基于分区初等元胞自动机的二维伪随机耦合映像格系统及其动态特性

董有恒[1]，赵耿[1,2]，马英杰[2]
（1. 北京邮电大学网络空间安全学院，北京 100089；2. 北京电子科技学院网络空间安全系，北京 100071）

摘 要：针对基于耦合映像格的时空混沌系统中，某些控制参数会导致弱混沌的现象，以及系统生成序列频率分布不均的情况，提出了一种基于分区初等元胞自动机的二维伪随机耦合映像格系统。首先，基于初等元胞自动机，设计了高维的分区初等元胞自动机。然后，根据该高维自动机的输出，实现了伪随机的耦合方案，同时将自动机的输出作为扰动添加至时空混沌系统中。利用 K 熵、分岔图等对二维伪随机耦合映像格系统的动态特性进行了对比分析，同时对系统生成序列的分布特性、相关性以及随机性进行了研究。结果表明，该系统建立了更强更广泛的混沌特性，拥有良好的复杂性、遍历性和非周期性。此外，该系统生成的序列具有更均匀的分布和序列之间更低的相关性，并拥有良好的伪随机性。因此，二维伪随机耦合映像格系统在密码系统和混沌保密通信中具有广阔的应用前景。

关键词：时空混沌系统；耦合映像格；初等元胞自动机；分岔图；均匀性
中图分类号：TN918
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2022001

Two-dimensional pseudo-random coupled map lattices system based on partitioned elementary cellular automata and its dynamic properties

DONG Youheng[1], ZHAO Geng[1,2], MA Yingjie[2]
1. School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100089, China
2. Department of Cyber Space Security, Beijing Electronic Science and Technology Institute, Beijing 100071, China

Abstract: To solve the weak chaos in the spatiotemporal chaotic system based on coupled map lattices under some control parameters and the un-uniformity of sequences generated by the coupled map lattices, a two-dimensional pseudo-random coupled map lattices (2D-PRCML) system was proposed. Firstly, the two-dimensional partitioned elementary cellular automata (2D-PECA) was designed to establish pseudo-random coupling. Secondly, iterative results of 2D-PECA were utilized to perturb the 2D-PRCML system. The chaotic behaviors of the proposed system, such as the bifurcation diagram, Kolmogorov-Sinai entropy, were investigated. Moreover, the uniformity of sequences generated by the 2D-PRCML system was discussed, and the correlation coefficients between any two sequences generated by different lattices were acquired. The analyses and tests indicate that the 2D-PRCML system exhibits stronger chaotic behavior. Furthermore, the sequence generated by the proposed system possesses better uniformity, randomness, and unpredictability. The outstanding properties of the 2D-PRCML system prove that it is more suitable for applying in cryptography and chaotic secure communication.

Keywords: spatiotemporal chaotic system, coupled map lattices, partitioned elementary cellular automata, bifurcation diagram, uniformity

收稿日期：2021−10−20；**修回日期**：2021−12−31
基金项目：北京高校“高精尖”学科建设基金资助项目（No.3201017）；国家自然科学基金资助项目（No.61772047）
Foundation Items: Beijing University’s “High Quality” Discipline Construction Project (No.3201017), The National Natural Science Foundation of China (No.61772047)

0 引言

混沌系统是一类确定性的动力系统，拥有遍历性、伪随机性、不可预测性以及初值敏感性等特殊性质[1-2]。自从 Lorenz[3]于 1963 年模拟天气预报时得到第一个经典的混沌动力系统后，多种混沌动力系统和混沌映射相继涌现出来，包括 Logistics 映射[4]、Henon 映射、Chebyshev 映射[5]、帐篷映射[6]以及将多个混沌映射混杂在一起的混杂混沌系统[7-8]等。这些系统被广泛应用于多个领域，尤其是在密码学方向。因为混沌系统的不可预测性和初值敏感性与密码学的要求十分契合，所以混沌系统已经应用于密码学中的多个方面，如图像加密[9-13]、S-盒的生成[14-15]、流密码[16-18]等。然而，混沌系统在有限精度的数字系统中运行时会不可避免地出现动力学特性退化[19-21]的现象，导致系统的周期变短，伪随机性被破坏。为了解决这一问题，学者提出了大量的方案，这些方案主要分为以下三类：提高系统的运算精度[22]、将多个混沌系统进行串联[23]、添加扰动[24]，其中最有效的方法是添加扰动，而扰动系统的输出相比于扰动控制参数和输入更有效[19]。

时空混沌系统[25-28]由于利用了空间上的耦合，不同位置的混沌系统输出通过耦合能够互相扰动，从而有效削弱了动力学特性退化的影响，因此拥有更强的混沌特性，逐渐成为混沌系统的研究热点。耦合映像格（CML, coupled map lattices）系统[29-30]这一启发式的设计方案被提出后，多种基于 CML 的时空混沌系统被提出，其中包括基于一维 CML[9, 31-32]和基于高维 CML[14,17,33]的两类时空混沌系统。后者的数据吞吐量以及系统的复杂性比前者好，因此，其在 S-盒生成和图像加密等数据量要求较大的密码系统中拥有更好的适用性。基于二维 CML 的时空混沌系统设计和应用更广泛，文献[33-34]基于 Arnold 映射提出了一种二维非线性耦合映像格系统并应用于图像加密中，研究表明该系统拥有较强的混沌特性，然而在某些控制参数下，该系统依然存在弱混沌的现象，而且处于混沌状态的格子数占比并不高，此外周期窗口依然存在于它的分岔图中。Zhou 等[14]基于 PWLCM-Sin 映射提出了一种二维混合伪随机耦合映像格系统，该系统有效减少了系统分岔图中的周期窗口，增强了系统的非周期性。然而，该系统的回归映射呈现明显的集中状态，生成序列的分布并不均匀，易受到回归映射分析[35]攻击。Liu 等[17]基于分段 logistics 映射提出了一种添加了偏移量的二维耦合映像格系统，该系统有效减少了周期窗口，并且实现了生成序列的均匀化，然而，对于某一固定的格子，其每回合施加的偏移量是根据格子索引和映像格系统的大小决定的，偏移量是固定的而非变化的，因此安全性有待提升。

为了解决上述存在的问题，在先前的工作中已经提出了一种一维的伪随机耦合映像格（PRCML, pseudo-random coupled map lattices）系统[36]，但由于该系统是一维的，数据量吞吐量和应用场景有限，为了进一步改进和优化，本文基于分区初等元胞自动机提出了一种二维伪随机耦合映像格（2D-PRCML, two-dimensional pseudo-random coupled map lattices）系统，主要贡献如下。

1) 对于二维耦合映像格系统，耦合计算的过程中需要 2 个维度的格子索引，为了满足这一数据需求，本文基于全局混沌的一维初等元胞自动机[37]设计了一种分区初等元胞自动机（PECA, partitioned elementary cellular automata），该自动机的迭代结果具有良好的长周期性和伪随机性。

2) 基于 PECA 的迭代结果，设计了一种伪随机的耦合方案。该方案中对某一固定格子的耦合随着系统迭代进行不断伪随机变化。这不仅增强了系统的混沌特性，而且加快了迭代过程中系统的能量传递。

3) PECA 的迭代结果通过进制转换和归一化后，作为伪随机扰动添加至系统中。首先，由于 PECA 本质上是一个离散的动力系统，因此不存在动力学特性退化的问题，其输出作为扰动能够进一步减弱 2D-PRCML 系统的退化问题。其次，这一扰动的绝对值和符号都是根据 PECA 得到的，因此也是伪随机变化的。分析结果表明，系统的非周期性、遍历性和序列的分布均匀性均得到改善，且各格子生成的序列之间的相关性显著降低。

