基于多层元胞自动机的动态随机耦合映像格系统性能分析

赵 耿[1,2],吴 锐[1,2*],马英杰[2],董有恒[2],黄思婕[1,2]
(1. 西安电子科技大学,陕西西安 710071;2. 北京电子科技学院,北京 100070)

摘 要: 基于多层元胞自动机的时空混沌系统设计了一款用于图像加密的伪随机数发生器. 针对现有的基于耦合映像格系统仍存在参数空间有限、局部混沌行为等问题,本文提出一种基于多层元胞自动机的伪随机耦合映像格系统. 在初等元胞自动机基础上设计出多层元胞自动机,将耦合系统与多层元胞自动机同时进行迭代,通过自动机的迭代输出得到耦合系统中每个格子的动态耦合方案以及伪随机扰动方法. 本文通过分岔图、Kolmogorov Sinai 熵和输出序列均匀性对耦合映像格系统进行对比分析,并分析了系统生成序列的随机性和任意两个格之间的相关性. 理论分析和实验结果表明,与其它耦合映射格系统相比,该系统具有更好的混沌特性和更大的参数空间,系统生成的序列具有较好的遍历性、均匀性和随机性. 研究结果表明该系统在密码学领域具有广阔的应用前景.

关键词: 耦合映像格系统;多层元胞自动机;混沌系统;动态耦合;密码系统
基金项目: 北京高校“高精尖”学科建设项目(No.3201017);国家自然科学基金(No.61772047)
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112(2024)09-3111-12
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20230134

Performance Analysis of Dynamic Random Coupled Map Lattices System Based on Multilayer Elementary Cellular Automata

ZHAO Geng[1,2], WU Rui[1,2*], MA Ying-jie[2], DONG You-heng[2], HUANG Si-jie[1,2]
(1. *Xidian University*, *Xi' an*, *Shaanxi* 710071, *China*;
2. *Beijing Electronic Science and Technology Institute*, *Beijing* 100070, *China*)

Abstract: A pseudo-random number generator for image encryption has been developed, utilizing a spatiotemporal chaotic system with multilayer elementary cellular automata. To solve the existing problems of limited parameter space and local chaotic behavior based on coupled image lattice system, a dynamic random coupled map lattices (DRCML) system based on a multilayer elementary cellular automaton (MECA) is proposed. The MECA is designed on the basis of the elementary cellular automaton (ECA), and DRCML system is iterating with the MECA simultaneously, and the DRCML system of each lattice in the coupled system and the pseudo-random perturbation method are obtained through the iterative output of the MECA. The DRCML system is compared and analyzed by bifurcation diagram, Kolmogorov Sinai entropy and output sequence uniformity , and the correlation between the randomness of the generated sequence of the system and any two lattices is analyzed. The theoretical analysis and experimental results show that the DRCML system has better chaotic properties and wider parameter space than other coupled map lattices systems, and the generated sequences have better ergodicity, uniformity and randomness. The results show that the DRCML system has a promising application in the field of cryptography.

Key words: coupled map lattices; multilayer elementary cellular automata; chaotic system; dynamic coupling; cryptosystem
Foundation Item(s): Beijing University's "High Quality" Discipline Construction Project (No.3201017); National Natural Science Foundation of China (No.61772047)

收稿日期:2023-02-15;修回日期:2023-08-10;责任编辑:梅志强
*通讯作者:吴锐

1 引言

混沌系统具有许多适合密码学的特征,包括伪随机性、初值敏感性、遍历性和不可预知性[1,2]. 因此结合混沌系统的加密算法,成为近些年来计算机科学和密码领域的研究热点之一[3,4]. 然而混沌系统在有限精度的数字计算机运行时,不存在真正的非周期的随机序列,会发生动力学退化现象[5,6],针对数字混沌系统存在如此固有缺陷,目前采取的解决方案有:采用更高精度的数字系统[7],但会造成系统资源的浪费;级联多个混沌系统[8,9],虽能够有效增加混沌系统的周期,但却降低了系统的动态复杂性;而添加扰动混沌方案能够有效缓解混沌系统动力学退化现象[10~12].

时空混沌系统由于利用空间上的耦合,使得不同位置的混沌输出通过耦合能够相互扰动,因此有效削弱了动力学退化的影响,并且相比低维混沌系统具有更好的特性,包括更大的参数空间、更好的随机性、更多的混沌序列以及更大的初始条件选择范围. Kaneko首先提出时空耦合映像格系统模型(Coupled Map Lattices,CML),该模型可以在时间和空间两个维度上改变整个系统的状态[13]. 其后众多研究者在此基础上继续研究,文献[14]基于Arnold映射开发出一种具有分数阶微分逻辑映射和空间非线性耦合的CML系统,扩大了系统控制参数范围,但系统的各个格子耦合状态是固定的,导致系统各个格子间的相关性较高. 文献[15]结合模运算通过分段线性函数混沌映射(Piece Wise Linear Chaotic Map,PWLCM)和sin映射导出二维随机耦合方案,通过与相邻的两个格子和一个由伪随机序列确定的格子相耦合迭代得到新一代格子的值,有效减少了周期性窗口,同时增强了系统的非周期性. 然而系统的映射图存在固定形状,易受回归映射分析攻击[16]. 文献[17]提出一种基于多个混沌映射的间歇性跳跃的CML系统模型,通过多个混沌映射生成的伪随机信息以复杂的非线性方式集成到格子耦合中,使各个格子耦合状态是时变的. 但耦合格子的选择在空间上任然是固定的,限制了系统的参数空间,同时导致局部混沌行为. 文献[18]采用logistic动态混合线性-非线性耦合方案,通过引入动态耦合系数保证耦合系数的动态效应,但系统的分支图中仍然存在周期窗口. 文献[19]通过双参数分型排序向量的方式控制时空混沌系统的迭代节点关系,各个格子间的耦合方式是时变的,消除了基于CML模型的节点固定选择模型的弊端,但其分岔图中仍有固定周期. 文献[20]将一维的Logistic-Chebyshev映射作为耦合映像格系统的动态耦合系数,使不同格子间的能量分布均匀,减少了分岔图中周期性窗口,但在某些控制参数下系统仍表现出弱混沌现象. 文献[21]通过引入正弦动态耦合系数,提高了系统中处于混沌状态的格子数量,增强了系统的混沌性能,但系统的分岔图中仍然存在固定周期. 文献[22]提出一种基于初等元胞自动机的伪随机耦合映射格方案,消除了系统分岔图的周期性窗口. 然而,某些元胞迭代规则下元胞的周期性较短,使得系统在某些固定参数下伪随机性较差,同时系统的控制参数不能突破[3,4]的极限范围.

为解决上述问题,本文提出一种多层初等元胞自动机的耦合映射系统,主要贡献如下:

(1)针对初等元胞自动机短周期性,提出一种多层元胞自动机(Multilayer Elementary Cellular Automata,MECA). 该自动机具有良好的长周期性和伪随机性.

(2)基于MECA设计一种耦合方案. 通过MECA的状态确定各个格子的耦合方案,使得对于同一个格子在不同时间维度中有着不同耦合方案,提升了系统中的能量传递.

(3)根据MECA的迭代过程中初始元胞状态,使其归一化后作为随机扰动加入到耦合系统中,进一步削弱时空混沌系统的动力学退化. 由于初始元胞自动机的状态在迭代过程中是在不断变化的,因此耦合方案具有一定的伪随机性.

