+x^{13}+ \\ \qquad x^{14}+x^{15}+x^{19}+x^{20}\end{cases} \tag{21}$$

为了便于观察所提系统的性能，将基于 Arnold 映射的二维非线性耦合映像格系统(Two-Dimensional Nonlinear Coupled Map Lattices，2D-NLCML)[28]、基于伪随机耦合和 PWLCM-Sin 映射的二维混合伪随机耦合 PS 映像格系统(Two-Dimensional Mixed pseu-do-random Coupling PS Map Lattice，2D-MCPML)[20]、基于分区初等元胞自动机的二维动态伪随机耦合映射格系统(Two-Dimensional Dynamic Pseudo-Random Coupled Map Lattices，2D-PRCML)[22]作为对比进行分析。采用了原文中的参数设置：将 2D-NLCML 系统中的控制参数 p 设为 12，q 设为 7，使其中的 Arnold 映射处于混沌状态；2D-MCPML 与 2D-PRCML 系统中的耦合强度参数 ε 设为 0.5，其他参数设置与 2D-DCML 保持一致。

4.1 分岔图

分岔图用于观察和描述系统行为的变化，特别是在具有非线性行为的混沌系统中。通过绘制输入参数与系统状态之间的关系来演示系统的动态行为，通过观察潜在的分叉现象来衡量系统在不同参数范围内可能发生的周期性变化。通过观察分岔图中点的密集分布和分形结构，可以推断系统在该参数范围内呈现出的混沌行为。混沌系统的遍历行为是指系统的轨迹能够覆盖相空间中的不同区域而不会陷入有限状态。一般情况下，对于单个混沌系统产生的小数序列，通过迭代后能够使序列的值在区间(0,1)上均匀分布，并且能够覆盖整个区间，则认为该混沌系统具有较好的遍历性。在仿真对比中，耦合强度参数统一设为 0.5，均以格点(6,6)生成的混沌序列作为分析对象，各系统的分岔图如图 7 所示。



(a)2D-NLCML (b)2D-MCPML

(c)2D-PRCML (d)2D-DCML

图 7 分岔图

Fig. 7 Bifurcation diagram

图 7 中，分岔图的横轴与纵轴分别表示控制参数和混沌序列的取值空间，数据点代表系统的状态。在图 7(a)中，2D-NLCML 借助非线性运算实现了非近邻耦合方案，改进了传统的固定耦合方式，构建出灵活的耦合格点选择。然而控制参数 $\mu\in(3,3.5)$时存在两个明显的周期点，说明系统的非周期性有待提高。在 $\mu>3.6$ 时才逐渐进入混沌状态，表明系统的能量传递速度较慢，且混沌序列值的分布在整个数据集空间的占比很小，说明系统的遍历性相对较差。在图 7(b)中，2D-MCPML 耦合格索引在系统迭代过程中会发生变化，有助于提升能量在整个系统中的传递速度。该系统在控制参数 μ 的整个值域都处于混沌状态，相较于 2D-NLCML 有较大程度的提高。然而混沌序列值不能覆盖整个值域空间，处于值域边缘的点很少，说明该系统的遍历性还有待提高。在图 7(c)中，2D-PRCML 利用分区初等元胞自动机的迭代结果来选择耦合对象，有效地提高了系统的复杂度，混沌序列值遍布整个分布空间，相较于 2D-MCPML，改善了系统的遍历性。控制参数 μ 在(3.57,4)内时系统处于全混沌状态，是由于 Logistic

映射本身具有良好的非周期特性。然而，在 $\mu\in[3,3.57]$ 区间内，系统的分岔图存在不规则线状的轨道，意味着该系统的混沌特性仅在特殊的固定点上出现，系统的伪随机性受到限制。而在图 7(d)中，得益于 EMS 提供的伪随机耦合方法以及添加的扰动，2D-DCML 在控制参数 μ 的整个值域内没有表现出明显的周期窗口，始终处于混沌状态，混沌序列值覆盖整个分布空间。因此相较于以上系统，2D-DCML 具备更好的非周期性，更强的遍历性，以及更优的混沌序列伪随机性。