1 设计原理

1.1 二维耦合映像格系统

在二维时空混沌系统中，典型的二维耦合映像格（2D-CML, two-dimensional coupled map lattices）[38]系统表达式为

$$x_{n+1}(i,j)=(1-\varepsilon)f[x_n(i,j)]+\frac{\varepsilon}{4}\{f[x_n(i+1,j)]+f[x_n(i-1,j)]+f[x_n(i,j+1)]+f[x_n(i,j-1)]\} \quad (1)$$

其中，时间维度 n=1, 2, 3, …，空间维度 i=1, 2, 3, …, R 和 j=1, 2, 3, …, L，整个耦合映像格系统中格子空间大小为 RL，耦合强度 $\varepsilon\in(0,1)$，该系统的边界条件为

$$\begin{cases} i-1=R, i=1 \\ i+1=1, i=R \\ j-1=L, j=1 \\ j+1=1, j=L \end{cases} \tag{2}$$

混沌映射 $f(x)$一般为 logistics 映射，该映射的数学表达式为

$$f(x)=\mu x(1-x) \tag{3}$$

其中，控制参数 $\mu\in(0,4]$，当 $3.57<\mu\leqslant 4$ 时，该映射处于混沌状态[9]。x 的取值范围为(0,1)。很显然，这种典型的 2D-CML 系统的耦合方式是邻近耦合。

1.2　分区初等元胞自动机

元胞自动机（CA, cellular automata）的概念由 Neumann 等[39]提出。CA 是一种在空间和时间上都离散的动力系统，该系统最初用来模拟生命系统中的自我复制现象，也是自然界中复杂现象的一种简化模型[40]。它主要由元胞、元胞空间、元胞邻居和迭代规则以及边界条件等构成。

初等元胞自动机（ECA, elementary cellular automata）是一种简单的一维元胞自动机[6]。在 ECA 中，各元胞只有 2 种状态，因此它们的状态值集合可以表示为{0,1}。元胞邻居仅有 2 个，即与其紧邻的 2 个元胞。初等元胞自动机的边界条件一般是周期的，可以表示为

$$\begin{cases} i+1=1, i=L \\ i-1=L, i=1 \end{cases} \tag{4}$$

其中，i 为元胞的索引，L 为该 ECA 中元胞的总个数。在 ECA 中，一个元胞的当前状态值是由其本身和 2 个邻居的前次状态值共同决定的，因此其迭代过程可以表示为一个布尔函数，即

$$S_{t+1}(i)=f_r(S_t(i-1), S_t(i), S_t(i+1)) \tag{5}$$

其中，时间维度 t=1, 2, 3, …，空间维度 i=1, 2, 3, …, L，因此，$S_t(i)$表示第 i 个元胞在 t 时刻的状态值。布尔函数f的计算结果由迭代规则 r 决定，以 $r=150$ 为例，其计算结果如表 1 所示。

表 1 中的迭代结果 $S_{t+1}(i)$ 可表示为二进制数 10010110，将其进一步转化为十进制数即迭代规则 150。显然，在 ECA 中，输入共有 8 种，即{000,001, 010, …,111}；输出有 2 种，即{1,0}，因此迭代规则共有 2^8，即 256 种。每种迭代规则对应一种 ECA。

表 1　当 r=150 时，布尔函数 f 的计算结果

迭代结果	二进制数							
$S_t(i-1)$	1	1	1	1	0	0	0	0
$S_t(i)$	1	1	0	0	1	1	0	0
$S_t(i+1)$	1	0	1	0	1	0	1	0
$S_{t+1}(i)$	1	0	0	1	0	1	1	0

根据 ECA 迭代结果的性质，迭代规则可分为以下五类[37, 41-42]：无效规则、固定点规则、周期规则、局部混沌规则和全局混沌规则。本文中，任意 2 种全局混沌规则下的 ECA 均可用于构建二维分区初等元胞自动机（PECA, partitioned elementary cellular automata）。ECA 中的全局混沌规则如表 2 所示[37]。

表 2　　ECA 中的全局混沌规则

种类	规则编号
全局混沌	18(183), 22(151), 30(86, 135, 149), 45(75, 89, 101), 60(102, 153, 195), 90(165), 105, 106(120, 169, 225), 129(126), 137(110, 124, 193), 146(182), 150, 161(122)

PECA 是一种至少包含 2 个拥有不同迭代规则 ECA 的高维动态系统，而其中二维分区初等元胞自动机（2D-PECA, two-dimensional partitioned elementary cellular automata）可表示为

$$\begin{cases} x_{t+1}(i)=f_{r1}[x_t(i-1), x_t(i), x_t(i+1)] \\ y_{t+1}(i)=f_{r2}[y_t(i-1), y_t(i), y_t(i+1)] \end{cases} \tag{6}$$

其中，$\boldsymbol{x}$ 和 $\boldsymbol{y}$ 分别代表 2 个拥有不同转换规则 r_1 和 r_2 的 ECA。空间维度 $i\in\{1, 2, 3, \ldots, L\}$即元胞的索引，各 ECA 中元胞的总数均为 L，t 代表时间维度。由式(6)可知，在 2D-PECA 中 2 个 ECA 的迭代是同步进行的。设 r_1=102，r_2=105，L=100，且 2 个 ECA 的初始值是随机生成的布尔向量，则该 2D-PECA 的迭代 200 次后的结果如图 1 所示。

2　系统设计

基于分区初等元胞自动机和二维耦合映像格，本文提出的 2D-PRCML 系统的数学表达式为

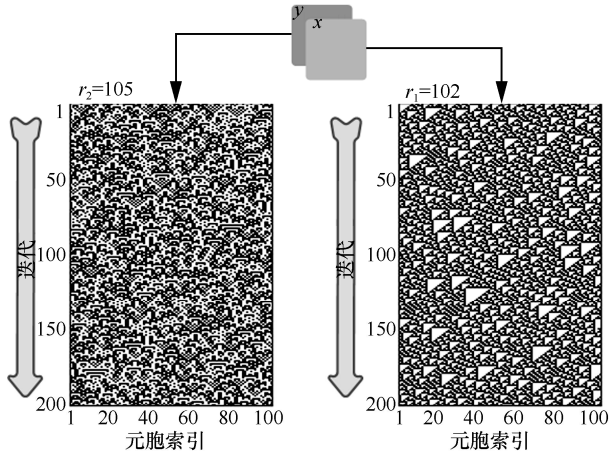

图 1　2D-PECA 的迭代 200 次后的结果（r_1=102, r_2=105）

$$x_{n+1}(i,j)=\{(1-\varepsilon)f(x_n(i,j))+\frac{\varepsilon}{4}[f(x_n(a,j))+f(x_n(b,j))+f(x_n(i,c))+f(x_n(i,d))]+0.5p_n\delta_n(i,j)\}\bmod 1 \tag{7}$$

其中，时间维度 n=1, 2, 3, …，空间维度（即格子的索引）i=1, 2, 3, …, R 和 j=1, 2, 3, …, L，一般设 R=L=m；ε 是耦合强度；f 是 logistics 映射；如式(3)所示，索引 a、b、c、d 由 2D-PECA 的迭代结果得到；p_n 是第 n 次迭代时根据 2D-PECA 计算得到的扰动值；$\delta_n(i,j)$ 是格子(i,j)在第 n 次迭代时扰动的符号，其值为−1 或 1；运算 mod 1 的目的是保留小数部分，从而保证计算结果始终在区间(0,1)上。

设 2D-PECA 中，2 个初等元胞自动机 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 各自的元胞个数 L_e 应大于 m 和 32 中的最大值，系统每迭代一次，即 n+1 时，2D-PECA 需先迭代 m 次得到 2 个布尔矩阵 $\boldsymbol{E}_1$ 和 $\boldsymbol{E}_2$。各参数详细的计算过程如下。