2 设计原理

2.1 时空混沌系统

耦合映像格系统是一种时空混沌系统,可以有效缓解混沌系统动力学退化,提高混沌系统的复杂性. 传统的耦合映像格系统模型(Coupled Map Lattices,CML)中,当前格子的状态是由相邻两个格子的状态所决定的[13],其公式定义如下

$$X_{n+1}(i)=(1-\varepsilon)f\left[X_n(i)\right]+\frac{\varepsilon}{2}\left\{f\left[X_n(i-1)\right]+f\left[X_n(i+1)\right]\right\} \tag{1}$$

其中,n表示系统的时间维度$(n=1,2,3,\cdots)$,i表示系统的空间维度$(i=1,2,3,\cdots,L)$,L为系统中总的格子数量. 系统的边界条件是周期的,即:第L个格子为第1个格子的左邻格子,第1个格子为第L个格子的右邻格子,$\varepsilon(0<\varepsilon<1)$表示系统耦合强度的大小,映射$f(x)$一般为一维logistic混沌映射,其公式定义如下

$$f(x)=\mu x(1-x),x\in(0,1) \tag{2}$$

其中,$\mu\left(0<\mu\leqslant 4\right)$为控制参数,当$3.57<\mu\leqslant 4$时系统处于混沌状态.

2.2 多层初等元胞自动机

元胞自动机(Cellular Automata,CA)是Neumann等人在1948年提出的,是一个在时间和空间上都离散的动力学系统,最初用于模拟生物系统的自我复制[23]. 初等元胞自动机(Elementary Cellular Au-

tomata,ECA)是由一维线性排列的元胞组成的一种特殊的元胞自动机,主要是由元胞、元胞空间、元胞邻居、迭代规则以及边界条件等所构成[24]. ECA中元胞邻居只有相邻的两个元胞,每个元胞的状态只有两种,分别为"0"和"1",边界条件一般是周期的,即:第L个元胞为第1个元胞的左邻元胞,第1个元胞为第L个元胞的右邻元胞. 元胞的迭代规则如图1所示.

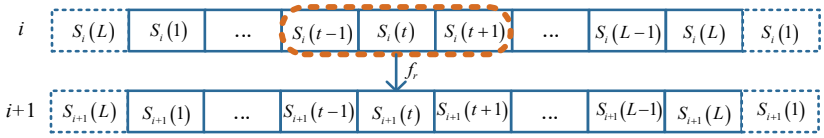


图1　ECA迭代规则

如图1所示,每个元胞更新的状态值是由当前元胞以及相邻两个元胞状态值通过局部转换函数f_r进行迭代得到,元胞的迭代方式可以表示为

$$S_{i+1}(t)=f_r\left[S_i(t-1),S_i(t),S_i(t+1)\right] \tag{3}$$

其中,$i(i=0,1,2,\cdots)$表示时间索引,$t(t=0,1,2,3,\cdots,L)$表示元胞索引,因此,$S_i(t),(S_i(t)\in\{0,1\})$表示为第$t$个元胞在$i$时刻的状态值,$f_r$是遵循迭代规则$r$的局部转换函数,即由集合$\{000,001,\cdots,111\}$映射到集合$\{0,1\}$,因此元胞状态的局部转移规则共有$2^8$种. 例如$r$=105的迭代规则如表1所示.

表1　r=105的迭代规则

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

根据ECA迭代结果,可将ECA迭代规则分为5类:无效规则、固定点规则、周期规则、局部混沌规则、全局混沌规则[24]. 具有全局混沌规则的ECA本质上是一个在时间和空间上都是离散的混沌动力学系统,能够有效缓解有限计算精度数字计算机的动态退化问题. 本文中任意三种全局混沌规则下的ECA均可以用于构建多层元胞自动机(Multilayer Elementary Cellular Automata,MECA),而具有全局混沌规则的ECA迭代规则如表2所示.

然而,理论上混沌ECA的最长周期是由有限长的元胞数量决定的,实际中是不能够达到ECA的最大长度,即

$$T_p\leqslant T_t\leqslant 2^L \tag{4}$$

其中,T_p是元胞的实际周期,T_t是元胞的理论周期,L为ECA中元胞的总数.

鉴于上述原因,本文提出一种多层初等元胞自动机MECA,来扩展实际周期,该结构是由3种不同迭代规则下的ECA来确定最终元胞的状态值,MECA结构图如图2所示.

图2为MECA结构内部图,黑色(白色)代表当前元胞的状态1(0),MECA元胞的状态值是通过在相同时间和空间范围内的3种不同规则的ECA的元胞状态值通过局部转换函数f_r迭代而来,3种不同的ECA会在MECA的迭代过程种而按自身的规则进行迭代,MECA会按照选中的规则进行迭代,表2中的规则均可在MECA迭代过程中使用. 分别仿真元胞长度L=100时,MECA迭代规则分别为$r_1=120,r_2=102,r_3=105,r=183$时的迭代结果,以及MECA迭代规则分别为$r_1=151,r_2=150,r_3=105,r=183$时的迭代结果,另选取ECA迭代规则$r=183$时迭代结果作为对比,结果如图3所示.

表2　ECA中全局混沌迭代规则

种类	编号规则
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)

图3(a)表示ECA在$r=183$时的迭代结果,图3(b)和图3(c)分别表示MECA在不同初始迭代规则下进行迭代的结果,图中蓝色(白色)分别代表元胞的状态1(0),横坐标表示元胞的索引值,纵坐标表示迭代次数,通过对比发现相同的迭代规则r=183下MECA和ECA迭代结果不同,并且不同的初始迭代ECA规则也会导致MECA迭代结果不同. 此外,通过计算同一个ECA的皮尔逊系数得到实际的元胞周期,例如序列$\{S_i(t),S_{i+1}(t),\cdots,S_{i+l}(t)\}$和序列$\{S_{i+\tau}(t),S_{i+\tau+1}(t),\cdots,S_{i+\tau+l}(t)\}$,其中$t$是元胞索引值,$l$是序列长度,$\tau(\tau=1,2,3,\cdots)$表示延时,为了不失一般性,本文设置$t=50,l=2\,000$,采用$r$=18、90、150、183作为对比条件,MECA、ECA皮尔逊系数如图4所示.

如图4所示,横坐标表示时间延时,纵坐标表示相关系数,值为1的相关系数对应的两个最接近的时延之间的长度为实际周期T_p. 根据实际周期的长度,本文将混沌规则分为三类:短周期规则$\left(T_p<l\right)$、中周期规则$\left(l<T_p<5l\right)$、长周期规则$\left(T_p>5l\right)$. 通过