4.2 LE 指数和 K 熵

李雅普诺夫指数(Lyapunov Exponent，LE)是评估动力系统混沌状态的一个重要指标[29]，常用于衡量混沌系统中相邻轨道在时间演化过程中的指数增长率，并且被作为确定系统敏感依赖性和混沌程度的手段。LE 的正值表示系统的指数敏感依赖性和混沌行为，负值则表示系统的收敛性和稳定性，LE 的值越高，系统的混沌性质和非周期性越明显[30-31]。离散动力系统 LE 的表达式为：

$$\lambda=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n}\ln\left|\frac{\mathrm{d}F(x_i)}{\mathrm{d}x_i}\right| \tag{22}$$

其中，i 表示离散时间步，$F(x)$表示动力系统的演化函数，λ 为该动力系统的 LE。对于高维时空混沌系统，采用 Wolf 方法[32]可以减少计算资源和内存的占用空间。Wolf 方法不仅可以通过度量轨迹间的局部稳定性来估计 LE，而且可以利用系统演化产生的序列来计算 LE。

在动力学分析中，可以使用 K 熵密度(Kolmogorov-Sinai Entropy Density，KED)和 K 熵阔度(Kolmogorov-Sinai Entropy Breadth，KEB)呈现混沌系统的时空特征。其中，KED 表示系统在相空间中的局部复杂度[33]，而 KEB 表示系统在整个相空间中的整体复杂度[34]。KED 与 KEB 的表达式为：

$$h=\sum_{i=1}^{R}\sum_{j=1}^{L}\lambda^{+}(i,j)/RL \tag{23}$$

$$\lambda^{+}(i,j)=\begin{cases}\lambda^{+}(i,j), & \lambda^{+}(i,j)>0\\ 0, & \lambda^{+}(i,j)\leqslant 0\end{cases} \tag{24}$$

$$hu=\sum_{i=1}^{L}\sum_{j=1}^{L}\frac{L^{+}_{(i,j)}}{L^{2}} \tag{25}$$

$$L^{+}_{(i,j)}=\begin{cases}1, & \lambda^{+}(i,j)>0\\ 0, & \lambda^{+}(i,j)\leqslant 0\end{cases} \tag{26}$$

其中，$\lambda^{+}(i,j)$代表统计模型中正的 LE；h 为基于所有正 LE 计算得到的混沌系统指标 KED，用于评估系统的局部混沌程度。当 h 的数值为正时，系统处于混沌状态，随着 h 数值的增大，系统状态的指数敏感性提升。$L^{+}_{(i,j)}$ 表示 LE 为正的格点数量。hu 代表 KEB，LE 为正的格点数越多，系统中混沌状态的比例越大，hu 的值越大，系统的整体混沌性和复杂性也越高，系统的动力学行为就越难以预测。各系统的 h 和 hu 在不同控制参数与耦合系数下的取值如图 8 和图 9 所示。

图 8 中，控制参数 μ、耦合强度 ε、K 熵密度 h 分别对应 x，y，z 轴。从耦合强度方面分析：在 2D-NLCML 中，当 $\alpha\in[0.001,0.01]$时，存在 $h=0$ 的点，系统处于周期状态；当 $\varepsilon\in(0.5,1]$时，KED 的值基本都小于 0.5，系统处于弱混沌状态。2D-MCPML 和 2D-PRCML 系统对此有所改善，系统的 KED 在整个参数区间上都为正值，且没有出现低值的现象，但是 K 熵密度分布大小并不均匀，说明系统的混沌状态并不稳定。从统计数据上看，在参数对的控制下，2D-NLCML，2D-MCPML，2D-PRCML，2D-DCML 的 KED 最小值分别为 0，0.2153，0.4266，0.7928，平均值分别为 0.0958，0.7066，0.7034，0.9032，处于 0.8 以上的占比分别为 0，26.24%，25.60%，99.52%。由此可见，2D-DCML 系统相比其他 3 种系统具备更高的复杂度、更难预测的混沌行为，以及更优的混沌特性。