2.1　索引

首先，从得到的 2 个布尔矩阵 $\boldsymbol{E}_1$ 和 $\boldsymbol{E}_2$ 的中间各截取一个大小为 $m\times m$ 的子矩阵，即与耦合映像格大小相同的矩阵 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$。然后根据当前格的位置(i,j)在 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ 中搜索参与耦合的 4 个格子的索引，其计算过程可表示为

$$(a,b,c,d)=\text{search}((i,j),\boldsymbol{X},\boldsymbol{Y}) \tag{8}$$

搜索函数的运算过程如图 2 所示。图 2 中，每列代表一个元胞，有（无）阴影填充的方格代表该元胞当前状态值为 1（0），每行代表 ECA 迭代一次的结果。其中，索引 a、b 由矩阵 $\boldsymbol{X}$ 和当前格的索引(i,j)得到，即矩阵 $\boldsymbol{X}$ 第 j 行中，与第 i 个元胞最近的 2 个状态值为 1 的元胞的索引，以图 2 为例，a=i−2 和 b=i+2 可以理解为在 e_1 的第 j 次迭代结果中，与元胞 i 最近的 2 个状态值为 1 的元胞的索引被用作耦合格的索引 a 和 b。同理，可由矩阵 $\boldsymbol{Y}$ 中第 i 行，与元胞 j 最近的 2 个状态值为 1 的元胞索引得到 c 和 d 的值。

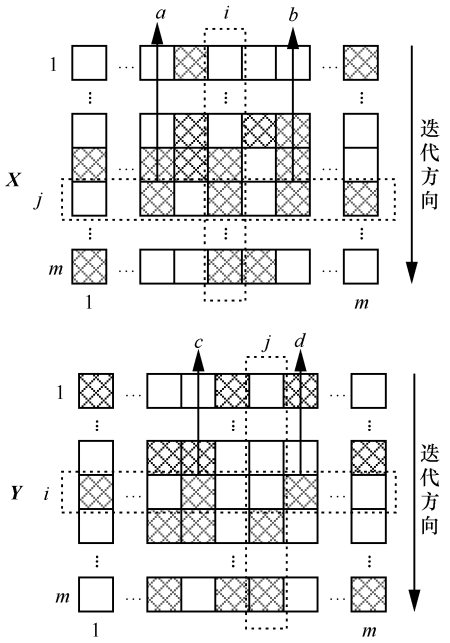

图 2　搜索函数的运算过程

每次系统进行迭代时，即 n+1 时，2D-PECA 都会迭代 m 次来更新布尔矩阵 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ 的值，而且根据第 1 节的表述，这一结果是伪随机的，所以每次系统进行迭代时，耦合格的索引 a、b、c、d 都会发生变化，且这一变化也是伪随机的。

这样做的目的如下。1) 增强系统的复杂性，提高系统的李雅普诺夫指数（LE, Lyapunov exponent），进一步提升系统的不可预测性；2) 加快系统能量的传递过程，使整个系统拥有更大范围的混沌。

2.2　扰动值 p_n

扰动值是由 2D-PECA 的第 m+1 次迭代结果得到的。2D-PECA 中 2 个 ECA 某一次的迭代结果可以看成 2 个 L_e 位的二进制数“$c_1c_2c_3\cdots c_{L_e}$”，其中 c_i（i=1,2,3,…,L_e）为第 i 个元胞当前的状态值。取所得到的二进制数的后 32 位来计算扰动值 p_n，即

$$p_n=\begin{cases}\dfrac{\text{bin2dec}(S_{\boldsymbol{x}}^{m+1}(c_{L_e-31}c_{L_e-30}\cdots c_{L_e}))}{2^{32}-1}, & n\text{ 为奇数}\\ \dfrac{\text{bin2dec}(S_{\boldsymbol{y}}^{m+1}(c_{L_e-31}c_{L_e-30}\cdots c_{L_e}))}{2^{32}-1}, & n\text{ 为偶数}\end{cases} \tag{9}$$

其中，函数 bin2dec 的作用是将二进制数转化为十进制数，S_x^{m+1} 和 S_y^{m+1} 分别代表初等元胞自动机 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 在第 m+1 次的迭代结果。显然，p_n 始终在区间(0,1)内。需要注意的是，当前 2D-PECA 第 m+1 次的迭代结果将作为整个系统下次迭代时 2D-PECA 的初始值。由于该迭代结果是伪随机的，因此得到的扰动也是伪随机的，这种伪随机扰动能够进一步削弱有限精度系统下的退化问题[19]。

2.3　扰动符号 $\delta_n(i,j)$

扰动符号是由 2.1 节中得到的矩阵 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$ 所决定的，其计算过程为

$$\delta_n(i,j)=\begin{cases}2(\boldsymbol{X}(i,j)-0.5), n\text{为奇数}\\ 2(\boldsymbol{Y}(i,j)-0.5), n\text{为偶数}\end{cases} \tag{10}$$

显然，经过计算 $\delta_n(i,j)$ 的值为 1 或−1。虽然在一次迭代的过程中，对系统中各个格子施加的扰动绝对值是相等的，均为 $0.5P_n$，但由于扰动符号的存在，使对每个格子施加的扰动正负是不同的，且系统每次迭代时 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$ 都会被 2D-PECA 的迭代所更新，因此扰动符号也是在伪随机变化的，这样可以有效降低各个格子之间的相关性。

3　性能分析

2D-PRCML 系统的各个参数设置如下：logistics 映射的控制参数 $\mu\in(0,4)$，系统的耦合强度 $\varepsilon\in(0,1)$。为了计算方便，本文设耦合映像格的空间维度 R=L=10，因此系统共有 100 个格子，令初始值 x_0=0.05，通过 logistics 映射迭代 99 次，将迭代后的结果连同初始值逐行填入 100 个格子中，完成各个格子的初始化。2D-PECA 中，初等元胞自动机 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的元胞数各为 100，两者初始值设为 100 bit 长的二进制随机数，即

$$\begin{cases}S_x^0=\text{02D1\_990D\_DF84\_2E15\_E308\_D744\_1}\\ S_y^0=\text{041C\_E93F\_6597\_1D2F\_71C4\_A442\_D}\end{cases} \tag{11}$$

其中，$\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的初始值 S_x^0 和 S_y^0 分别为 16 进制数。根据 1.2 节，本文选择全局混沌规则 102 和 105 分别作为 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的迭代规则。

除了基于邻近耦合的传统 2D-CML 系统，本文还选取了 2 个较新颖的二维时空混沌系统作为对比：基于 Arnold 映射的二维非线性耦合映像格（2D-NLCML, two-dimensional nonlinear coupled map lattices）系统[33-34]、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（2D-MCPML, two-dimensional mixed pseudo-random coupling PS map lattice）系统[14]。2D-NLCML 系统中，Arnold 映射的控制参数 p 和 q 分别设为 12 和 7，以使其处于混沌状态。2D-MCPML 系统中，参数 σ=0.5，其他参数设置和 2D-PRCML 系统相同。

3.1　耦合方案分析

各系统耦合方案对比如图 3 所示，其中，黑色格子表示当前正在运算的格子，灰色格子表示参与耦合运算的格子。如图 3(a)所示，传统的 2D-CML 系统的耦合方案是邻近耦合。当前格子与其相邻的上下左右 4 个格子进行耦合，且这种耦合是固定的不变的，即对于格子(i, j)来说，在迭代的过程中，参与耦合的 4 个格子始终为(i+1, j)、(i−1, j)、(i, j+1)、(i, j−1)。这种方案计算简单、易于实现，但能量传递方式缓慢固定，复杂性不高。