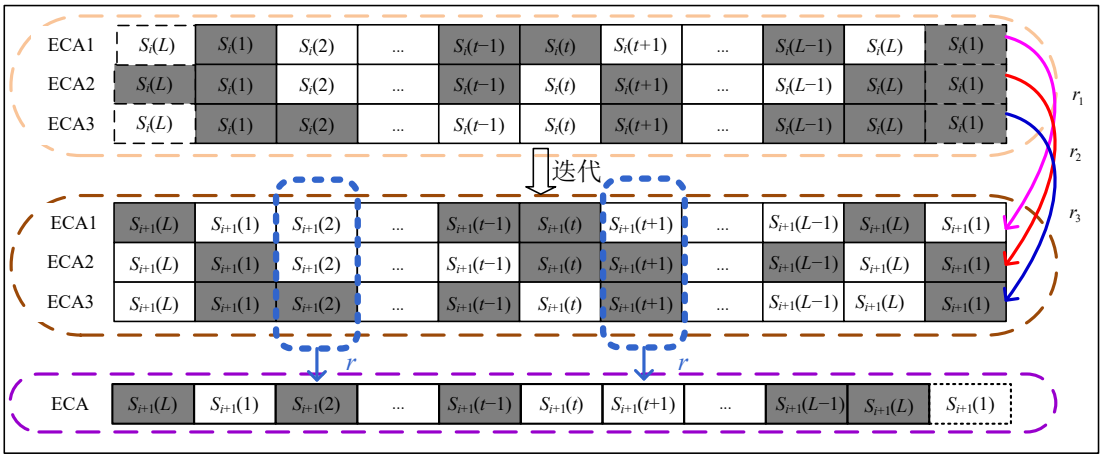
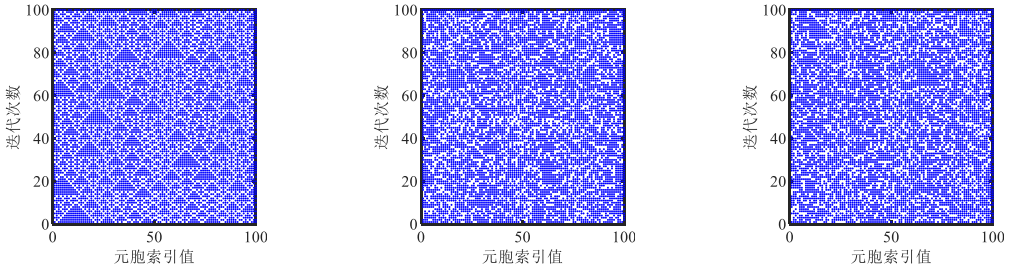
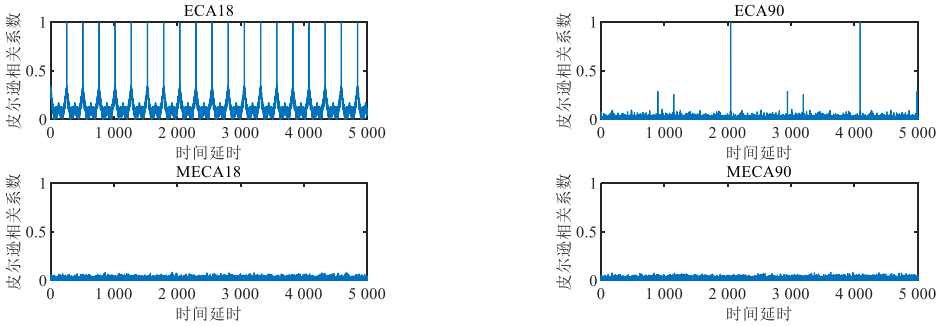


图2 MECA结构图

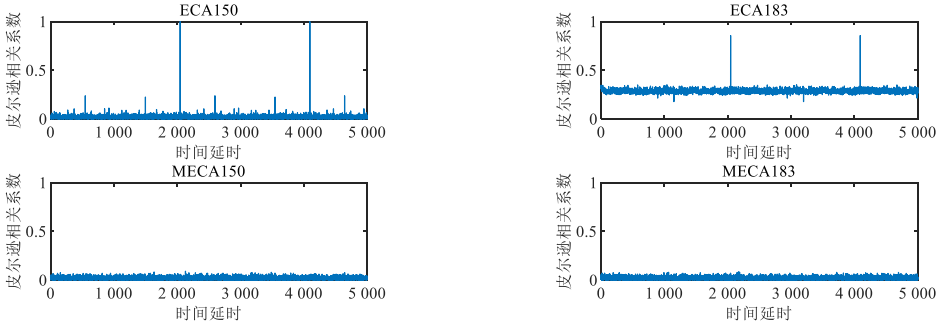


(a) ECA(r=183) (b) MECA(r=183) (c) MECA(r=183)

图3 r=183时ECA与MECA迭代结果图



(a) r=18 (b) r=90



(c) r=150 (d) r=183

图4 ECA与MECA的皮尔逊相关系数对比

对比图4(*a*)~(*d*)不难发现*r*=18属于短周期混沌ECA,*r*=150,*r*=90属于中周期混沌ECA,*r*=183属于长周期混沌ECA. 并且通过对比发现在同种迭代规则下,无论是*r*=18、150、90还是*r*=183,MECA的实际周期长度比ECA的实际周期长度要明显增加,并且不同迭代规则下,MECA的不同延时序列间的皮尔逊相关系数均小于0.1,因此MECA的伪随机性比ECA要强.

2.2　系统设计

本文提出的具有扰动的多层初等元胞自动机的动态随机耦合映像格系统(Dynamic Random Coupled Map Lattices,DRCML)的数学表达式为

$$\begin{cases} y_{n+1}(i)=\dfrac{(1-\varepsilon)}{2}\left\{f\left[x_n(a)\right]+f\left[x_n(b)\right]\right\} \\ \qquad\qquad +\dfrac{\varepsilon}{2}\left\{f\left[x_n(c)\right]+f\left[x_n(d)\right]\right\} \\ x_{n+1}(i)=\left\{\dfrac{\text{bin 2dec}\left[\Phi\left(\text{uint 32}\left(\text{floor}(y_{n+1}(i)\times 2^{32})\right)\right)\right]}{2^{32}}\right. \\ \qquad\qquad \left.+p\left(S_n\right)\times\sigma(S_n(i))\right\}\bmod 1 \end{cases} \tag{5}$$

其中,f为式(2)中一维logistic函数,$\varepsilon(0<\varepsilon<1)$表示系统耦合强度的大小,$i(i=1,2,3,\cdots,L)$表示当前格子的索引值,$L$表示系统总的格子数,$n(n=1,2,3,\cdots)$表示系统的时间维度,floor(·)表示向下取整函数,uint 32(·)将常数转换为无符号32位数,bin 2dec(·)为二进制转换为十进制,$\Phi(\cdot)$表示依次取出每个格子中无符号数32位数的1~32位. a、b、c、d表示耦合格子的索引值,其数值是通过MECA迭代搜寻得到. $p\left(S_n\right)$是根据MECA中迭代过程3个初始ECA元胞状态得到的扰动. $\sigma(S_n(i))$表示当前扰动符号的数值,$\sigma(S_n(i))$的数值大小为±1,mod 1是为了保留结果的小数部分,使得最终的运算结果保持在(0,1)区间范围之内. 以下是各个参数的详细计算过程.

$$p\left(S_n\right)=\frac{0.5\times\text{bin 2dec}\left(S_nC_1\left(b_{45}b_{46}\cdots b_{56}\right)S_nC_2\left(b_{45}b_{46}\cdots b_{56}\right)S_nC_3\left(b_{45}b_{46}\cdots b_{56}\right)\right)}{2^{36}-1} \tag{8}$$

其中,bin 2dec(·)函数表示将二进制数转换为十进制数,S_nC_1,S_nC_2,S_nC_3分别代表MECA迭代过程中3个初始ECA第n次迭代的结果,不难发现扰动值的取值范围为(0,0.5). 由于MECA中3个初始ECA是在不断迭代变化的,因此扰动值的大小也是在不断变化的,这使得扰动值得变化也是随机的,能够有效缓解系统的动力学退化现象.

2.2.1　耦合格子索引值

每次耦合映像格系统迭代时,MECA会首先完成迭代,生成与DRCML系统长度相同的元胞序列,并且根据当前格子的索引在MECA中寻找参与当前格子相耦合的四个格子索引a、b、c、d,在MECA元胞序列寻找耦合格子对应的索引值,搜寻函数为

$$[a,b]=\text{search }0\left(S_n,i\right) \tag{6}$$

$$[c,d]=\text{search }1\left(S_n,i\right) \tag{7}$$

其中,S_n为式(3)中元胞自动机的迭代的结果,n为式(5)中的迭代次数,i为式(5)中当前格子的索引值,所提系统总的格子数为100. search $1\left(S_n,i\right)$表示寻找第i个元胞左右两个最近元胞状态为"1"的元胞索引值,search $0\left(S_n,i\right)$表示寻找第i个元胞左右最近两个状态为"0"的元胞索引值,search函数返回的结果为上述两个单元格的索引值. 其搜索过程如图5所示.