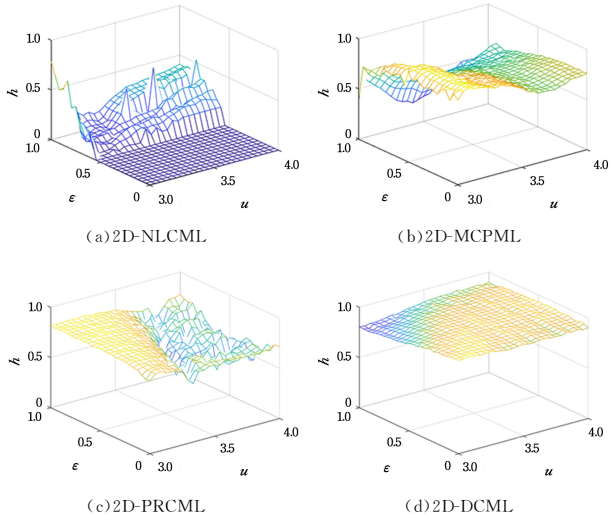


图 8 K 熵密度

Fig. 8 K-entropy density

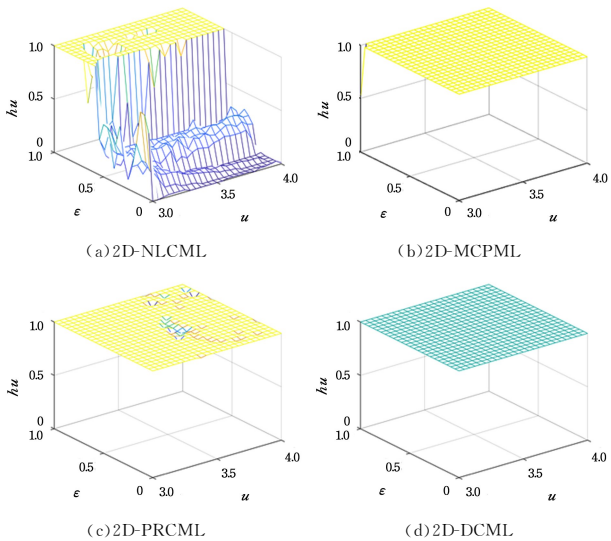


图 9 K 熵阔度

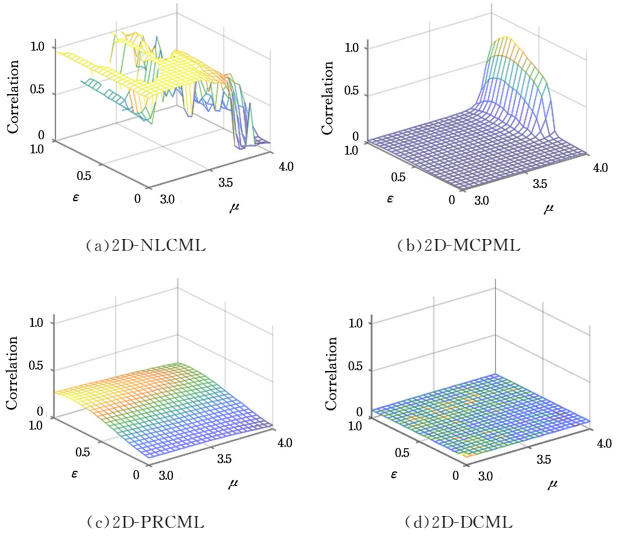
Fig. 9 K-entropy breadth

图 9 给出了各系统的 K 熵阔度值。从耦合强度方面分析：在 2D-NLCML 中，仅当 $\varepsilon\in(0.6,1]$时，系统的 KEB 才存在等于 1 的值，即 $\varepsilon<0.6$ 时，系统中的混沌序列更趋向于有序的状态；2D-MCPML 与 2D-PRCML 中均存在不等于 1 的 hu。统计数据显示：在参数对 μ 和 ε 的作用下，2D-NLCML，2D-MCPML，2D-PRCML，2D-DCML 各系统中 K 熵阔度值为 1 的占比分别为 36.16%，99.84%，92.80%，100%。由此可见，2D-DCML 系统参数空间范围内所有格点均处在强混沌状态。

4.3 相关性分析

为了评估二维耦合映像格中格点序列之间的线性相关

性，本文采用了 Pearson 相关系数来对序列间的依赖关系进行分析，通过控制参数空间范围内的不同参数来计算相关系数。如果不同格点序列之间的相关性较低，说明它们的演化路径相对独立，这意味着在密码系统应用中难以恢复出原始数据信息。因此，分析不同格点序列间的相关性可以揭示时空混沌系统的动力学特性和复杂性，对于设计高效安全的密码系统具有关键意义。图 10 展示了各系统在相同条件下的皮尔逊相关系数。