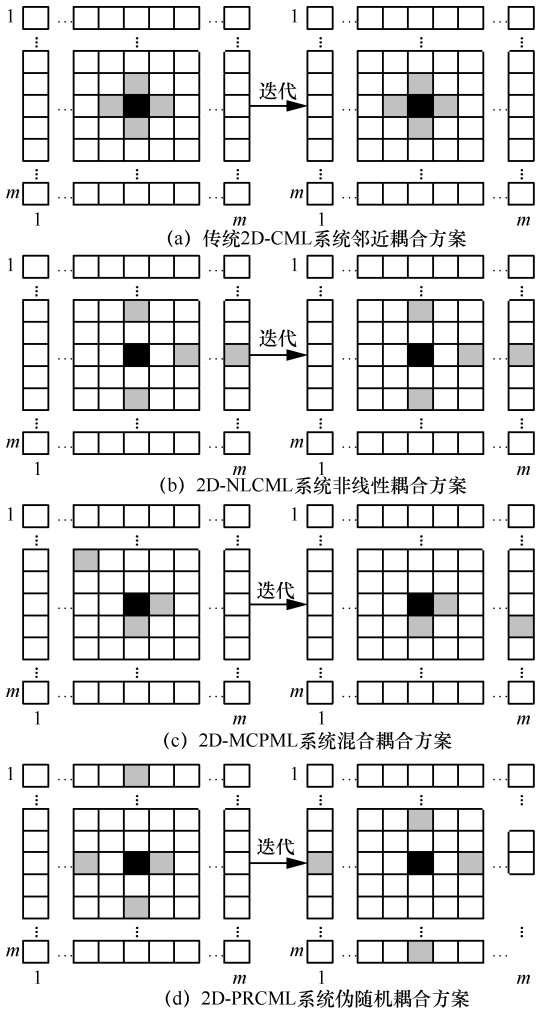

图 3　各系统耦合方案对比

在 2D-NLCML 系统中，耦合方案是由 Arnold 映射所决定的[33-34]，数学表达式为

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} i+1 \\ i-1 \end{bmatrix} (\mathrm{mod}\, R) \tag{12}$$

$$\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} j+1 \\ j-1 \end{bmatrix} (\mathrm{mod}\, L) \tag{13}$$

其中，p 和 q 为控制参数，R 和 L 分别为耦合映像格的总行数和总列数。通过上述运算可以得到与格子(i,j)耦合的 4 个格子：(a,j)、(b,j)、(i,c)、(i,d)。虽然 Arnold 映射是非线性的运算，且 p 和 q 的某些取值可以导致混沌，但在此方案中，p 和 q 是固定不变的值，且在每一次系统的迭代过程中，该映射只迭代一次，也就是说输入 i+1 不变，不管系统迭代多少次得到的耦合格始终是(a,j)。该方案只是利用非线性运算实现了非近邻的耦合，但如图 3(b)所示，耦合方案依然是固定不变的，所以对于系统混沌特性的提升是有限的。

在 2D-MCPML 系统中，耦合方案有所改进。参与耦合的格子不再是邻近或者固定的，而是随着系统迭代有所变化[14]。在该方案中，与格子(i, j)耦合的格子共有 3 个，包括相邻的 2 个格子$(i+1,j)$和$(i,j+1)$，以及一个根据格子(i, j)的当前值计算出的随机位置的格子(a, b)。计算过程如下。设耦合映像格的大小为 $R\times L$，假设格子(i, j)当前的值为 0.409 671 42，a=(40 mod R)+1, b=(96 mod L)+1。由于格子(i, j)的值随着系统的迭代不断变化，(a, b)也随之不断变化，且当该系统处于混沌状态时，这一变化将是伪随机的，如图 3(c)所示。然而，这种耦合方案依赖于系统混沌映射本身的特性，后续分析发现该方案所设计的混沌映射迭代结果分布并不均匀，所以在此基础上求出的随机耦合格其分布也是非均匀的；其次该耦合方案中依然存在邻近成分，所以对能量传递速度的提升是有限的。

本文所提出的 2D-PRCML 系统中，根据第 2 节的描述，所用的耦合方案基于 2D-PECA 的迭代结果，所选择的迭代规则又使 2D-PECA 系统处于混沌状态，由此得到参与耦合的 4 个格子位置均处于伪随机变化之中，如图 4(d)所示。该方案有效地加快了系统的能量传递速度，提高了系统的复杂性。

3.2　李雅普诺夫指数和 K 熵

LE 是衡量动力系统运行时，在相空间中邻近轨迹分离速率的一个重要参数[43-44]，通常用来评价混沌系统的不可预测性。它的数学定义为

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| \frac{\mathrm{d}F(x)}{\mathrm{d}x} \right|_{x=x_i} \tag{14}$$

其中，λ 为动力系统 $F(x)$的 LE，i 为时间维度。对于一个混沌系统来说，至少应该拥有一个正的 LE，且 LE 的值越大，说明该系统的混沌特性越强[8-10, 45]。为了不失一般性，与文献[10, 31-32]相同，本文采用 Wolf 法[43]，通过系统生成的序列来计算 LE。

K 熵密度（KED, Kolmogorov-Sinai entropy density）是计算时空混沌系统中所有正的 LE 在格子总数下的均值[46-47]，在二维时空混沌系统中，其计算式为

$$h = \frac{\sum_{i=1}^{R} \sum_{j=1}^{L} \lambda^{+}(i,j)}{RL} \tag{15}$$

其中，h 代表 KED，λ^{+}代表大小为 RL 的耦合映像格中正的李雅普诺夫指数，i 和 j 代表 LE 为正的格子索引。h 为正意味着系统中存在处于混沌状态的格子，h 的值越大，代表系统的混沌特性越强，复杂性越高。在不同的控制参数和耦合强度下，各系统的 KED 如图 4 所示。

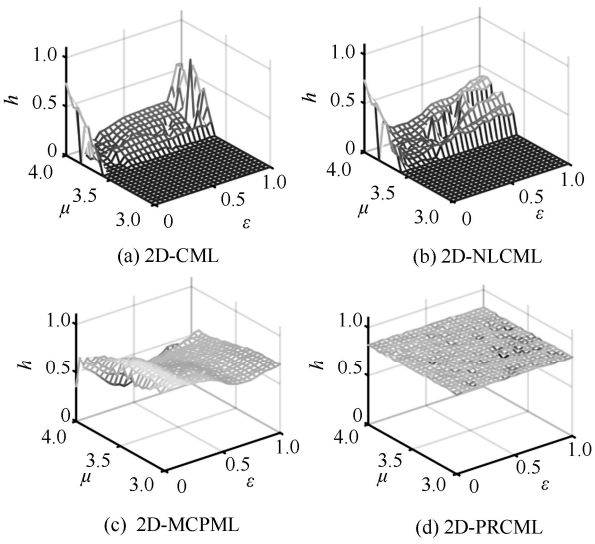

图 4　各系统的 KED

图 4 中 x、y、z 轴分别代表控制参数 μ、耦合强度 ε、K 熵密度 h。如图 4 所示，在 2D-CML 和 2D-NLCML 系统中，只有μ>3.6 时才存在正的 KED，即仅在区间 $\mu\in$(3.6, 4]时，才会存在处于混沌状态的格子，且 2D-CML 系统中，在 ε=0.2 附近有一小段弱混沌区间，在 2D-NLCML 系统中对此有所改

善，且随着 ε 的增大，KED 有所提高。在 2D-MCPML 以及 2D-PRCML 系统中，整个参数区间上 KED 均大于 0，即均存在处于混沌状态的格子。同时统计发现，图 4(c)中，仅有 9.12%的参数对(μ, ε)所对应的 KED 达到了 0.8，而在图 4(d)中，这一比例高达 99.68%。因此，可以得出结论，2D-PRCML 系统的混沌特性要远强于前三类系统。