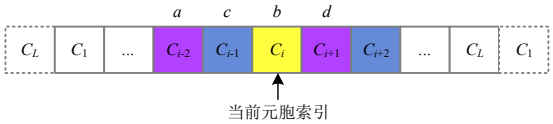


图5　search函数计算过程图

如图5中,黄色格子代表当前系统格子索引对应的MECA中元胞位置,蓝色(紫色)代表当前元胞的状态1(0),通过搜索函数search1,search0可以得到$a=i-2$,$b=i+1$,$c=i-1$,$d=i+2$. 通过增加参与耦合格子的数量以及参与耦合格子索引的不确定性,提高DRCML系统的李亚普洛夫指数值从而提高系统的混沌特性,同时降低了当前格子与系统中各个格子之间的相关性,确保了整体DRCML系统的安全性.

2.2.2　扰动值

扰动值$p\left(S_n\right)$是通过MECA迭代过程中初始的三个ECA共同组合得到的,其中S_n由元胞状态组成的一个二进制数$S_n=b_1b_2b_3\cdots b_{100}$,$b_i$表示第$i$个元胞的状态值,本文分别取MECA系统迭代过程中3个ECA元胞序列中间12位组成共36位01序列对系统进行扰动,扰动值计算规则:

2.2.3　扰动符号

扰动符号$\delta\left(S_n(i)\right)$是根据MECA迭代结果来确定

$$\delta\left(S_n(i)\right)=\begin{cases}1, S_n(i)=1\\ -1, S_n(i)=0\end{cases} \tag{9}$$

其中,$S_n(i)$表示第n次迭代过程中,MECA中第i个元胞的状态. 由式(9)可知扰动符号的值为±1,并且随着MECA的不断迭代,$\delta\left(S_n(i)\right)$的数值也在不断变化,所以

对每个格子施加的扰动值是不同的，这样扰动符号数值的变化也是伪随机的，降低了各个格子之间地相关性，提高了系统的复杂度.

3 系统性能分析

本节将仿真DRCML系统的各项性能，DRCML系统的控制参数$\mu\in(3,4]$，耦合系数$\varepsilon\in(0,1)$，一维logistic混沌映射f的初始值设为0.05，将f的初始值，以及系统通过迭代99次得到的结果的值依次放入到100个格子中，完成DRCML系统中各个格子的初始化操作. 采用3个100 bit二进制数来初始化MECA中3个ECA状态，S_nC_1，S_nC_2，S_nC_3的初始值为

$$\begin{cases} S_nC_1=\text{D0A5\_2EA3\_B3E8\_66F9\_C4C8\_B49A\_F} \\ S_nC_2=\text{51A2\_DAA8\_E425\_26F9\_B9F4\_BA01\_9} \\ S_nC_3=\text{BFB1\_895E\_425D\_4E2A\_644F\_8210\_A} \end{cases} \tag{10}$$

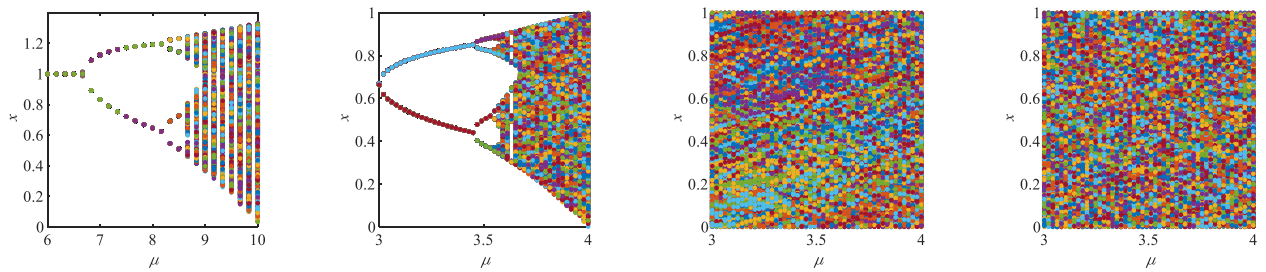
其中，S_nC_1、S_nC_2、S_nC_3表示的是16进制数，并且选取全局混沌规则$r_1=105$，$r_2=102$，$r_3=120$作为MECA中初始3个ECA的迭代规则，$r=183$作为MECA迭代规则，这样能够保证MECA的混沌性. 另外，选取表2中任意混沌规则均可达到同样的效果.

本文讨论了如下三种模型的性质：(1)基于分数阶logistic方程的非线性耦合映射格系统(Nonlinear Coupled Map Lattices，NCML)[14]；(2)logistic动态混合线性—非线性耦合映射格系统(Logistic-Dynamic Mixed Linear-Nonlinear Coupled Map Lattices，LDMLNCML)[18]；(3)基于初等元胞自动机的伪随机动态耦合映射格系统(Pseudo Random Coupled Map Lattices，PRCML)[22]与本文所提出的DRCML系统进行对比. 其中LDMLNCML中$\eta=0.8$，对于NCML系统的分段常数$r=0.25$，分阶数导数$\alpha=0.9$，控制参数$\mu\in[6,10]$，PRCML系统中初始元胞状态选取DRCML系统中的S_nC_1，其它初始数值与DRCML初始数值相同.

3.1 分岔图

分岔图用来评价混沌系统的周期性和遍历性. 为进行比较分析，本文设置系统的耦合参数$\varepsilon=0.5$，并选择第50个格子作为分析对象，上述系统的分岔图如图6所示.

如图6(a)所示，由于利用分数阶logistic方程，NCML系统中控制系数μ的范围由[3,4]扩张到[6,10]，当控制参数$\mu<9$时系统存在周期性窗口，在区间[9,10]时该系统进入混沌状态，并且在$\mu=10$时系统迭代及结果才充满整个空间，系统的遍历性较差. 由图6(b)可知，当LDMLNCML系统的控制参数$\mu<3.6$时，系统出现周期性窗口，在区间[3.6,4]时系统进入混沌状态，并且在$\mu=4$时系统迭代结果才充满整个空间，系统的遍历性差. 图6(c)的PRCML系统和图6(d)的DRCML系统在控制参数$\mu\in(3,4]$区间内系统周期性几乎消失，系统在$\mu=3$即进入混沌状态，并且迭代结果都充满了整个空间，系统的遍历性较好. 但在$\mu\in(3,3.4]$区间PRCML系统具有一些特定的轨道，此时系统的随机性较差.

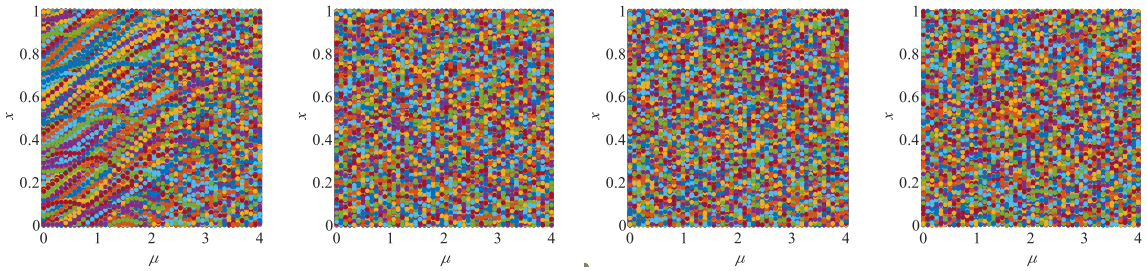


(a) NCML (b) LDMLNCML (c) PRCML (d) DRCML

图6 NCML、LDMLNCML、PRCML、DRCML系统分岔图

为了进一步凸显DRCML系统优势，我们将控制参数μ由[3,4]扩充至[0,4]，PRCML、DRCML系统分岔图如图7所示.

