整数帐篷映射周期现象的分析及抵抗策略研究

李 博 刘建东 钟 鸣 刘玉杰 徐浩强
(北京石油化工学院信息工程学院 北京 102617)

摘 要 该文设计一种改进型耦合动态整数帐篷映射模型,引入 Rabbit 流密码中的计数器机制。针对整数帐篷映射的短周期现象,从扩展精度、动态扰动和扩展维度三个角度,对四种不同的整数帐篷映射模型生成的混沌序列进行周期性分析,证明了改进型模型能够较大地改善整数帐篷映射的短周期现象。针对该模型的相关性、初值敏感性、离散 Lyapunov 指数、NIST 随机性等混沌特性进行仿真分析,结果表明该模型性能优越,具有极高的密码学应用价值。

关键词 整数帐篷映射 短周期 有限精度 混沌密码

中图分类号 TP309.7 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.06.049

ANALYSIS OF PERIODIC PHENOMENA OF INTEGER TENT MAPPING AND STUDY OF RESISTANCE STRATEGIES

Li Bo Liu Jiandong Zhong Ming Liu Yujie Xu Haoqiang
(*College of Information Engineering, Beijing Institute of Petrochemical Technology, Beijing 102617, China*)

Abstract An improved coupled dynamically integer tent mapping model is designed and a counter mechanism in Rabbit stream cipher is introduced in this model. Aimed at the short-period phenomenon of integer tent mapping, the chaotic sequence generated by four different integer tent mapping models was analyzed periodically from the perspectives of extended precision, dynamic disturbance and extended dimension. It was proved that the improved model could greatly improve the short-period phenomenon of integer tent mapping. According to the chaotic characteristics of the model, such as correlation, initial value sensitivity, discrete Lyapunov index, randomness of NIST, etc., simulation analysis was carried out. The results show that the model has excellent performance and high cryptography application value.

Keywords Integer tent mapping Short period Finite accuracy Chaos cryptography

0 引 言

混沌运动具有不可预测性和伪随机特性,这是确定性非线性系统最具吸引力的地方,确定性与随机性、有序性与无序性的结合,呈现为一种矛盾对立统一关系。这种伪随机不稳定的特性在部分控制系统中是不被允许的存在,但相反在密码学中有着重大价值,并且混沌的初值敏感性以及有界遍历性与密码学相符合,依据这些特性,近年来混沌密码算法的研究已经取得较大进展[1-3]。

尽管混沌密码算法的研究已经十分广泛,但是却有着不可忽视的两个问题,一是传统密码算法工作在有限离散集,而混沌密码却是在实数域上构造的。由于实数域上存在着无穷多的无理数,不可避免会对混沌密码的计算产生影响;二是计算机有限精度效应引起的短周期问题,短周期意味着弱密钥[4]。由于以上两个根本原因,混沌密码算法的安全性尚且无法得到人们的信任。

与混沌密码算法研究形成鲜明对比的是,由 Cryptico 公司设计的 Rabbit 流密码[5]取得了巨大成功,Rabbit 流密码是利用整数式迭代实现的。它是目前安全性较高、加解密速度极快的流密码之一,在各种处理器平台上都有不凡的表现。因此可以将其构造思想迁

收稿日期:2020-12-30。北京市教委面上项目(KM201810017005)。**李博**,硕士生,主研领域:混沌密码,图像加密。**刘建东**,教授。**钟鸣**,硕士生。**刘玉杰**,硕士生。**徐浩强**,硕士生。

移到混沌密码算法设计中,并将混沌映射变换到整数集内实现,具有运算简单、速度快的特点,且在运算方式上与传统密码算法具有很好的一致性,可充分发挥其拉伸与折叠的非线性本质及良好的均匀分布特性及平衡特性来完成混淆与扩散操作。数字化后的混沌映射定义在了有限整数集上,但其动力学特性却有所退化,其固有的短周期现象必须加以解决以满足密码学对安全性能的要求。

目前的主流混沌密码算法针对短周期现象的解决方式大多采用扩展精度、增加扰动和扩展维度三种方法。文献[6]中根据迭代次数的奇偶性进行扩展,将生成序列的周期扩展到 $2(n+1)$,但周期大小受到极大限制。文献[7]将精度定义为实数计算中的小数点后可以表示出的最小精确度,对 Logistic 映射进行精度的可扩展性研究,并基于此设计了一种并行化计算的算法,但却牺牲了算法的可移植性。文献[8]提出了将帐篷映射与取模运算结合,并引入动态参量,对整数帐篷映射的短周期现象起到了部分的改善作用。许多研究证明了多种混沌映射组合的方式可进一步提高算法安全性[9-11],有着更好的密码学应用前景,却牺牲了算法的执行效率。

近年来混沌映射的动力学特性研究陆续有新的进展,证明了混沌密码的安全可靠。针对于混沌映射的短周期问题有了许多研究成果[12-13],但整数帐篷映射短周期现象领域的研究仍然有许多空白。