K 熵阔度（KEB, Kolmogorov-Sinai entropy breadth）是由 Zhang 等[25,47]提出的，用来统计固定参数下时空混沌系统中处于混沌状态的格子占比，其定义为

$$\mathrm{hu}=\frac{L^{+}}{L} \tag{16}$$

其中，hu 表示 K 熵阔度，L^{+}表示系统中李雅普诺夫指数为正的格子数，L 表示系统中的格子总数。KEB 可以从空间层面上来衡量系统的混沌特性。hu 的值越大，系统中处于混沌状态的格子越多，即系统拥有越广泛的混沌特性。各系统的 KEB 如图 5 所示。与 K 熵密度相对应，图 5(a)和图 5(b)中，仅当 μ>3.6 时，2D-CML 和 2D-NLCML 系统才存在 KEB=1，即只有当 $\mu\in$(3.6, 4]时，所有的格子才有可能都处于混沌状态。统计结果表明，在图 5(a)和图 5(b)中，整个参数区间上分别仅有 28.96%和 29.76%的参数对(μ, ε)使系统所有的格子处于混沌状态，即 2D-CML 和 2D-NCML 系统所建立的混沌范围在空间上是有限的。与之相反，在图 5(c)和图(d)中，KEB=1 的比例分别达到了 99.84%和 100%，即在 2D-MCPML 和 2D-PRCML 系统中，大部分的参数对下，空间上所有的格子均能建立较强的混沌状态。

综上所述，2D-PRCML 系统相比于本文提到的其他时空混沌系统具有更强的混沌特性，KED 均值达到了 0.815 4，这也说明该系统的复杂性和不可预测性更高。同时，2D-PRCML 系统建立的混沌状态足够广泛，在整个参数范围 $\mu\in$(3, 4]，$\varepsilon\in$(0,1)中，所有的格子均能达到混沌状态。进一步地，当 2D-PRCML 应用于密码系统中时，由于具有更多的参数对(μ, ε)使系统处于不可预测的混沌状态，这大大扩展了(μ, ε)作为密钥时的密钥空间。

3.3　分岔图

分岔图是用来分析混沌系统特性的一个重要工具，描绘了混沌系统中特有的倍周期分岔现象，可以直观地衡量在不同的控制参数下混沌系统的遍历性和非周期性。

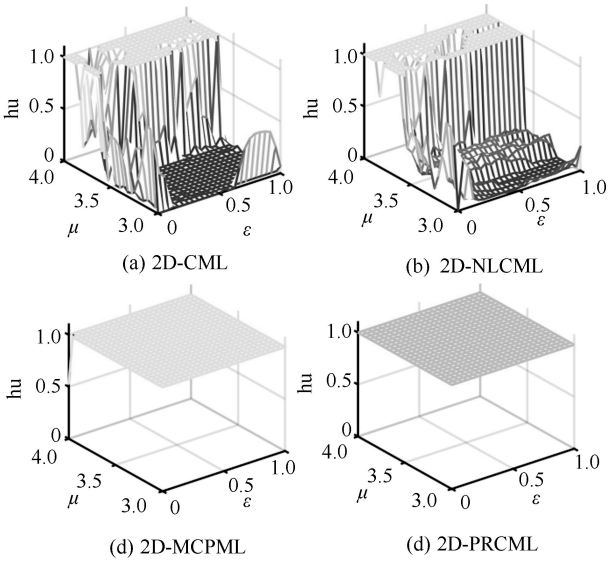

图 5　各系统的 KEB

为了进行对比分析，本文设各系统的耦合强度 ε=0.35，并选择格子(5,5)生成的序列 $\{x(i)|i=1,2,3,\cdots\}$来绘制分岔图，各系统的分岔图如图 6 所示。

显然，图 6(a)和图 6(b)在 μ<3.6 时均存在有明显的周期窗口，而 2D-CML 系统的非周期性甚至要优于 2D-NLCML，因为在 $\mu\in$(3, 3.5)时，图 6(b)明显存在 2 个固定的周期点，而在图 6(a)中，虽然有周期点，但周期点不止 2 个，因此周期长度要更长。从遍历性的角度，图 6(a)和图 6(b)仅在 μ=4 时，序列的取值才能够充满整个值域。在图 6(c)和图 6(d)中，周期窗口在整个区间 $\mu\in$(3, 4)上消失了，所以 2D-MCPML 和 2D-PRCML 系统的非周期性更好，拥有更好的不可预测性和伪随机性。此外，图 6(c)中，分岔图并没有充满 x 的整个值域[0,1]，落在最小值 0 和最大值 1 附近的点很少，这说明 2D-MCPML 系统的遍历性稍差。而在图 6(d)中，2D-PRCML 系统在整个控制参数区间 $\mu\in$(3, 4)上均有很好的遍历性，因为生成的序列能够充满整个值域[0,1]。综上所述，2D-PRCML 系统在控制参数区间 $\mu\in$(3, 4)上拥有更好的非周期性和遍历性。

3.4　分布均匀性

密码系统中要求作为密钥流或随机数的序列，其分布特性应该足够均匀。混沌系统生成序列的分布均匀性应从 2 个角度来分析：一是回归映射上的分布，二是各格子生成序列本身的频率分布特性。

研究系统的回归映射是为了判断系统能否抵

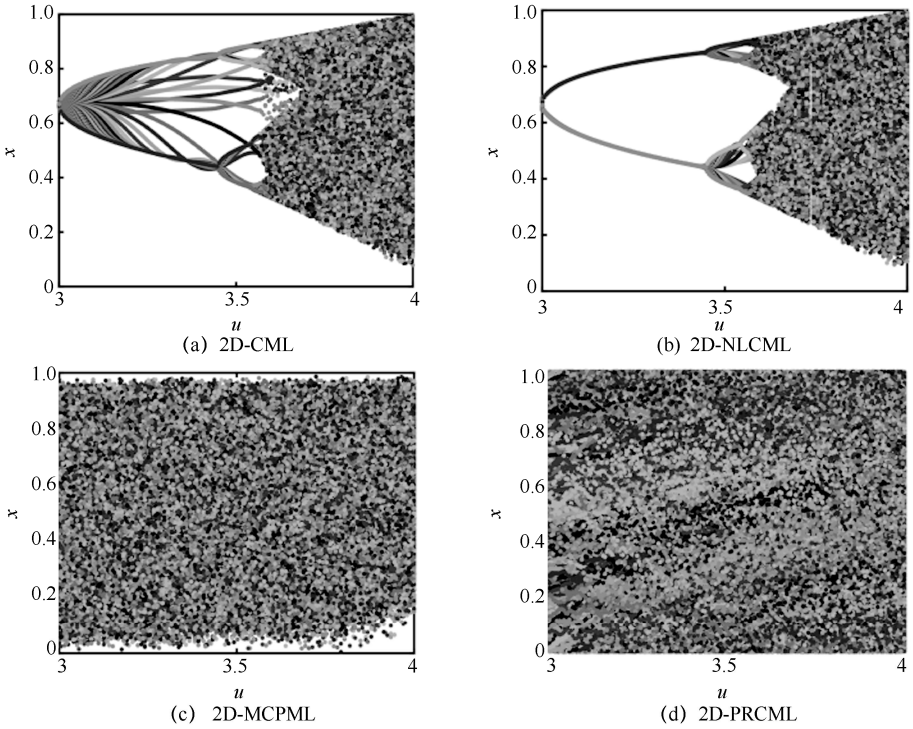

图 6 ε=0.35 时各系统的分岔图

抗回归映射分析攻击[35-36]。回归映射分析攻击是针对混沌密码系统的一种有效攻击手段，其可通过混沌系统生成的序列来估算系统的各控制参数，从而达到预测系统之后生成序列的目的。而回归映射的特征越明显，分布越集中，则系统越容易被攻破。