通过图7(a)可以发现在迭代规则r=183时PRCML系统在控制参数$\mu\in[0,3]$时系统的分岔图有近似平行的轨道，表明此时系统混沌特性只出现在某些固定的点上，系统的伪随机性较差. 图7(b)、图7(c)、图7(d)分别仿真了在r=183、r=120、r=45时DRCML系统的分岔图，DRCML系统将控制参数扩展到[0,4]，系统的分岔图分布均匀且没有固定的轨道，具有良好的非周期性、遍历性、伪随机性. 造成这种结果有两方面原因，在$\mu\in(0,3.57]$区间内系统表现出良好的非周期性和遍历性是由于根据MECA不断迭代的结果，为系统添加不同的伪随机扰动以及不同的耦合方式造成的，而在$\mu\in(3.57,4]$区间内是由于logistic本身具有良好的混沌特性以及为系统添加的伪随机扰动和不同的耦合方式造成的. 由于DRCML系统的控制参数由[3,4]增加到[0,4]，且没有周期窗口，在密码系



(a) PRCML(r=183)　(b) DRCML(r=183)　(c) DRCML(r=120)　(d) DRCML(r=45)

图7　PRCML、DRCML系统分岔图对比

统中使用DRCML系统时,可以使用更多的控制参数μ作为密钥,极大的扩充了密钥空间.

3.2　Kolmogorov-Sinai熵分析

李雅普诺夫指数(Lyapunov exponent,LE)描述了动力学系统中相空间中相邻轨道的分离速率,用来评价混沌动力学系统的不可预知性,其定义为

$$\lambda=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|\frac{\mathrm{d}F(x)}{\mathrm{d}x}\right|_{x=x_i} \tag{11}$$

其中,$F(x)$为动力学系统的数学表达式. 并且通常采用wolf法计算LE[18,25].

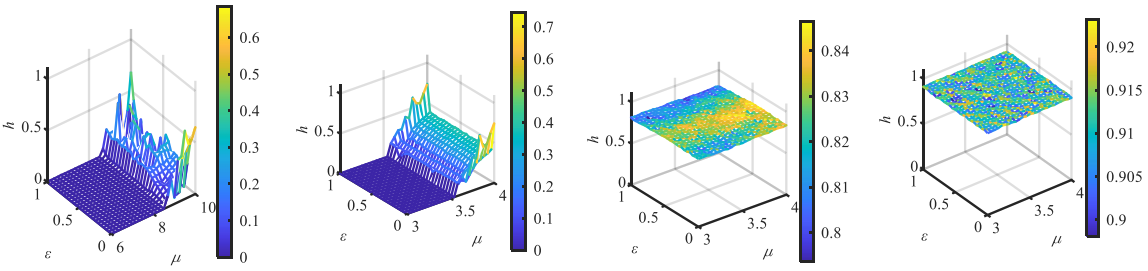
基于LE,一般采用K熵密度(Kolmogorov-Sinai Entropy Density,KED)和K熵阔度(Kolmogorov-Sinai entropy breadth,KEB)来描述时空特性,其计算公式为

$$h=\frac{\sum_{i=1}^{n}\lambda^{+}(i)}{L} \tag{12}$$

$$\mathrm{hu}=\frac{L^{+}}{L} \tag{13}$$

其中,h和hu分别代表KED和KEB. i表示系统的空间维度,L为时空混沌模型的总格数,L^{+}表示含有正LE的格数,$\lambda^{+}(i)=\begin{cases}\lambda(i),\lambda(i)>0\\0,\lambda(i)\leqslant 0\end{cases}$表示模型中正的LE指数.

参数h为正数,表明系统处于混沌状态,h数值越大表明该系统的混沌特性越强. 在不同控制参数以及耦合系数下,各系统的h值范围如图8所示.



(a) NCML　(b) LDMLNCML　(c) PRCML　(d) DRCML

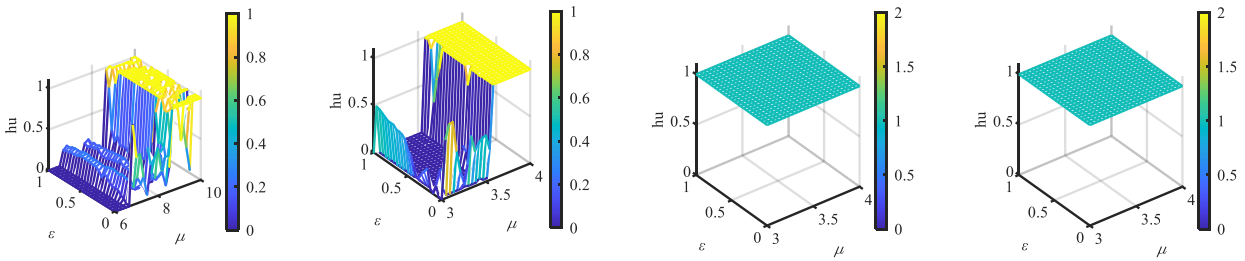
图8　NCML、LDMLNCML、PRCML、DRCML系统KED参数

图8中x轴表示控制系数μ,y轴表示耦合系数ε,z轴表示K熵密度大小,图8(a)NCML系统在控制系数$\mu\in[8.5,10]$时系统处于混沌状态,但系统的K熵密度均小于0.6,并且K熵密度大于0.2占比11.2%,系统整体混沌性能较差. 图8(b)LDMLNCML系统在控制参数$\mu\in[3.57,4]$时,系统处于混沌状态,虽然系统K熵密度较NCML系统有所提升,K熵密度大于0.2的格子占比25.44%,但系统整体的K熵密度也均小于0.6. 而图8(c)PRCML和图8(d)DRCML系统在$\mu\in(3,4),\varepsilon\in(0,1)$的整个区间均处于混沌状态,并且K熵密度均高于0.8,而DRCML系统K熵密度均高于0.9,明显高于PRCML系统,验证了DRCML系统混沌性能的优越性.

hu表示处于混沌状态的格子占总系统格子数量的比例,可以从空间的角度来衡量系统的混沌性能,hu值越大表示处于混沌状态的格子就越多,hu=1表示系统中所有格子都处于混沌状态. 在不同控制参数以及耦合系数下,各系统的KEB参数如图9所示.

如图9(a)NCML系统和图9(b)LDMLNCML系统在所有(μ,ε)参数对下,KEB=1的格子统计占分别为20.64%和42.88%,此时系统处于混沌状态的格子较少. 而图9(c)PRCML和图9(d)DRCML系统hu=1的格子统计占比均为100%. 这意味着两个系统在所有(μ,ε)参数对下系统中的各个格子均处于混沌状态.