本文设计了一种改进型耦合动态整数帐篷映射模型,引入了 Rabbit 流密码中的计数器来驱动动态参量。本文以整数帐篷映射为例,从扩展精度、动态扰动及扩展维数的三种主流解决方法,对四种不同整数帐篷映射进行周期性分析,填补了整数帐篷映射短周期领域研究的空白,最后针对本文提出的改进型模型的混沌特性进行了详细分析,从相关性、初值敏感性、Lyapunov 指数以及 NIST 随机性等仿真分析结果来看,模型能够生成均匀分布且相互独立的伪随机序列,具有优越的混沌特性,在混沌密码学领域有着较高的应用价值。

1　帐篷映射及整数帐篷映射模型

帐篷映射的定义为:

$$F_\alpha: x_{i+1} = \begin{cases} \dfrac{x_i}{\alpha} & 0 \leqslant x_i < \alpha \\ \dfrac{1-x_i}{1-\alpha} & \alpha \leqslant x_i \leqslant 1 \end{cases} \tag{1}$$

该映射是均匀分布的。当参数 $\alpha = 0.5$ 时帐篷映射为满映射,将其由实数域运算等价转化为整数域运算,得到整数帐篷映射:

$$F_\beta: x_{i+1} = \begin{cases} 2x_i & x_i \in [0, 2^{n-1}) \\ 2(2^n - 1 - x_i) + 1 & x_i \in [2^{n-1}, 2^n - 1] \end{cases} \tag{2}$$

式中:i 为迭代次数,n 为有限精度。式(1)的乘(除)法运算在有限整数域内转化为式(2)的移位操作[14]。映射 F_β 仍可由折线表示,并服从定义域 $[0, 2^n - 1]$ 上的均匀分布。

动态整数帐篷映射模型将整数帐篷映射与取模运算结合,引入动态参量,仍保持特有的伸长和折叠特性,其伸长特性使相邻迭代值指数分离,其折叠特性保持序列有界遍历。公式如下:

$$F_\gamma: x_{i+1} = \begin{cases} 2g_i & g_i \in [0, 2^{n-1}) \\ 2(2^n - 1 - g_i) + 1 & g_i \in [2^{n-1}, 2^n) \end{cases} \tag{3}$$

$$g_i = (x_i + k_i) \bmod 2^n \tag{4}$$

式中:mod 为取模运算;2^n 为格点状态变量的取值上限。图 1 中动态参量 k_i 控制 F_γ 映射的“帐篷”水平移动。

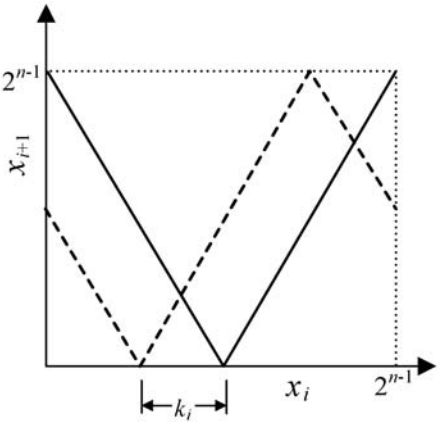


图 1　动态整数帐篷映射

文献[12]证明了耦合映像格子与混沌系统紧密结合可以具有极高的安全性。基于此,文献[15]更进一步地将动态整数帐篷映射作为耦合映像格子模型中的非线性函数,增强模型的混乱与扩散特性。耦合映像格子模型是非线性时空混沌领域中的一种重要模型。

耦合动态整数帐篷映射的定义如下:

$$x_{j,i+1} = (f[g_{j,i}] + f[g_{j-1,i}] + f[g_{j+1,i}]) \bmod 2^n \tag{5}$$

$$f[g_{j,i}] = \begin{cases} 2g_{j,i} & g_{j,i} \in [0, 2^{n-1}) \\ 2(2^n - 1 - g_{j,i}) + 1 & g_{j,i} \in [2^{n-1}, 2^n) \end{cases} \tag{6}$$

$$g_{j,i} = (x_{j,i} + k_{j,i}) \bmod 2^n \tag{7}$$

式中:$x_{j,i}$ 表示第 j 个格点的第 i 步迭代所得状态变量值;n 为系统精度(本文中为计算机字长)。式(7)中非线性函数 f 选用动态整数帐篷映射式(3),耦合整数帐篷映射中三个相邻格点值决定下一次迭代的格点值。每一个格点的变化可以影响到下一次迭代的三个

格点,这种耦合方式有利于信息的混乱与扩散。

2 改进型耦合动态整数帐篷映射模型设计

动态参量 $k_{j,i}$的选择与短周期现象密切相关,本文引入 Rabbit 流密码中的计数器以驱动耦合动态整数帐篷映射模型中的动态参量 $k_{j,i}$,消除整数帐篷映射的短周期现象。改进型耦合动态整数帐篷映射模型流程如图 2 所示。