(a)2D-NLCML (b)2D-MCPML

(c)2D-PRCML (d)2D-DCML

图 10 相关性分析

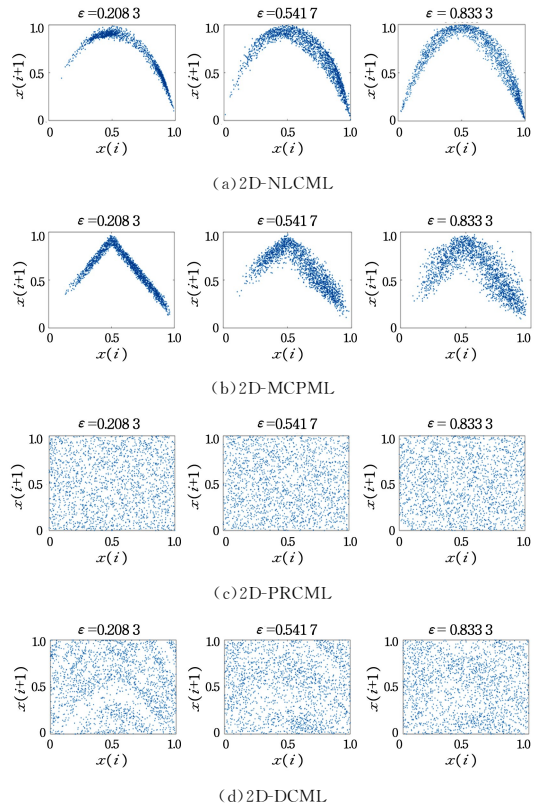
Fig. 10 Broad correlation analysis

在工程领域中，当皮尔逊系数等于 1 时，说明两条序列是完全正相关的，只有相关系数小于 0.3 时，序列之间才相互独立，被认为没有相关性[35]。在图 10 中，2D-NLCML 系统的相关系数大多都大于 0.5，甚至部分等于 1；2D-MCPML 与 2D-PRCML 系统对此进行了优化，但系统的相关系数值在部分参数对的控制下波动幅度较大，序列之间的独立性有待进一步提高。统计数据显示：2D-NLCML，2D-MCPML，2D-PRCML，2D-DCML 系统中相关系数值小于 0.1 的占比分别为 1.28%，90.72%，19.84%，100%，特别是 2D-DCML 系统的相关系数平均值达到 0.0834。所提系统混沌序列之间的线性相关性相对较弱，攻击者很难通过少数格点的输出结果来推导其余的密钥信息，保障了密码系统的安全性。

4.4 回归映射和频率分布

在密码系统中，混沌序列的分布均匀性是衡量密钥流安全性和抗攻击能力的重要依据，系统的输出序列不均匀分布会削弱密码系统的抗干扰能力。因此，利用回归映射和频率分布来评估混沌系统生成序列的均匀性是一种有效的方法，可以进一步验证密码系统的安全性。回归映射的形状和分布可以揭示系统的非线性特性和混沌程度，耦合映像格输出序列的频率分布可以进一步验证系统的均匀性和随机性。回归映射分析攻击可以通过控制参数和混沌系统的动力学行为对生成序列的影响，推断出混沌系统的初始条件、非线性函数形式等，构建回归模型，并利用历史序列数据进行参数估计，从而预测出系统后续的输出序列。回归映射图中各点之间的平均间隔距离越大，分布越分散，对密码破解技术的抵抗能力越强。因此，系统是否能够抵御回归映射分析攻击可以通过回归映射图的分布特性得出。

本方案选择二维耦合映像格中坐标为(6,6)的格点进行评估，控制参数 μ 的值设为 3.9，ε=0.2083，0.5417，0.8333。迭代 15000 次后，各系统的回归映射如图 11 所示。