综上所述,DRCML系统相比于上述提出的其它方



(a) NCML (b) LDMLNCML (c) PRCML (d) DRCML

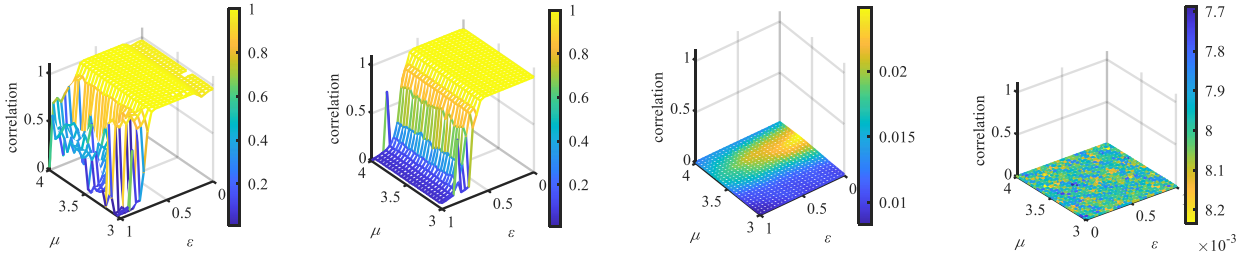
图9 NCML、LDMLNCML、PRCML、DRCML系统KEB参数

案,系统的混沌性能更好,并且KED的均值等于0.911,表明该系统具有良好的复杂性以及不可预知性,在应用于密码系统时,由于所有(μ,ε)参数对均能够使系统进入混沌状态,因此在(μ,ε)作为密钥时,扩大了系统整体的密钥空间.

3.3 相关性分析

一些基于CML的图像加密系统可以同时使用多个格子来驱动排列和扩散相,每个格子都可以被视为一个独立的加密器件,两个格子间的相关性越低,对抗信息泄露的能力就越强. 因此研究CML系统格子间的相关性对基于CML的密码系统的有重要意义. 本文计算了系统在不同控制参数以及耦合系数下不同格子生成的序列之间的皮尔逊相关系数的平均值,各系统的皮尔逊相关系数如10图所示.

如图10(*a*)NCML系统的相关系数大多在1附近,然而在工程上,通常认为皮尔逊相关系数在[0,0.3]区间内,两个序列是不相关的,而NCML系统和图10(*b*)LDMLNCML系统相关系数小于0.3的统计占比分别在8.8%和24.32%. 图10(*c*)PRCML系统以及图10(*d*)DRCML系统的皮尔逊相关系数均在0.3以下,并且DRCML系统的皮尔逊相关系数均在8×10^{-3}左右显著低于其它三种系统. 因此,各个格子间的相关系数极小.



(a) NCML (b) LDMLNCML (c) PRCML (d) DRCML

图10 NCML、LDMLNCML、PRCML、DRCML系统相关系数对比

与此同时本文将控制参数范围由[3,4]扩充到[0,4]与PRCML系统进行对比,其结果如图11所示.

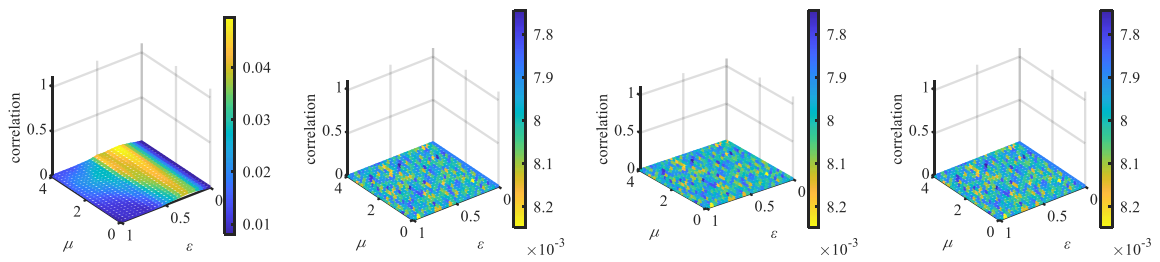
通过对比图11发现,PRCML系统与DRCML系统在任何(μ,ε)参数对下,皮尔逊相关系数均小于0.3,PRCML系统的相关系数平均在0.025 5,而DRCML分别在元胞r=183、r=120、r=45迭代规则下系统在相关系数均值为8×10^{-3},DRCML系统各个格子之间的相关性较PRCML系统的相关性低,因此DRCML系统作为应用与密码系统时,使得敌手很难通过某些格子的输出推断出其它各个格子的输出,系统的安全性得以提升.

3.4 回归映射和输出均匀性分析

系统回归映射是评估系统是否能抵抗返回图攻击,在密码系统中,系统分布应该是均匀的,本文通过回归映射和输出均匀性分析来评估各CML系统生成的序列值的均匀性. 选取系统中第50个格子,在$\mu=4$,耦合系数$\varepsilon=0.25,0.5,0.75$时系统的回归映射图,各系统的回归映射图如12所示.

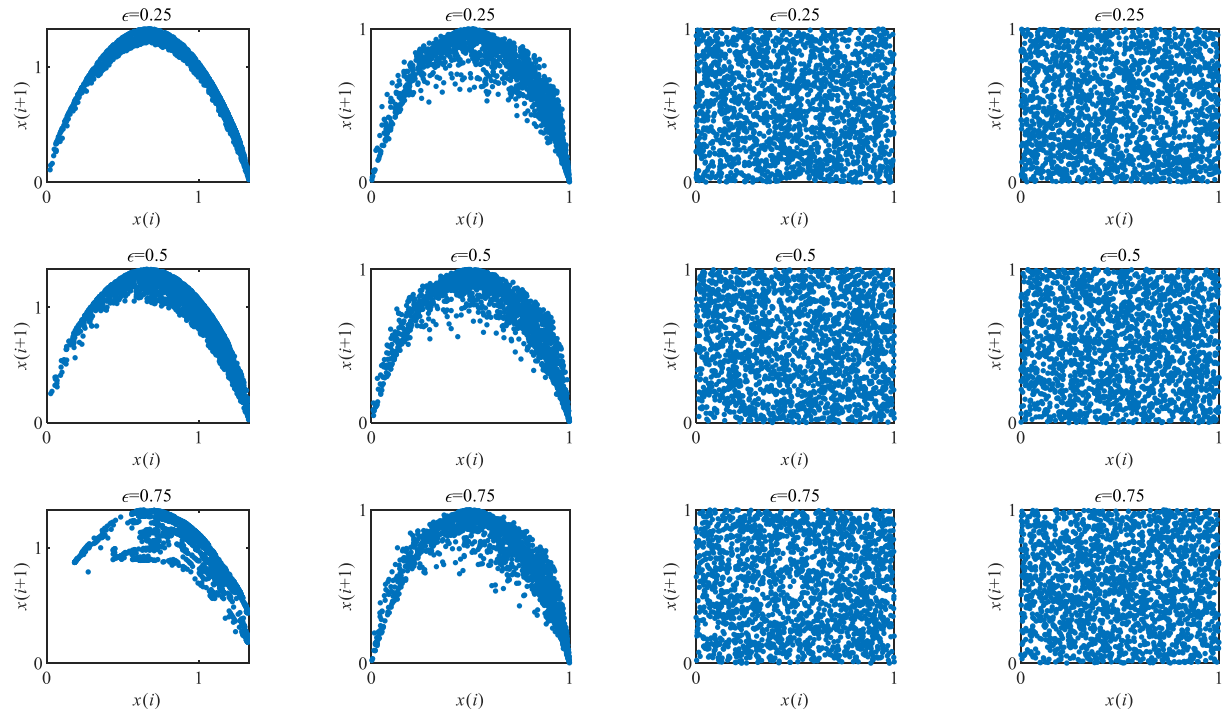
通过对比发现,图12(*a*)NCML系统和图12(*b*)LDMLNCML系统的回归映射在一条固定的抛物线附近,随着耦合系数的增大而逐渐发散,因此很容易遭受回归映射分析攻击,而图12(*c*)PRCML和图12(*d*)DRCML系统回归映射发散在整个区间,各个点均匀分布在整个区间,因此能够有效抵抗回归映射分析攻击.