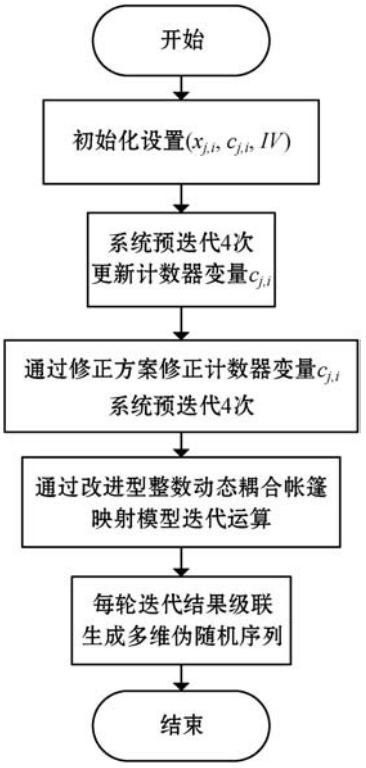


图 2 改进型耦合动态整数帐篷映射模型流程

具体步骤说明如下:

(1) 初始设置耦合格点 $L=8$,表示有 8 个状态变量 $x_{j,i}$和 8 个计数器变量 $c_{j,i}$,其中 j 为格点序号,i 为迭代次数,每个变量长度为 32 bit。

(2) 计数器系统和耦合动态整数帐篷映射模型进行预迭代 4 次,使整个系统处于混沌状态,通过式(8)对预迭代 4 次后的 8 个计数器变量($j=0,1,\cdots,7$)进行更新,以防止逆运算破解。

$$c_{j,4}=c_{j,4}\oplus x_{(j+4\bmod 8),4} \tag{8}$$

(3) 设置修正方案中所需的 IV 变量,IV 长度为 64 bit。修正方案的意义在于通过 IV 变量来修正计数器变量,进行 IV 变量与 8 个计数器变量之间的运算,公式如下:

$$c_{0,4}=c_{0,4}\oplus IV^{[31..0]} \quad c_{1,4}=c_{1,4}\oplus(IV^{[64..48]}\diamond IV^{[31..16]})$$
$$c_{2,4}=c_{2,4}\oplus IV^{[64..32]} \quad c_{3,4}=c_{3,4}\oplus(IV^{[47..32]}\diamond IV^{[15..0]})$$
$$c_{4,4}=c_{4,4}\oplus IV^{[31..0]} \quad c_{5,4}=c_{5,4}\oplus(IV^{[64..48]}\diamond IV^{[31..16]})$$
$$c_{6,4}=c_{6,4}\oplus IV^{[64..32]} \quad c_{7,4}=c_{7,4}\oplus(IV^{[47..32]}\diamond IV^{[15..0]})$$

式中:⊕为按位异或符;◇为连接运算符。系统预迭代 4 次,使系统状态变量与 IV 变量之间线性无关,修正后的计数器变量确保将 2^{64}大小的 IV 变量引向不同的映射轨道。

(4) 计数器的动力学定义如下:

$$c_{j,i+1}=\begin{cases}c_{0,i}+a_0+\varnothing_{7,i}\bmod 2^{32} & j=0\\ c_{j,i}+a_j+\varnothing_{j-1,i+1}\bmod 2^{32} & j>0\end{cases} \tag{9}$$

通过判断格点序号 j 的大小选用不同的函数更新计数器变量,取模运算确保计数器的有界性,式(9)中 $\phi_{j,i+1}$初始化为 0,通过式(10)迭代。

$$\varnothing_{j,i+1}=\begin{cases}1 & c_{0,i}+a_0+\varnothing_{7,i}\geqslant 2^{32}\wedge j=0\\ 1 & c_{j,i}+a_j+\varnothing_{j-1,i+1}\geqslant 2^{32}\wedge j>0\\ 0 & \text{其他}\end{cases} \tag{10}$$

该公式依据计数器系统,判别是否超过取值上界 2^{32}与格点序号 j 是否为“0”两个条件,进行赋值。其中常量 a_j 定义如下:

$$a_0=a_3=a_6=0x4D34D34D$$
$$a_1=a_4=a_7=0xD34D34D3$$
$$a_2=a_5=0x34D34D34$$

(5) 改进型耦合动态整数帐篷映射模型。计数器驱动的动态参量 $k_{j,i}$定义如下:

$$k_{j,i}=((x_{j,i}+c_{j,i})^2\oplus((x_{j,i}+c_{j,i})^2\gg n))\bmod 2^n \tag{11}$$
$$g_{j,i}=(x_{j,i}+k_{j,i})\bmod 2^n \tag{12}$$
$$x_{j,i+1}=(f[g_{j,i}]+f[g_{w,i}]+f[g_{v,i}])\bmod 2^n \tag{13}$$

f 选用上述的改进后的整数动态帐篷映射模型作为非线性函数,耦合空间格点位置 w、v 则由猫映射得出,j、w、v 的取值范围为{0,1,…,7};本模型迭代生成下一格点序列的过程如图 3 所示,图中的①、②、③进行的运算分别对应式(11)、式(12)、式(13)。