(a)2D-NLCML

(b)2D-MCPML

(c)2D-PRCML

(d)2D-DCML

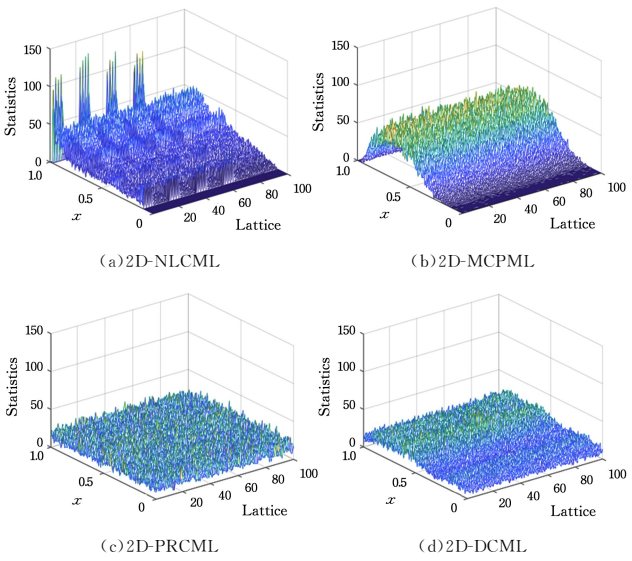
图 11 回归映射

Fig. 11 Regression mapping

在图 11 中，2D-NLCML 系统的回归映射分布始终集中在抛物线附近；2D-MCPML 系统的分布则靠近一条折线；2D-PRCML 系统改善了这种状况，但在耦合系数处于低值的情况下，仍存在较为明显的集中区域。随着耦合系数的增大，前两个系统中回归映射的点逐渐分散，但在相空间中的分布仍不均匀。2D-DCML 系统的回归映射图中没有明显的密集区域，点与点之间的距离相对均等，类似于均匀的噪点点阵，能够有效抵抗回归映射分析攻击。

混沌序列的频率分布特征可用于检验序列信息抵抗穷举搜索攻击的能力。本方案通过统计序列值域的分段分布，控制参数 μ=3.9，耦合系数 ε=0.8333，各个系统迭代 7000 次，选择各格点序列尾部 5000 个元素，降低初始条件的影响，将序列的值域平均划分为 300 个区间，统计每一区间序列元素的数量。各系统生成序列的频率分布如图 12 所示。

图 12 中的 x，y，z 轴分别代表格点值域[0,1]的分段区间、二维耦合映像格的格点总数和格点序列值在各个区间的元素数量。其中，2D-NLCML 系统生成的序列值大多分布在高值域区，2D-MCPML 系统则集中在 0.65 附近，并且两者的序列值落在区间[0,0.1]的个数几乎为 0；2D-PRCML 系统和 2D-DCML 系统的序列频率在各个值域区间内分布相对均匀，意味着其构造出的密码算法的粗糙度优于另外两个系统。



(a)2D-NLCML (b)2D-MCPML

(c)2D-PRCML (d)2D-DCML

图 12 频率分布

Fig. 12 Frequency distribution

4.5 NIST 测试

NIST SP800-22 是国家标准与技术研究院(NIST)开发的一种用于统计随机性测试的标准，该标准通过检测序列中的非随机特征来确定序列的随机性，目前被广泛应用于各种随机性统计测试[36]。NIST 共含有 15 个检测项，通过不同的统计特性提供全面而细致的随机性评估，它的评估准则为：通过的样本总量具有上下界，每个检测项计算出来的 P 值大于显著性水平 $\alpha\in[0.001,0.01]$ 表示通过。为验证时空混沌系统生成序列的优良性，将 α 设置为峰值 0.01，意味着该测试项具有 99%的可信度；如果 $l\geqslant 1\times 10^6$，说明被测试序列是随机的。

在本次测试中，2D-DCML 系统的初始条件为：控制参数 μ 设置为 3.999；耦合系数 $l\geqslant 1\times 10^6$ 设为 0.5；完成 15 个检测项的样本序列的比特长度要求 $l\geqslant 1\times 10^6$，将系统迭代 1 020 000 次，并选取尾部 1×10^6 次迭代产生的混沌序列，以尽量减小初始值的影响。将长度设置为 100×10^6，格点值在区间(0,1)的序列通过式(27)量化为 NIST 测试所要求的二进制序列。

$$y=unit32\{floor[(2^{32}-1)x]\} \tag{27}$$

其中，x 表示混沌序列，y 表示量化后的比特序列，$floor$ 是向下取整函数，$unit32$ 是数据类型转换函数。分别对得到的 32 个长度为 1×10^8 的二进制数据样本进行 NIST 测试。测试发现，2D-DCML 系统生成的 32 个数据样本的 15 项测试均达到了显著性水平 α 的统计假设检验，其中一个样本集的 100 组序列的 NIST 测试结果如表 3 所列。