对于输出均匀性分析,本文设置耦合系数$\varepsilon=0.5$,控制参数$\mu=4$,系统迭代10^4次,使系统的每个格子产生序列的长度为10^4,为减少初始值的影响删除每个格



(a) PRCML(r=183)　(b) DRCML(r=183)　(c) DRCML(r=120)　(d) DRCML(r=45)

图 11　PRCML 与 DRCML 系统相关系数对比



(a) NCML　(b) LDMLNCML　(c) PRCML　(d) DRCML

图 12　各系统分别在 ε=0.25,0.5,0.75 的回归映射图

子生成序列的前 1 500 个元素,然后将剩余序列等分为 400 个片段,统计每个片段中的序列元素的数量,各系统序列生成的频率分布如图 13 所示.

如图 13 所示,图 13(a)NCML 系统在生成的序列集中在值 0.5 附近,图 13(b)LDMLNCML 系统生成的序列集中在值域[0.8, 1]附近,通过对比发现图 13(c)PRCML 系统以及图 13(d)DRCML 系统各个格子生成的序列分布在值域[0,1]上,明显优于前两种系统,并且 DRCML 的分布均匀性更好.

3.5　NIST 测试

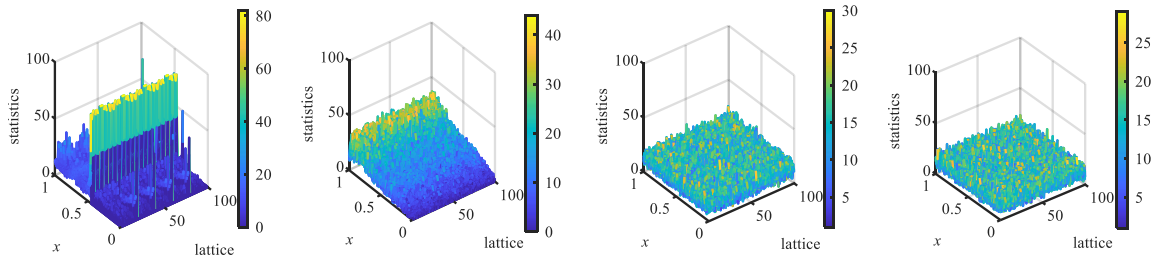
NIST SP800-22 套件由美国国家标准与技术研究所开发,是评估序列随机性和不可预知性的重要统计测试工具,本文使用该套件来检测 DRCML 系统生成数据的随机性.

首先,采用元胞 r=183 迭代规则,系统的控制系数 $\mu=4$,耦合系数为 $\varepsilon=0.5$,迭代 10^6 次,其中 DRCML 系统包含 100 个格子,每个格子产生的序列长度为 10^6,将生成的(0,1)随机序列进行量化,量化函数如下

$$\boldsymbol{y}=\text{unit}\,32[\text{floor}(\boldsymbol{x}\times 2^{32})] \tag{14}$$

其中,floor(·)函数是向下取整函数,unit 32(·)表示将元素转换为 32 位无符号整数,$\boldsymbol{y}$ 为 32 位无符号数. 将生成的十进制数序列 $\boldsymbol{x}$ 被量化为 0 到 2^{32} 之间的 32 位无符号数,通过按位提取操作,共得到 100 组数据,每组数据包含 32 条长度为 10^6 不同的“01”序列,选取第 32 位“01”序列进行测试,测试结果如表 3 所示.

表 3 为序列通过 NIST 检测结果,根据 NIST SP800-22 测试标准,通过率区间为



(a) NCML (b) LDMLNCML (c) PRCML (d) DRCML

图 13 NCML、LDMLNCML、PRCML、DRCML 系统输出均匀性分析

$$\hat{p}\pm 3\sqrt{\frac{\hat{p}\times(1-\hat{p})}{m}},\hat{p}=1-\alpha \tag{15}$$

其中，m 为样本数. 在本次检测中，设置显著性水平 $\alpha=0.01$，$p>10^{-4}$，就认为该序列是是随机的，置信水平为 99%. 通过表 3 结果可知，p 值均大于 10^{-4}，并且通过率都在 96% 以上，显然经过量化后生成的序列通过了 NIST 检验，并且后续测试了其余 31 条数据也均通过了 NIST 测试. 因此，本文提出的系统具有良好的随机性，在密码学领域以及序列密码等方面有广阔的应用领域.

表 3 NIST 随机性检测结果

序号	测试项	P 值	通过率	结果
1	Frequency	0.971 699	98/100	通过
2	Block Frequency	0.739 918	100/100	通过
3	Cumulative Sums*	0.383 827	97/100	通过
4	Runs	0.759 756	98/100	通过
5	Longest Run	0.122 325	100/100	通过
6	Rank	0.997 823	98/100	通过
7	FFT	0.759 756	97/100	通过
8	Nonoverlapping Template*	0.798 139	97/100	通过
9	Overlapping Template	0.739 918	96/100	通过
10	Universal	0.319 084	99/100	通过
11	Approximate Entropy	0.867 692	99/100	通过
12	Random Excursions*	0.116 519	55/57	通过
13	Random Excursions Variant*	0.095 617	56/57	通过
14	Serial*	0.191 687	99/100	通过
15	Linear Complexity	0.474 986	100/100	通过

注：图中带“*”表示该测试用例还包括多个子测试，此处列出了最差结果.

3.6 计算复杂度分析

计算复杂度反映了执行目标算法在时间和空间上的消耗，为开发实用软件提供指导. 对于时间复杂度：与 NCML、LDMLNCML、PRCML 一样，所提出的 DRCML 系统在其计算过程中也有两个嵌套“for”循环. 外部“for”循环通过 N 次迭代运行动态系统，而内部“for”循环遍历 L 格. 因此，本文中提到的 4 个基于 CML 的系统都具有二次时间复杂度，即 $O(NL)$. 其次对于空间复杂性：由于需要保存生成的大小为 $N\times L$ 的伪随机矩阵，这就需要二次元的空间复杂度 $O(NL)$. 与 NCML 和 LDMLNCML 系统相比 PRCM 和 DRCML 系统虽不需要占用额外的空间来保存由辅助混沌映射得到的中间变量，但需要占用额外的空间来保存 ECA 的状态值. 但由于这些占用的中间变量均可以在两个嵌套的“for”循环中单独执行，所以最终的空间复杂度为 $O(NL)$ 保持不变. 本文使用 MATLAB R2021a 软件在 Intel（TM）Core i5-11500 CPU、32 GB 内存和 Windows 11 操作系统的计算机上评估相关系统的性能. 通过仿真计算了 100 个格子迭代 1 000 次共生成 195 KB 的密钥流的平均时间，并计算了额外所需空间大小，系统控制系数 μ 的变化数量为 100，其结果如表 4 所示.

表 4 时间消耗与额外空间大小

种类	NCML	LDMLNCML	PRCML	DRCML
消耗时间/s	0.574 2	0.606	0.772 3	0.911 6
额外空间大小/KB	65	67	74	78

表 4 列出了仿真结果，时间复杂度上，由于 DRCML 和 PRCML 系统中 ECA 会随着系统不断迭代，因此消耗时间较 NCML 和 LDMLNCML 系统的消耗时间明显有所增加，其中 DRCML 系统消耗时间最长. 空间复杂度上，DRCML 系统较 NCML 只增加了 13 KB，显然空间大小并无太大变化，并且对于现代设备来说 78 KB 几乎可以忽略不计，因此作为图像加密的伪随机数发生器计算复杂度上处于可接受范围.