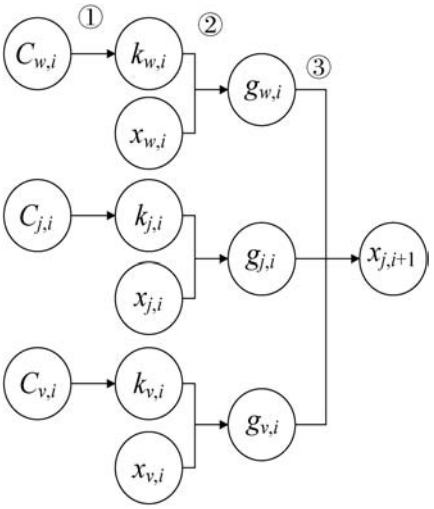


图 3 模型迭代运算过程

改进型模型内部由 513 位组成,分为 8 个 32 位状

态变量 $x_{j,i}$、8 个计数器变量 $c_{j,i}$和一个计数器进位 $\phi_{j,i}$,从内部状态位的组合中每次迭代生成一个 128 位的伪随机序列输出,可以将伪随机数据用于加密领域。该模型可以对多达 264 块的明文进行加密,且密钥的大小为 128 位,修正方案确保了不可能进行逆运算等,除穷举攻击外无其他简单的攻击方法。在第四部分针对本文模型生成的伪随机序列进行性能分析。

3　整数帐篷映射周期性分析

计算机的有限精度条件下意味着数字化混沌系统不可能存在真正意义上的混沌轨道,只可能使混沌轨道周期无限制增大[12]。整数帐篷映射是通过帐篷映射离散化定义在有限域内,必然存在周期现象,其混沌特性退化严重。短周期现象的存在也是一些学者质疑数字化混沌系统安全性的主要因素[7]。

针对整数帐篷映射的周期性是评判混沌映射模型优劣性的重要因素。与混沌本身的吸引子不同,计算机有限精度引起的短周期问题,可能导致存在许多周期轨道[12]。整数混沌系统的短周期现象是混沌密码算法的一个安全缺陷,实际应用中,混沌密码算法所选用混沌映射的周期性应尽可能大。本文从周期长度对比和相空间轨道两个方面针对整数帐篷映射进行周期性分析。

3.1　周期对比分析

本文的精度定义为计算机字长 n。由于有限精度效应,一个字长为 n 的计算机,通过混沌映射生成伪随机序列时,最多迭代 2^n 次,序列势必会进入周期状态,出现重复点甚至平衡点(不动点)。打破短周期行为的方法,基本可分为三个类别:扩展精度、动态扰动及扩展维数。对于整数帐篷映射(式(2)),一个完整的迭代周期 T 为:初始状态值 x_0 经过迭代 i 次后,迭代值 x_i 回归初始值,开始出现重复点,采用最短迭代轮数,即 $x_i = x_0$($i>0$ 且取最小值)[8],此时周期长度 $T = i$。加入动态扰动和扩展维度后的模型在遵循整数帐篷映射的周期判定方式的基础上,需要考虑动态扰动和多维度因素对周期的影响,具体判定方式如表 1 所示,表中 i 为迭代次数,j 为耦合格子序号,$\wedge$ 为运算符与。

表 1　不同模型周期判别方式

模型类型	周期判别方式
整数帐篷映射	$x_i = x_0$
动态整数帐篷映射	$x_i = x_0$ && $k_i = k_0$
二维整数帐篷映射	$x_i = x_0$ && $y_i = y_0$

续表 1

模型类型	周期判别方式
耦合整数帐篷映射	$x_{j,i} = x_{j,0}(j=0,1,\cdots,7)$
本文模型	$x_{j,i} = x_{j,0}$ && $k_{j,i} = k_{j,0}(j=0,1,\cdots,7)$

本文将精度定义为计算机字长 n,编写了周期分析程序,计算相同条件下从扩展精度的角度分别对整数帐篷映射、动态整数帐篷映射、耦合整数帐篷映射及二维整数帐篷映射等模型的周期。周期测试条件设定为:取精度 $n=3$ 至 10 bit 的状态变量 x_i,定义状态变量 x_i 为整型变量,对于定义域内$[0-2^n)$的初始值遍历,进行 2^n 轮周期测试,计算得到四种模型的生成序列随精度变化的周期分布关系。测试结果如图 4 – 图 7 所示。