本文设 μ=4，选择格子(5,5)生成的序列作为代表，则各系统的回归映射如图 7 所示。

由图 7(a)～图 7(c)可知，2D-CML、2D-NLCML 系统的回归映射均集中在一条抛物线附近，而 2D-MCPML 系统的则集中在一条折线附近，且随着耦合强度 ε 的增大，回归映射中的点逐渐发散。因此，上述 3 种系统的回归映射具有 2 个特点：1) 集中在某些区域，2) 对耦合强度的变化敏感，故这 3 种系统极易受到回归映射分析攻击。图 7(d)中，2D-PRCML 系统的回归映射的分布近似于噪点的分布，没有集中的形状，同时随着 ε 的变化，回归映射依旧保持这种类似于噪点的均匀分布，因此能够很好地抵抗回归映射分析攻击。

进一步地，本文设 ε=0.625，μ=4，让每个系统迭代 6 000 次，系统中的各个格子生成长度为 6 000 的序列，去除序列中前 1 000 个元素，减少初值的影响；然后将序列的值域[0,1]平均分成 200 段，统计序列中落在每一段中的元素个数。各系统生成序列的频率分布如图 8 所示。

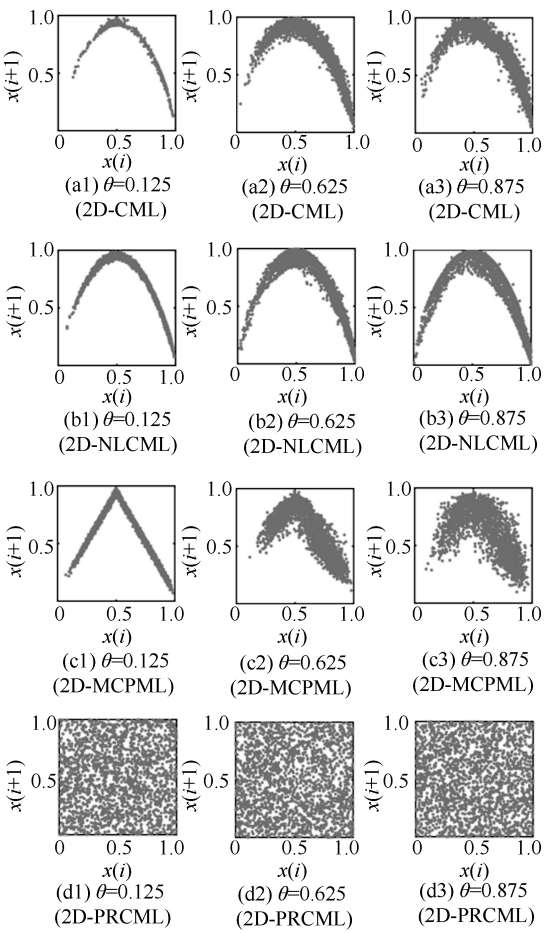

图 7 各系统在不同耦合强度下的回归映射

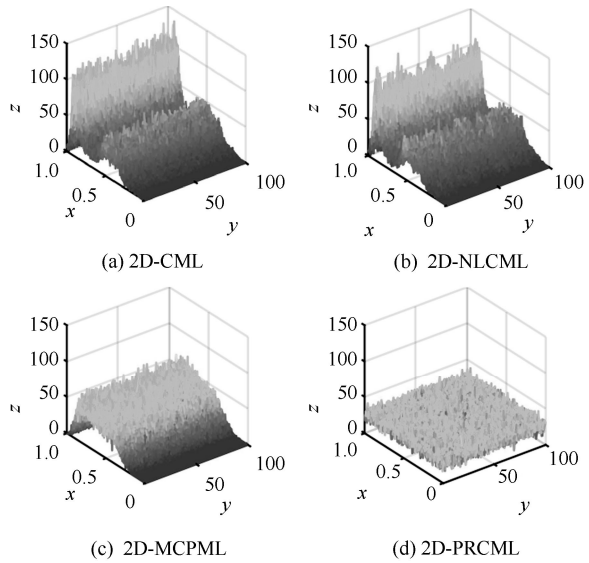

图 8　各系统生成序列的频率分布

图 8 中 x、y、z 轴分别代表在序列值域[0,1]上的分段，10×10 个格子的编号以及某一格子生成的序列在某一分段上的元素个数。显然，2D-PRCML 系统中各个格子生成序列的频率分布比其他 3 种系统更加均匀。

3.5　相关性分析

在密码系统中，本文希望同一系统同一时间生成的各个序列之间应该相互无关，在时空混沌系统中可以理解为无法通过一个或多个格子生成的序列计算推导出其他格子生成的序列。因此，研究时空混沌系统中各个格子之间的相关性对其在密码系统中的应用具有重要意义[48]。因此本文计算了各系统在不同参数对下，不同格子生成序列之间的皮尔逊相关系数的均值，相关性分析如图 9 所示。

工程上，当皮尔逊相关系数小于 0.3 时，可以认为不相关。对图 9 进行统计结果表明，在 2D-CML 和 2D-NLCML 系统中仅有 6.88%和 5.2%的参数对(μ,ε)下，各序列之间的相关系数小于 0.3。而在 2D-MCPML 和 2D-PRCML 系统中，这一比例分别达到了 91.8%和 100%。因此 2D-PRCML 系统所生成的各个序列之间的相关性很弱，在密码系统中敌手很难通过一个或多个格子的输出计算推导出其他格子的输出，即该系统的安全性较高。

3.6　NIST 随机性检测

为了进一步验证本文方案生成序列的随机性，以及其在伪随机数生成方面的应用潜力，本文引入了应用广泛，且较权威的美国国家标准技术研究所（NIST, National Institute of Standards and Technology）的随机数检测套件 SP800-22 对 2D-PRCML 系统生成的数据进行了检测[49]。

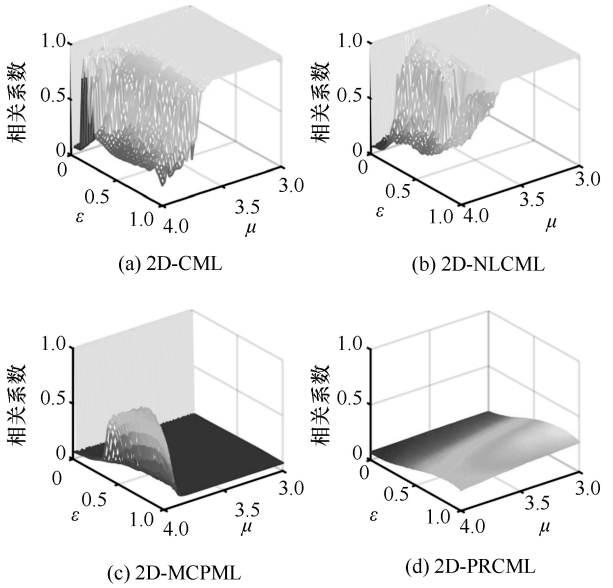

图 9　相关性分析

首先，对 2D-PRCML 生成的(0,1)的数据 $\boldsymbol{x}$ 进行量化。

$$\boldsymbol{y} = \mathrm{floor}(2^{32}\boldsymbol{x}) \tag{17}$$

其中，函数 floor(•)为向下取整函数，$\boldsymbol{y}$ 为无符号的 32 位数。截取 $\boldsymbol{x}=\{x_1, x_2,\cdots, x_{1000000}\}$量化后生成的序列 $\boldsymbol{y}$ 中每个元素的后 16 位，生成 16 条长度为 10^6 的 0,1 序列进行随机性检测，并检测 100 组数据检测结果如表 3 所示。