表 3 列出了序列经过 15 项测试后计算得到的 P 值以及 100 组数据的通过占比。根据检测标准，若 100 组数据中通过测试的数据组不少于 96 组，则该检测项被视为通过[37]。表中所有测试集的 P 值均大于 0.01，且通过测试的数据组比例满足要求，表明 2D-DCML 系统生成的混沌序列具有良好的伪随机性，在密码算法和伪随机数生成器等方面有较高的应用价值。

表 3 NIST 随机性测试结果

Table 3 NIST randomness test results

No	Statistical-test	*P-value*	*Proportion*
1	Frequency	0.911 413	98/100
2	BlockFrequency	0.883 171	97/100
3	CumulativeSums 1	0.834 308	98/100
	CumulativeSums 2	0.514 124	99/100
4	Runs	0.304 126	98/100
5	LongestRun	0.419 021	100/100
6	Rank	0.162 606	98/100
7	FFT	0.090 936	100/100
8	NonOverlappingTemplate *	0.699 313	97/100
9	OverlappingTemplate	0.171 867	98/100
10	Universal	0.798 139	99/100
11	ApproximateEntropy	0.657 933	98/100
12	RandomExcursions *	0.170 294	97/100
13	RandomExcursionsVariant *	0.041 438	98/100
14	Serial 1	0.678 686	100/100
	Serial 2	0.191 687	100/100
15	LinearComplexity	0.419 021	99/100

注：带“*”表示多个同类测试集中最低的通过率。

4.6 计算复杂度分析

计算复杂度分为时间复杂度与空间复杂度，常用来评估算法的性能。通过分析算法在输入规模增长时所需的时间和空间资源的增长率，可以选择最优算法进行性能优化，并预测算法在处理大规模问题时的执行时间，以提高程序的执行效率。对于时间复杂度，本文提到的 4 个时空混沌系统都是通过二维耦合映像格的方式迭代输出混沌序列。这些系统的运行都需要 3 个嵌套的“for”循环操作来完成，Logistic 映射的时间复杂度为 O(1)，故以上系统的时间复杂度同为 O($RLNum$)，这意味着对于格点数确定的混沌系统，时间复杂度会随着迭代次数 Num 的增加而线性增长。对于空间复杂度，与 2D-NLCML 和 2D-MCPML 系统不同，2D-PRCML 需要借助 ECA 的迭代值定位耦合格，2D-DCML 需要借助 EMS 来定位耦合格。忽略常数项的影响，以上系统的空间复杂度为 O($RLNum$)。

本方案的配置信息为：Intel © Corei5-8300H CPU@2.30GHz、NVIDIA GeForce GTX 1060 显卡、8GB 内存以及 Windows 10 操作系统。使用 MATLAB R2021b 软件运行以上 4 个系统；控制参数的并行数设置为 1，仿真 100 个格点迭代 999 次的时空混沌系统，每个系统的仿真重复运行 10 次。计算各系统开始执行到结束的平均时间间隔和总的空间占用量，结果如表 4 所列。

表 4 计算复杂度分析结果

Table 4 Computational complexity analysis results

2D-System	*Time*/s	*Space*/MB
NLCML	2.958 6	0.269 5
MCPML	4.518 5	0.285 1
PRCML	4.973 6	0.280 2
DCML	3.907 1	0.291 0

2D-DCML 系统是通过事先生成的 EMS 来确定耦合格的选择，混沌系统的时间消耗主要取决于耦合格的选择与系统迭代次数，因此本文所提系统的消耗时间比 2D-MCPML 和 2D-PRCML 少。尽管 2D-DCML 需要额外的空间来存储 EMS，导致其空间占用略高于其他 3 种系统，但现代计算机可以轻松