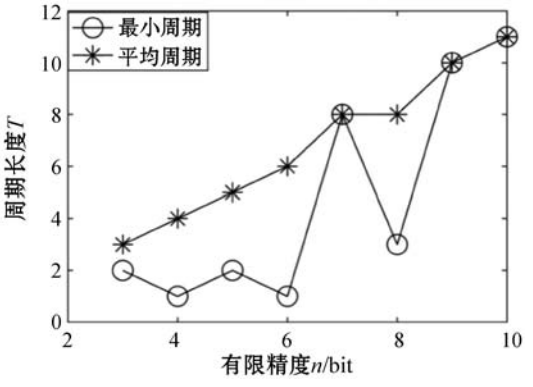


图 4　不同精度下整数帐篷映射周期分布图

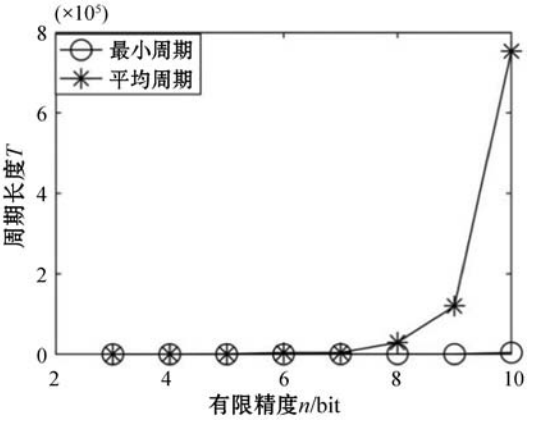


图 5　不同精度下动态整数帐篷映射周期分布图

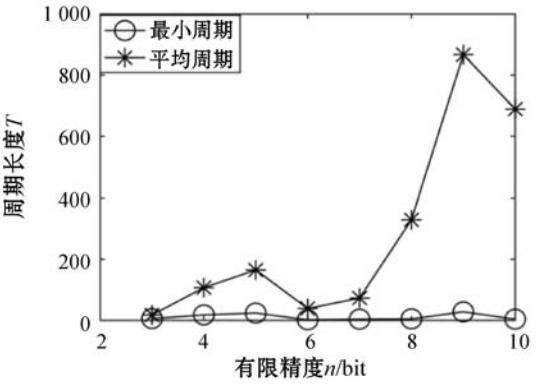


图 6　不同精度下耦合整数帐篷映射周期分布图

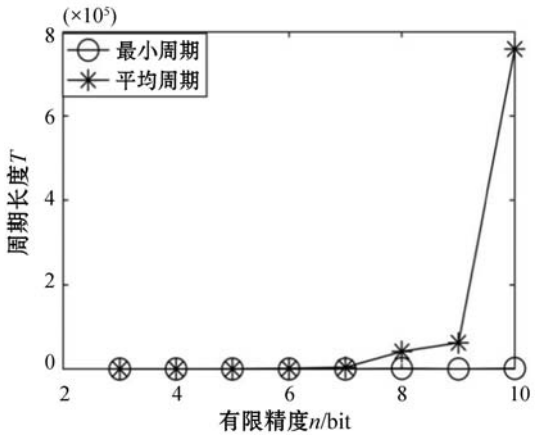


图 7 不同精度下二维整数帐篷映射周期分布图

图 4 显示了整数帐篷映射模型随着精度的扩展，周期长度 T 的大小整体呈上升趋势，但动力学特性退化严重，陷入周期轨道。动态扰动机制的实质是通过增加动态参量，以求打破整数帐篷映射模型的固定周期轨道。图 5 为动态整数帐篷映射模型的周期分布图。随着精度 n 的增加，其周期指数级增长。

扩展维度的方法为耦合映像格子模型和二维模型[16]。耦合整数帐篷映射保留有帐篷映射独特的拉伸折叠特性，通过同一迭代时刻不同格子间的相互作用，加以取模运算等多重非线性作用，以求打破固定的周期轨道，如式(7)所示。二维整数帐篷映射则通过增加迭代运算复杂度的方式，使得迭代值 x_i、y_i 对下一迭代值 x_{i+1}、y_{i+1} 的生成加以影响，即二维模型生成的两个序列 X、Y 之间相互作用。周期测试结果如图 6 - 图 7 所示，耦合模型改善短周期现象的效果并不理想，二维模型则取得了一定的改善效果。通过以上分析得出，四种模型的周期长度均随着精度的扩展有所增长，扩展精度不失为解决短周期问题的一种方法，动态扰动和扩展维度从一定程度上也可以改善模型的短周期现象，但仍然不能在根本上打破模型的短周期轨道。

混沌映射的短周期现象是混沌密码算法的安全短板。计算机最小存储单元为字节 byte。本文选取计算精度 $n=8$ bit，即一个字节 byte，计算模型的周期长度，将上述四种模型与本文提出模型进行对比分析，结果如表 2 所示。可以看出，整数帐篷映射以及耦合整数帐篷映射的最小周期均为个位数，出现了重复点和不动点。动态模型以及二维模型在初值遍历的条件下，最小周期的大小虽然超过了取值空间的大小，但其安全性仍然不够。相比之下本文提出的由计数器驱动的改进型映射模型的最小周期长度远远大于映射取值空间，在精度不大的情况下周期足够长，避免出现重复点以及不动点，从而打破模型固有的周期轨道。