表 3 列出了量化后 100 组数据的后 16 位生成的伪随机数的检测结果。本文取显著性水平 α=0.01，即当每项测试的结果 p>0.01 时，则通过该测试，这意味着该序列为随机序列的置信度水平为 99%。而表 3 中列出了 100 组测试数据的通过率，根据文献[24, 50]，100 组数据中有不少于 96 组数据通过测试，即可认为该数据通过了随机性检测，具有良好的随机性。显然，经量化后的 16 位数据生成的序列均通过了 NIST 随机性检测。这有力地证明了本文提出的系统具有良好的随机性，即本文方案在伪随机数生成器和序列密码方面具有巨大的应用潜力。

3.7　应用前景分析

本文方案除在密码学领域有着较好的应用前景外，在混沌保密通信方面也有着巨大的实用价值。

表 3 NIST 随机性检测结果

测试项目	Bit-1st	Bit-2nd	Bit-3rd	Bit-4th	Bit-5th	Bit-6th	Bit-7th	Bit-8th	Bit-9th	Bit-10th	Bit-11th	Bit-12th	Bit-13th	Bit-14th	Bit-15th	Bit-16th
Frequency	99	98	98	99	98	100	99	98	98	97	98	100	100	99	100	100
Block frequency	100	100	100	99	100	98	99	99	99	97	99	99	99	99	98	100
Cumulative Sums(Forward)	99	98	100	98	98	100	99	99	98	97	98	100	100	100	100	98
Cumulative Sums(Reverse)	99	98	99	100	100	100	98	100	96	98	98	100	100	100	100	100
Runs	97	100	99	100	97	99	99	100	100	99	99	99	100	97	100	99
Longest runs	96	99	98	99	100	100	98	99	96	99	100	100	99	100	98	99
Rank	99	100	100	97	99	100	99	97	98	100	100	97	99	99	100	100
FFT	100	99	100	100	99	99	96	98	99	99	99	100	100	98	98	99
Non-overlapping template*	98	99	99	100	99	99	100	100	100	100	100	100	99	99	100	100
Overlapping template	98	100	100	99	100	100	100	99	98	98	100	100	100	98	100	98
Universal	98	99	99	99	98	100	100	100	98	99	100	99	100	98	99	98
Approximate Entropy	100	97	99	98	100	98	100	97	100	99	99	99	99	99	99	100
Random Excursions*	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
Random Excursions Variant*	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass
Serial 1	100	100	100	98	100	100	99	100	99	99	99	100	99	99	98	100
Serial 2	100	99	100	99	98	99	98	99	99	99	98	100	99	98	100	99
Linear Complexity	100	99	99	98	98	99	98	99	99	100	100	100	99	99	98	97

注：带“*”的测试下还包含多个子测试，利用子测试中的最低通过率来判断是否通过该测试，通过则用“pass”来表示

混沌系统产生的序列具有非周期性、连续宽带频谱、类噪声等特性，在相空间中具有极其复杂的运动轨迹和不可预测性，因此有着天然的隐蔽性，非常适合作为保密通信的载体。然而，目前混沌保密通信有着以下几点问题亟待解决[51]：1) 模拟电路实现的混沌保密系统，很难做到收发两端的完全匹配；2) 相空间重构和回归映射分析攻击的出现使通信中使用的混沌映射有被敌手精确预测的可能，从而降低系统的安全性；3) 数字电路的有限精度导致的混沌系统动力学退化问题；4) 混沌系统直接生成的序列分布不均，伪随机性不足。

本文方案很好地改善或优化了上述问题。1) 本文提出的 2D-PRCML 系统是个离散的动力学系统，完全可由数字系统实现，因此混沌保密通信收发两端的匹配较容易。2) 分布均匀性分析发现，2D-PRCML 系统的输出序列在回归映射的分布呈现不规则且分布均匀的状态，不同于其他系统的输出分布过于集中于某一固定形状，因此可以有效抵抗相空间重构或回归映射分析攻击。3) 2D-PRCML 系统通过耦合，各格子间相互扰动有效削弱了动力学退化的问题，进一步地，本文方案中引入了基于 PECA 这一离散系统的扰动，可以更有效地削弱系统的动力学退化问题。4) 均匀性分析和伪随机测试的结果证明，2D-PRCML 系统的输出序列具有良好的均匀性和伪随机性，因此安全性方面也有所保证。

综上，本文提出的 2D-PRCML 系统可以有效改善混沌保密通信中存在的部分问题，因此在该方面具有良好的应用前景。

4 结束语

基于分区初等元胞自动机和二维耦合映像格系统，本文提出了一种二维时空混沌系统，即二维伪随机耦合映像格系统。首先，本文基于初等元胞自动机设计了一种二维分区初等元胞自动机，以满足二维时空混沌系统的数据需求；然后，基于 2D-PECA 设计了一种伪随机耦合方案，同时利用 2D-PECA 的迭代结果，对系统中的各格子添加了不同的伪随机扰动。动态特性分析结果表明，相比于本文提到的其他二维时空混沌系统，2D-PRCML 系统拥有更强和更广泛的混沌特性，且拥有更好的遍历性和非周期性。同时，2D-PRCML 系统生成的序列在回归映射和频率分布上具有良好的均匀性。进一步地，这些序列在经过简单量化后，生成的 0,1 序列能够通过 NIST 随机性测试，证明了其良好的

伪随机性。此外，本文还分析了时空混沌系统中各格子生成序列之间的相关性，结果表明 2D-PRCML 系统所生成序列之间的相关性要明显低于其他系统，且均小于 0.3，从而保证了系统的安全性。综上所述，这些良好的性质表明 2D-PRCML 在密码系统中，特别是伪随机数生成器和序列密码方面具有巨大的应用前景。同时，在混沌保密通信方面也具有良好的实用价值。

参考文献：

[1] ALAWIDA M, SAMSUDIN A, TEH J S. Enhanced digital chaotic maps based on bit reversal with applications in random bit generators[J]. Information Sciences, 2020, 512: 1155-1169.

[2] 黄春光, 程海, 丁群. 基于 PUF 的 Logistic 混沌序列发生器[J]. 通信学报, 2019, 40(3): 182-189.
HUANG C G, CHENG H, DING Q. Logistic chaotic sequence generator based on physical unclonable function[J]. Journal on Communications, 2019, 40(3): 182-189.

[3] LORENZ E N. Deterministic nonperiodic flow[J]. Journal of the Atmospheric Sciences, 1963, 20(2): 130-141.

[4] LIU C Y, DING Q. A modified algorithm for the logistic sequence based on PCA[J]. IEEE Access, 2020, 8: 45254-45262.

[5] LIU Y, QIN Z, LIAO X F, et al. A chaotic image encryption scheme based on Hénon-Chebyshev modulation map and genetic operations[J]. International Journal of Bifurcation and Chaos, 2020, 30(6): 2050090.

[6] NASKAR P K, BHATTACHARYYA S, NANDY D, et al. A robust image encryption scheme using chaotic tent map and cellular automata[J]. Nonlinear Dynamics, 2020, 100(3): 2877-2898.

[7] HAMDI M, MIRI J, MOALLA B. Hybrid encryption algorithm (HEA) based on chaotic system[J]. Soft Computing, 2021, 25(3): 1847-1858.

[8] SAHASRABUDDHE A, LAIPHRAKPAM D S. Multiple images encryption based on 3D scrambling and hyper-chaotic system[J]. Information Sciences, 2021, 550: 252-267.

[9] WANG M X, WANG X Y, ZHAO T T, et al. Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme[J]. Information Sciences, 2021, 544: 1-24.

[10] 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.

[11] ZHANG X, YE R S. A novel RGB image encryption algorithm based on DNA sequences and chaos[J]. Multimedia Tools and Applications, 2021, 80(6): 8809-8833.