3.7 密钥敏感性分析

密钥敏感性分析是证明加密算法对密钥变化敏感性的重要分析之一. 如果密钥其中一个比特的变化往往会产生不同的密码图像，则证明该密码系统是有效的. 假设系统的精度为 10^{-15}，分别设置一个正确密钥 $K=\{\mu=3.7,\lambda=0.05,\varepsilon=0.5\}$ 和设置两个仅改变正确密钥中的一位进行对比

$$\begin{cases}K_1=\{\mu=3.7+10^{-15},\lambda=0.05,\varepsilon=0.5\}\\K_2=\{\mu=3.7,\lambda=0.05+10^{-15},\varepsilon=0.5\}\end{cases} \tag{16}$$

将量化后序列的第32位“01”序列作为密钥流与大小为1 024×1 024的Male图像进行异或加密,通过像素变化率(Number of Pixel Changing Rate,NPCR)和归一化平均变化强度(Unified Averaged Changed Intensity,UACI)来确定上述密文间差异进行定量估计,NPCR和UACI计算公式为[12]

$$\mathrm{NPCR}(\boldsymbol{I}_1,\boldsymbol{I}_2)=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\mathrm{sign}\left(\boldsymbol{I}_1(i,j)-\boldsymbol{I}_2(i,j)\right)\right|\times 100\% \tag{17}$$

$$\mathrm{UACI}(\boldsymbol{I}_1,\boldsymbol{I}_2)=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|\boldsymbol{I}_1(i,j)-\boldsymbol{I}_2(i,j)\right|}{F}\times 100\% \tag{18}$$

其中,M,N表示密文图像大小,$(i,j)(i=1,2,\cdots,M;\ j=1,2,\cdots,N)$表示像素值索引,$F$表示支持的最大像素值,$\mathrm{sign}(\cdot)$表示符号函数,$\boldsymbol{I}_1,\boldsymbol{I}_2$表示两张不同图片. 原始密钥与两种不同密钥加密Male图像后生成图像间NPCR和UACI值如表5所示.

表5　不同密钥生成图像的NPCR和UACI值对比

密钥种类	NPCR	UACI
K,K_1	99.610 3%	33.444 7%
K,K_2	99.603 7%	33.478 1%
K,K	0	0

通过表5可知,在相同密钥情况下,加密后的图像NPCR以及UACI的值均为0,而在DRCML系统的控制参数以及初始值进行微小改变时,两种不同密钥加密后的图像与原始图像的NPCR值均大于临界值99.599 4%,并且UACI值大小处于临界区域[33.418 3%,33.508 8%]之内[12]. 因此,两种密钥加密后图像之间没有关联,加密图像过程中对密钥的变化十分敏感,系统具有较高的密钥敏感性.

4　结论

在ECA的基础上我们设计了一种MECA,使其具有更长的周期性以及更低的自相关性,在此基础上通过MECA的初始元胞为每个格子添加不同的扰动数值,并根据MECA的迭代结果得到新的耦合方案,有效缓解了混沌系统应用于有限精度数字计算机时产生的动力学退化. 通过Kolmogorov-Sinai熵、分岔图、回归映射图、输出序列均匀性分析、相关分析和NIST SP800-22测试等标准对所提出系统的动态特性进行分析,并且通过密钥敏感性测试,证明提出的系统对初始值具有较好的密钥敏感性. 通过对比发现所提出的系统具有更复杂的动态特性,并且系统的非周期性、均匀性、相关性和随机性相比其它系统都得到了显著改善. 综上所述,DRCML系统具有更大的参数范围,因此具有更多的密钥和更大的密钥空间等新特点,在密码学领域具有广阔的应用前景.

参考文献

[1] 张轶, 翟盛华, 陶海红. 雨衰时间序列的混沌识别与预测[J]. 电子学报, 2023, 51(2): 365-371.
ZHANG Y, ZHAI S H, TAO H H. Chaos identification and prediction for rain attenuation time series[J]. Acta Electronica Sinica, 2023, 51(2): 365-371. (in Chinese)

[2] 赵耿, 马英杰, 陈磊, 等. 基于扰动时空混沌系统的动态S盒设计[J]. 电子学报, 2022, 50(8): 2037-2042.
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. (in Chinese)

[3] 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.

[4] 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, JERRY Gao, et al. Cryptographic feature analysis on 2D coupled map lattices based on piecewise logistic map[J]. Acta Electronica Sinica, 2019, 47(3): 657-663. (in Chinese)

[5] WANG C F, DI Y, TANG J Y, et al. The dynamic analysis of a novel reconfigurable cubic chaotic map and its application in finite field[J]. Symmetry, 2021, 13(8): 1420.

[6] 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.

[7] 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.

[8] ZHOU Y C, HUA Z Y, PUN C M, et al. Cascade chaotic system with applications[J]. IEEE Transactions on Cybernetics, 2015, 45(9): 2001-2012.

[9] LAN R S, HE J W, WANG S H, et al. Integrated chaotic systems for image encryption[J]. Signal Processing, 2018, 147: 133-145.

[10] LIU L F, XIANG H Y, LI X J. A novel perturbation method to reduce the dynamical degradation of digital chaotic maps [J]. Nonlinear Dynamics, 2021, 103(1): 1099-1115.

[11] CARDOSO W B, AVELAR A T, BAZEIA D. Effects of chaotic perturbations on a nonlinear system undergoing two-soliton collisions[J]. Nonlinear Dynamics, 2021, 106

(4): 3469-3477.
[12] 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.
[13] KANEKO K. Pattern dynamics in spatiotemporal chaos Pattern selection, diffusion of defect and pattern competition intermettency[J]. Physica D Nonlinear Phenomena, 1989, 34(1/2): 1-41.
[14] 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.
[15] 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.
[16] 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.
[17] HUANG R, HAN F, LIAO X J, et al. A novel intermittent jumping coupled map lattice based on multiple chaotic maps[J]. Applied Sciences, 2021, 11(9): 3797.
[18] 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.
[19] XIAN Y J, WANG X Y TENG L, et al. Cryptographic system based on double parameters fractal sorting vector and new spatiotemporal chaotic system[J]. Information Sciences, 2022, 596: 304-320.
[20] WANG X Y, DU X H. Pixel-level and bit-level image encryption method based on Logistic-Chebyshev dynamic coupled map lattices[J]. Chaos, Solitons & Fractals, 2022, 155: 111629.
[21] WANG X Y YANG J J. Spatiotemporal chaos in multiple coupled mapping lattices with multi-dynamic coupling coefficient and its application in color image encryption[J]. Chaos Solitons and Fractals, 2021, 147: 110970.
[22] 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.
[23] VON NEUMANN J, BURKS A W Theory of Self-Reproducing Automata[M]. Urbana: University of Illinois Press, 1966.
[24] 董有恒, 赵耿, 马英杰. 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[J]. 通信学报, 2022, 43(1): 71-82.
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. (in Chinese)
[25] 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.

作者简介

赵 耿 男,1964年2月出生于四川省苍溪市. 博士,教授,主要研究领域为混沌密码理论及应用. 中国电子学会会员编号:E190005205S.
E-mail: zg@besti.edu.cn

吴 锐 男,1997年10月出生于安徽省桐城市. 硕士,主要研究领域为混沌保密通信.
E-mail: ruiwu@stu.xidian.edu.cn

马英杰 女,1979年6月出生于吉林省通化市. 博士,副教授,主要研究领域为混沌保密通信.
E-mail: dmzm12@163.com

董有恒 男,1995年5月出生于山东省济宁市. 博士,主要研究领域为混沌密码学.
E-mail: Dyh_231@bupt.edu.cn

黄思婕 女,1998年5月出生于山西省抚州市. 硕士,主要研究领域为混沌扩频通信.
E-mail: 20011210147@stu.xidian.edu.cn