整数帐篷映射的短周期现象仍存在着一些其他影响因素，例如初始值的设定。对于整数帐篷映射，仿真分析得出绝大部分短周期轨道与初始值设定无关，但可能会导致陷入不动点或周期很短的轨道，在精度 n 确定的条件下，初始值不同导致整数帐篷映射存在很多相同大小的周期轨道，一定程度上证明了整数帐篷映射的混沌特性。

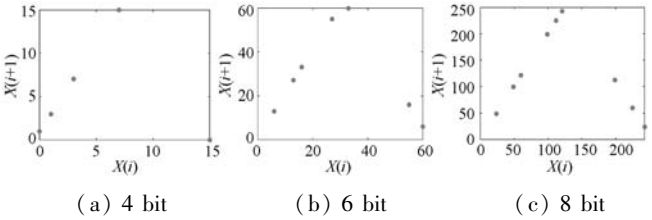
表 2 8 bit 下不同模型的周期长度

模型名称	最小周期	平均周期
整数帐篷映射	3	8
耦合整数帐篷映射	5	329
动态整数帐篷映射	512	29 654
二维整数帐篷映射	1 407	41 510
本文模型	>1 000 000	>1 000 000

本文编写的周期分析程序原则上适用于无穷长字长条件，考虑到计算机算力及周期分析程序复杂度的影响，精度 n 大于 10 bit 耗时极大，同时精度 n 越小越容易陷入周期轨道，以上所得测试结果已具有较强的代表性。目前主流计算机字长均为 32、64 位，将精度 n 扩展到 32、64 bit，本文提出的改进型耦合动态整数帐篷映射模型势必可以更好地打破整数帐篷映射的短周期轨道。

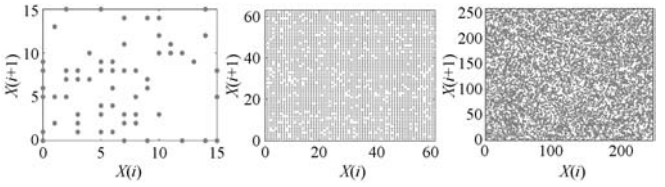
3.2 相空间轨道分析

相空间分析用来研究时间序列中，上一迭代值 x_i 对后一个迭代值 x_{i+1} 的影响。对比整数帐篷映射模型与本文模型在精度 n 为 4、6、8 bit 下迭代 10 000 次生成序列的相空间结构图。图 8 为整数帐篷映射模型的相空间结构图，不同精度下的整数帐篷映射均呈现重复点与不动点状态，在局部点上呈现简单的重复和跳跃，且相邻迭代值之间相关性较高。图 9 为本文模型生成序列的相空间结构图，随着精度 n 的增加，相空间轨道呈现混乱无序且有界遍历状态，表明序列安全性较高。与整数帐篷映射模型对比，由计数器驱动的本文模型生成序列的短周期现象明显改善，同时也改善了由整数化引起的帐篷映射动力学特性退化的问题，具有一定的抗混沌退化能力。



(a) 4 bit (b) 6 bit (c) 8 bit

图 8 不同精度下整数帐篷映射生成序列的相空间结构图



(a) 4 bit　(b) 6 bit　(c) 8 bit

图 9　不同精度下本文模型生成序列的相空间结构图

4　模型性能分析

本文提出的改进型耦合动态整数帐篷映射模型,消除了整数帐篷映射的短周期现象,同时其并行生成的多维伪随机序列保留了帐篷映射的混沌特性。下文对本文模型进行了相关性、初值敏感性、离散 Lyapunov 指数 NIST 随机性测试等仿真分析,分析结果表明该模型的生成序列保留了良好的混沌特性,且多维序列之间相互独立,具有良好的混沌密码学特性。

4.1　相关性测试

两个变量之间的 Pearson 相关系数定义为两个变量之间的协方差和标准差的商。对于估算样本来说,Pearson 相关系数常用 r 表示:

$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}} \tag{14}$$

Pearson 相关系数是用协方差除以两个变量的标准差得到的。计算本文模型生成的 8 个伪随机序列两两之间的 Pearson 互相关系数。从表 3 可以看出本文模型的互相关系数远远小于 0.01,不同格点序列值间相关程度较低,序列之间相互独立。

表 3　不同格点序列之间的互相关系数

格点号	L1	L2	L3	L4	L5	L6	L7	L8
L1	1	0.001 3	0.002 2	0.004 4	0.000 4	0.000 8	-0.008 6	0.001 2
L2	-0.001 3	1	-0.001	0.001 7	-0.003 1	0.003 9	0.001 1	0.005 7
L3	-0.002 2	-0.001	1	0.000 5	0.000 6	0.001 4	-0.000 2	0.001 1
L4	0.004 4	0.001 7	0.000 5	1	-0.002 8	0.002	0.000 1	-0.004 8
L5	0.000 4	-0.003 1	0.000 6	-0.002 8	1	-0.007	-0.000 1	-0.005 1
L6	0.000 8	0.003 9	0.001 4	0.002	-0.007	1	0.003 2	0.001 5
L7	-0.008 6	0.001	-0.000 2	0.000 1	-0.000 1	0.003 2	1	-0.002 3
L8	0.001 2	0.005 7	0.001 1	-0.004 8	-0.005 1	0.001 5	-0.002 3	1