处理稍微增加的存储需求，而不会对性能产生明显的影响。因此，所提系统能够在相同时间和空间资源内生成更多的混沌序列，进一步应用到S盒的构造以及分组密码中。

结束语 本文提出了一种基于m序列和球腔体的二维动态耦合映像格系统，旨在优化和改善传统2D-CML系统的动力学退化行为以及较高的序列相关性等现象。

首先，本文通过引入最佳反馈多项式替换的方法，对m序列进行改进和拓展，构建了EMS。在m序列和EMS的性能对比中，借助均衡性、自相关函数和线性复杂度等测试方法验证了EMS的随机性、安全性和抗线性攻击能力。其次，通过EMS构造的迭代矩阵确定了当前格点的耦合对象和扰动符号。再次，以球腔体为灵感构建了新的混沌映射，该映射以所提系统的混沌值为基底，构造了分段可调节的扰动函数，以使系统处于符合期望的状态。最后，通过分析动态特性发现：2D-DCML系统在LE图谱中正值占比为95.9%；在分岔图中呈现出良好的非周期性和遍历性；其K熵密度值处于0.8以上的占比为99.52%；所提系统拥有良好的均匀性，并且能够有效地抵御回归映射分析攻击；其生成的混沌序列间相关系数的均值达到了0.083 43，表明其序列之间的独立性明显高于其他系统。所提系统经过量化处理后的混沌序列成功通过了NIST测试，证明该系统生成的混沌序列具有良好的随机性。

综上，2D-DCML系统具有较强的混沌特性和密码安全性，在S盒的构造和图像加密上具有不错的应用潜力。

参 考 文 献

[1] ZHENG J, HU H P. A highly secure stream cipher based on analog-digital hybrid chaotic system[J]. Information Sciences, 2022, 587: 226-246.

[2] PENG J J, ZHU C X, JIANG D H. A new 2D-ASC chaotic system and its image encryption applications[J]. Modern Physics Letters B, 2023, 37(10): 2350009.

[3] QIN M H, LAI Q. Extreme multistability and amplitude modulation in memristive chaotic system and application to image encryption[J]. Optik, 2023, 272: 170407.

[4] ZHOU Z Q, XU X M, YAO Y X, et al. Novel multiple-image encryption algorithm based on a two-dimensional hyperchaotic modular model[J]. Chaos, Solitons & Fractals, 2023, 173: 113630.

[5] ZHOU S, QIU Y Y, QI G Y, et al. A new conservative chaotic system and its application in image encryption[J]. Chaos, Solitons & Fractals, 2023, 175: 113909.

[6] WANG Y, MA J B, CHEN Y, et al. New pseudorandom number generator based on spatiotemporal chaos[J]. Computer Engineering and Applications, 2018, 54(11): 97-102.

[7] ZHAO G, MA Y J, CHEN L, et al. Design of Dynamic S-Box Based on Perturbed Spatiotemporal Chaotic System[J]. Acta Electronica Sinica, 2022, 50(8): 2037-2042.

[8] ZHOU S, QIU Y Y, WANG X Y, et al. Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box[J]. Nonlinear Dynamics, 2023, 111(10): 9571-9589.

[9] DA SILVA S S, CARDOSO M, NARDO L, et al. A New Chaos-Based PRNG Hardware Architecture Using the HUB Fixed-Point Format[J]. IEEE Transactions on Instrumentation and Measurement, 2023, 72: 1-8.

[10] LIU H F, ZHOU X F, LIANG X L, et al. Image encryption algorithm based on multiple chaotic systems[J]. Journal of Shaanxi University of Science & Technology, 2022, 40(1): 188-195.

[11] FLORES V A, GARCÍA G E E, INZUNZA G E, et al. Implementing a chaotic cryptosystem in a 64-bit embedded system by using multiple-precision arithmetic[J]. Nonlinear Dynamics, 2019, 96(1): 497-516.

[12] LAI Q, YANG L, CHEN G. Design and Performance Analysis of Discrete Memristive Hyperchaotic Systems With Stuffed Cube Attractors and Ultraboosting Behaviors[J]. IEEE Transactions on Industrial Electronics, 2023, 71(7): 7819-7828.

[13] NING H, ZHAO G, LI Z Y, et al. A novel method for constructing dynamic S-boxes based on a high-performance spatiotemporal chaotic system[J]. Nonlinear Dynamics, 2024, 112(2): 1487-1509.

[14] ZHANG Y Q, HE Y, WANG X Y. Spatiotemporal chaos in mixed linear-nonlinear two-dimensional coupled logistic map lattice[J]. Physica A: Statistical Mechanics and its Applications, 2018, 490: 148-160.

[15] KANEKO K. Spatiotemporal Intermittency in Coupled Map Lattices[J]. Progress of Theoretical Physics, 1985, 74(5): 1033-1044.

[16] ZHAO G, PAN Z, MA Y J, et al. A Novel One-Dimensional Migration-Coupled Mapping Lattice System and Its Dynamic Characteristics[J]. Application Research of Computers, 2023, 40(11): 3289-3293.