[12] 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 X H, LIAO C L, ZHU C X, et al. Image encryption algorithms based on chaos through dual scrambling of pixel position and bit[J]. Journal on Communications, 2014, 35(3): 216-223.

[13] 石航, 王丽丹. 一种基于压缩感知和多维混沌系统的多过程图像加密方案[J]. 物理学报, 2019, 68(20): 39-52.
SHI H, WANG L D. Multi-process image encryption scheme based on compressed sensing and multi-dimensional chaotic system[J]. Acta Physica Sinica, 2019, 68(20): 39-52.

[14] 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.

[15] 韩丹丹, 闵乐泉, 赵耿, 等. 一维鲁棒混沌映射及 S 盒的设计[J]. 电子学报, 2015, 43(9): 1770-1775.
HAN D D, MIN L Q, ZHAO G, et al. One-dimensional robust chaotic map and the construction of S-box[J]. Acta Electronica Sinica, 2015, 43(9): 1770-1775.

[16] DRIDI F, EL-ASSAD S, EL-HADJ YOUSSEF W, et al. The design and FPGA-based implementation of a stream cipher based on a secure chaotic generator[J]. Applied Sciences, 2021, 11(2): 625.

[17] LIU Z, WANG Y, ZHAO Y, et al. A stream cipher algorithm based on 2D coupled map lattice and partitioned cellular automata[J]. Nonlinear Dynamics, 2020, 101(2): 1383-1396.

[18] 陈铁明, 蒋融融. 混沌映射和神经网络互扰的新型复合流密码[J]. 物理学报, 2013, 62(4): 040301.
CHEN T M, JIANG R R. New hybrid stream cipher based on chaos and neural networks[J]. Acta Physica Sinica, 2013, 62(4): 040301.

[19] LI S J, CHEN G R, MOU X Q. On the dynamical degradation of digital piecewise linear chaotic maps[J]. International Journal of Bifurcation and Chaos, 2005, 15(10): 3119-3151.

[20] BECK C, ROEPSTORFF G. Effects of phase space discretization on the long-time behavior of dynamical systems[J]. Physica D: Nonlinear Phenomena, 1987, 25(1-3): 173-180.

[21] BINDER P M, JENSEN R V. Simulating chaotic behavior with finite-state machines[J]. Physical Review A: General Physics, 1986, 34(5): 4460-4463.

[22] FLORES-VERGARA A, GARCÍA-GUERRERO E E, INZUNZA-GONZÁLEZ 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.

[23] CHEN C, SUN K H, HE S B. An improved image encryption algorithm with finite computing precision[J]. Signal Processing, 2020, 168: 107340.

[24] LUO Y L, LIU Y Q, LIU J X, et al. Counteracting dynamical degradation of a class of digital chaotic systems via Unscented Kalman Filter and perturbation[J]. Information Sciences, 2021, 556: 49-66.

[25] ZHANG Y Q, WANG X Y, LIU L Y, et al. Spatiotemporal chaos of fractional order logistic equation in nonlinear coupled lattices[J]. Communications in Nonlinear Science and Numerical Simulation, 2017, 52: 52-61.

[26] 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.

[27] 王永, 马键滨, 陈燕, 等. 一种新的基于时空混沌的伪随机数发生器[J]. 计算机工程与应用, 2018, 54(11): 97-102.
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.

[28] 王永, 赵毅, Jerry Gao, 等. 基于分段 logistic 映射的二维耦合映像格子模型的密码学相关特性分析[J]. 电子学报, 2019, 47(3): 657-663.
WANG Y, ZHAO Y, GAO J, et al. Cryptographic feature analysis on 2D coupled map lattices based on piecewise logistic map[J]. Acta Electronica Sinica, 2019, 47(3): 657-663.

[29] CHATÉ H, MANNEVILLE P. Spatio-temporal intermittency in

coupled map lattices[J]. Physica D: Nonlinear Phenomena, 1988, 32(3): 409-422.

[30] KANEKO K. Pattern dynamics in spatiotemporal chaos[J]. Physica D: Nonlinear Phenomena, 1989, 34(1/2): 1-41.

[31] WANG X Y, GUAN N N, ZHAO H Y, et al. A new image encryption scheme based on coupling map lattices with mixed multi-chaos[J]. Scientific Reports, 2020, 10: 9784.

[32] WANG M X, WANG X Y, WANG C P, et al. Spatiotemporal chaos in cross coupled map lattice with dynamic coupling coefficient and its application in bit-level color image encryption[J]. Chaos, Solitons & Fractals, 2020, 139: 110028.

[33] 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.

[34] HE Y, ZHANG Y Q, WANG X Y. A new image encryption algorithm based on two-dimensional spatiotemporal chaotic system[J]. Neural Computing and Applications, 2020, 32(1): 247-260.

[35] PENG Y X, SUN K H, HE S B. An improved return maps method for parameter estimation of chaotic systems[J]. International Journal of Bifurcation and Chaos, 2020, 30(4): 2050058.

[36] DONG Y H, ZHAO G. A spatiotemporal chaotic system based on pseudo-random coupled map lattices and elementary cellular automata[J]. Chaos, Solitons & Fractals, 2021, 151: 111217.

[37] LI W, PACKARD N. The structure of the elementary cellular automata rule space[J]. Complex Systems. 2000, 4(3): 281-297.

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

[39] NEUMANN J, BURKS A W. Theory of self-reproducing automata[M]. Urbana: University of Illinois Press, 1966.

[40] LANGTON C G. Self-reproduction in cellular automata[J]. Physica D: Nonlinear Phenomena, 1984, 10(1-2): 135-144.

[41] WOLFRAM S. Cellular automata as models of complexity[J]. Nature, 1984, 311(5985): 419-424.

[42] WOLFRAM S, MALLINCKRODT A J. Cellular automata and complexity[J]. Computers in Physics, 1995, 9(1): 55.

[43] 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.

[44] 万求真，周昭腾. 具有多参数恒 Lyapunov 指数谱的新型统一混沌系统[J]. 通信学报, 2020, 41(6): 202-213.
WAN Q Z, ZHOU Z T. Novel unified chaotic system with constant Lyapunov expective spectrum with multiple parameters[J]. Journal on Communications, 2020, 41(6): 202-213.

[45] WANG X Y, FENG L, WANG S B, et al. Spatiotemporal chaos in coupled logistic map lattice with dynamic coupling coefficient and its application in image encryption[J]. IEEE Access, 2018, 6: 39705-39724.

[46] WANG X Y, ZHAO H Y, FENG L, et al. High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices[J]. Optics and Lasers in Engineering, 2019, 122: 225-238.

[47] 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.

[48] YAN J, BECK C. Distinguished correlation properties of Chebyshev dynamical systems and their generalisations[J]. Chaos, Solitons & Fractals: X, 2020, 5: 100035.

[49] BASSHAM L E I, 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.

[50] HU G Z, LI B B. Coupling chaotic system based on unit transform and its applications in image encryption[J]. Signal Processing, 2021, 178: 107790.

[51] 王兴元. 混沌系统的同步及在保密通信中的应用[M]. 北京: 科学出版社, 2012.
WANG X Y. Synchronization of chaotic systems and its application in secure communication [M]. Beijing: Science Press, 2012.

[作者简介]

董有恒（1995− ），男，山东济宁人，北京邮电大学博士生，主要研究方向为混沌密码理论及应用等。

赵耿（1964− ），男，四川苍溪人，博士，北京邮电大学教授、博士生导师，主要研究方向为混沌密码理论及应用、信息安全等。

马英杰（1979− ），女，吉林通化人，博士，北京电子科技学院副教授、硕士生导师，主要研究方向为通信系统、混沌保密通信等。