自相关是互相关的一种特殊情况,主要用来衡量一个序列在不同迭代时间的状态函数变量取值的相似程度。采用文献[17]中的分析方法,进行序列自相关分析。图 10 为生成序列的自相关系数图,横坐标 lag 表示迭代时间间隔,纵坐标为自相关系数值,图中点表示自相关函数值,直线表示置信区间,置信区间为[-0.01 0.01]。图 10 显示自相关系数值在 0 值上下微小浮动变化,并未超出置信区间,证明一个序列不同迭代时间的状态变量值之间相关程度极低,任一时间格点序列都难以通过其他格点序列来推算得到。

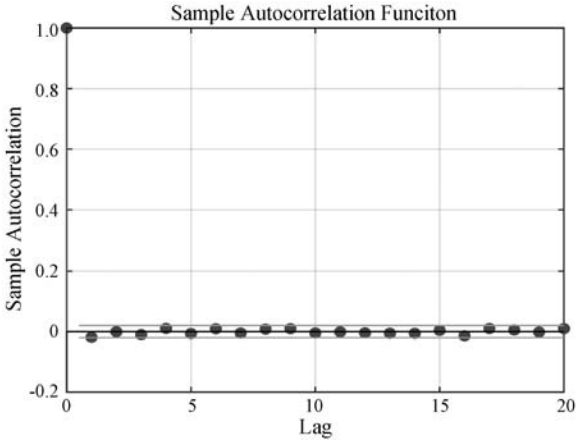


图 10　序列自相关系数图

4.2　初值敏感性

本文所提出的改进型耦合动态整数帐篷映射模型有着较强的初值敏感性,是一种经典的数字化时空混沌模型。初始状态值改变 1 bit,模型的运动轨迹就会发生极大地改变。采用像素变化率(NPCR)测试明文敏感性的方法,测试在初始值相差 1 bit、2 bit、3 bit、4 bit 条件下模型生成序列之间的差异。NPCR 的最佳理想值为 99.609 4%。

针对混沌系统的 NPCR 测试表达式如下:

$$\begin{cases} D(i) = \begin{cases} 1 & X_1(i) \neq X_2(i) \\ 0 & X_1(i) = X_2(i) \end{cases} \\ \mathrm{NPCR} = \dfrac{\sum_i D(i)}{M} \times 100\% \end{cases} \tag{15}$$

仿真结果如图 11 所示,在改变初始值 1 至 4 bit 下,序列的 NPCR 值均在 99.60% 上下小范围浮动,接近于理想值。由此可知,本文模型具有极高的初值敏感性。

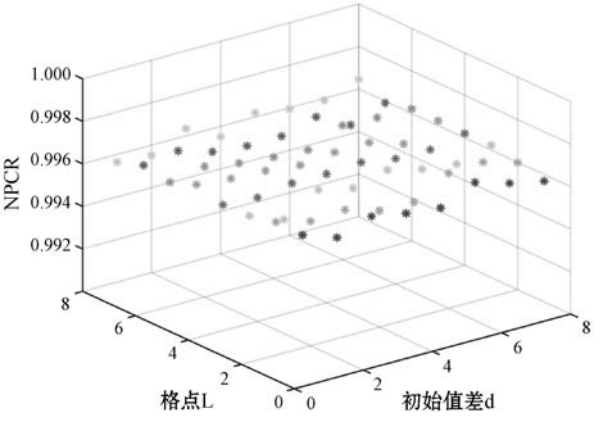


图 11　初值敏感性

4.3 离散 Lypunov 指数

Lyapunov 指数,又称李雅普诺夫特征指数,是识别混沌运动的重要依据之一。Lyapunov 指数为正值则证明模型是混沌的。区别于实数域混沌映射 Lyapunov 指数的计算,文献[18]提出了更具有实用价值的整数域 Lyapunov 指数计算方法:

$$\lambda_F^{(s)} = \frac{1}{M-1}\sum_{i=0}^{M-2} \mathrm{In}\frac{d(2F^s(m_{i+1}),F^s(m_i))}{d(m_{i+1},m_i)} \quad (16)$$

式中:λ 表示模型的最大 Lyapunov 指数;S 表示系统维数;M 表示模型迭代后得到序列的数据长度;d 表示相邻数据点的欧氏距离;F 表示模型的映射关系;m_i 表示模型的数据点。仿真运算结果如图 12 所示,该模型最大离散 Lyapunov 指数值稳定分布在 4 到 6 之间,其值恒大于 0,证明该模型是混沌的。