[17] AZAM N A, MURTAZA G, HAYAT U. A novel image encryption scheme based on elliptic curves and coupled map lattices [J]. Optik, 2023, 274: 170517.

[18] DONG Y H, ZHAO G, MA Y J, et al. A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata[J]. Information Sciences, 2022, 593: 121-154.

[19] LV Z W, SUN F Y, CAI C X. A new spatiotemporal chaotic system based on two-dimensional discrete system[J]. Nonlinear Dynamics, 2022, 109(4): 3133-3144.

[20] ZHOU P Z, DU J X, ZHOU K, et al. 2D mixed pseudo-random coupling PS map lattice and its application in S-box generation [J]. Nonlinear Dynamics, 2021, 103(1): 1151-1166.

[21] LIU Z, LIU J Y, ZHANG L Y, et al. Performance of the 2D Coupled Map Lattice Model and Its Application in Image Encryption[J]. Complexity, 2022(2): 1-18.

[22] NING H, ZHAO G, DONG Y H, et al. A Novel Two-Dimensional Dynamic Pseudo-Random Coupled Map Lattices System Based on Partitioned Elementary Cellular Automata[J]. Applied Sciences, 2022, 12(23): 12399.

[23] LAI Q, YANG L, LIU Y. Design and realization of discrete memristive hyperchaotic map with application in image encryption. [J]. Chaos Solitons Fractals, 2022(165): 112781.

[24] KANEKO K. Spatiotemporal chaos in one- and two-dimensional coupled map lattices[J]. Physica D: Nonlinear Phenomena, 1989, 37(1/2/3): 60-82.

[25] WANG X Y,ZHAO M C,FENG S J,et al. An image encryption scheme using bit-plane cross-diffusion and spatiotemporal chaos system with nonlinear perturbation[J]. Soft Computing,2023,27(3):1223-1240.

[26] ZHANG G F,ZHENG L L,SU Z P,et al. M-Sequences and Sliding Window Based Audio Watermarking Robust Against Large-Scale Cropping Attacks[J]. IEEE Transactions on Information Forensics and Security,2023,18:1182-1195.

[27] DOU Y Q,LI M. An Image Encryption Algorithm Based on Compressive Sensing and M Sequence[J]. IEEE Access,2020,8:220646-220657.

[28] ZHANG Y Q,HE Y,LI P,et al. A new color image encryption scheme based on 2DNLCML system and genetic operations[J]. Optics and Lasers in Engineering,2020,128:106040.

[29] KANTZ H. A robust method to estimate the maximal Lyapunov exponent of a time series[J]. Physics Letters A,1994,185(1):77-87.

[30] LI S L,LIU Y Z,REN F Y,et al. Design of a High Throughput Pseudorandom Number Generator Based on Discrete Hyper-Chaotic System[J]. IEEE Transactions on Circuits and Systems II:Express Briefs,2023,70(2):806-810.

[31] SHAO S W,LI J,SHAO P,et al. Chaotic Image Encryption Using Piecewise-Logistic-Sine Map[J]. IEEE Access,2023,11:27477-27488.

[32] 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.

[33] WANG X Y,YANG J J,GUAN N N. High-sensitivity image encryption algorithm with random cross diffusion based on dynamically random coupled map lattice model[J]. Chaos,Solitons & Fractals,2021,143:110582.

[34] ZHANG Y Q,WANG X Y. Spatiotemporal chaos in Arnold coupled logistic map lattice[J]. Nonlinear Analysis:Modelling and Control,2013,18(4):526-541.

[35] DONG Y H,ZHAO G,MA Y J. Two-dimensional pseudo-random coupled map lattices system based on partitioned elementary cellular automata and its dynamic properties [J]. Journal on Communications,2022,43(1):71-82.

[36] BASSHAM I L E,RUKHIN A L,SOTO J,et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications[R]. National Institute of Standards and Technology,2010.

[37] SU Y Y,TONG X J,ZHANG M,et al. Efficient image encryption algorithm based on dynamic high-performance S-box and hyperchaotic system[J]. Physica Scripta,2023,98(6):65215.

MA Yingjie, born in 1979, Ph.D. Her main research interests include communication system and chaotic secure communication.

TIAN Yan, born in 1999, postgraduate. His main research interests include secure communication and chaotic block cipher.

(责任编辑:何杨)