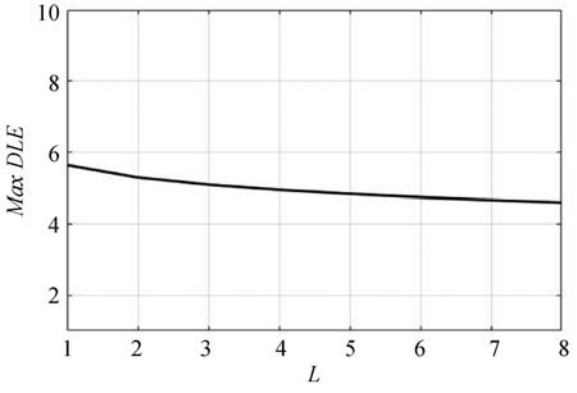


图 12 不同格点序列的最大离散 Lyapunov 指数

4.4 NIST 随机性测试

基于美国国家标准与技术研究院(NIST)提供的 Special Publication 800 - 22 标准,sts-2.1.2 测试套件是由 15 个测试项目组成的统计软件包,可用来测试任意长度的二进制伪随机序列[19]。NIST 测试基于数理统计中假设检验的方法,使用统计量 P_value 进行判定。本次测试取显著性水平 $\alpha = 0.01$,若 P_value $\geqslant \alpha$,则接受原假设,通过该项测试,证明序列是随机的。测试结果如表 4 所示,本文模型生成的序列通过了 NIST 测试的全部测试,具有良好的随机性。

表 4 NIST 随机性测试结果

测试项	P_value(L)
近似熵测试	0.982 4
块内频率测试	0.257 1
累积和测试(前向,反向)	0.509 7 0.395 3
离散傅里叶变换测试	0.182 3
频率测试	0.190 8
线性复杂度测试	0.436 5

续表 4

测试项	P_value(L)
块内最长连续“1”测试	0.731 4
非重叠模板匹配测试	(通过)
重叠模板匹配测试	0.608 0
二元矩阵秩测试	0.550 2
游程测试	0.429 2
序列测试	0.770 4 0.518 5
通用统计检验测试	0.040 6
随机偏移测试	(通过)
随机偏移变化测试	(通过)

5 结 语

本文研究讨论了现阶段混沌理论在密码学应用中遇到的主要问题。从扩展精度、动态扰动和扩展维度三个角度分析不同整数帐篷映射模型的短周期现象,并引用 Rabbit 流密码中的计数器系统驱动动态参量,提出一种改进型耦合动态整数帐篷映射模型。通过周期对比及相空间轨道的研究分析,从而得出该模型解决了整数帐篷映射的短周期问题。针对该模型的相关性、初值敏感性、混沌性及随机性等特性进行仿真分析。研究结果表明,该模型生成的序列改善了帐篷映射整数化以后混沌退化的问题,保留了帐篷映射良好的混沌特性,且序列之间相互独立,随机性良好。本文模型适用于构造哈希函数、构建伪随机序列发生器及图像视频加密等领域。

下一步工作:(1) 解决混沌密码应用环境限制的问题。对于算法设计来说,需要考虑到底层硬件和上层应用的影响。在实际应用中混沌密码对平台的兼容性以及稳定性等有着一定的要求。可将本文模型移植到 Linux 操作系统中进行对比研究。(2) 提高本文模型执行效率。当前计算机配备的是具有多核心多线程的 CPU,可引入并行计算思想,比如采用共享存储并行编程接口(OpenMP),充分释放 CPU 的性能;使用 Hadoop 大数据分布式系统基础架构,搭配基于内存的 Spark 计算引擎构建大数据平台,本文模型利用循环迭代生成伪随机序列的算法可以充分发挥 Spark 计算引擎的优势。

参 考 文 献

[1] Falih S M. A simple chaotic image cryptography algorithm based on new quadratic chaotic map[J]. Journal of University of Babylon,2017,25(4):1255 - 1267.

[2] Alawida M, Samsudin A, The J S, et al. A new hybrid digital chaotic system with applications in image encryption[J]. Signal Processing,2019,160:45 – 58.
[3] Meysam A C, Shahram J, Narhe N K. A novel keyed parallel hashing scheme based on a new chaotic system[J]. Chaos Solitons and Fractals,2016,87:216 – 225.
[4] Shu J L, Xuan Q M, Yuan L C, et al. On the security of a chaotic encryption scheme: Problems with computerized chaos infinite computing precision[J]. Computer Physics Communications,2003,153(1):52 – 58.
[5] Boesgaard M, Vesterager M, Pedersen T, et al. Rabbit: A new high-performance stream cipher [C]//International Workshop on Fast Software Encryption,2003:307 – 329.
[6] 刘建东. 扩展整数帐篷映射与动态散列函数[J]. 通信学报,2010,31(5):51 – 59.
[7] 刘嘉辉,张宏莉. 基于可扩展精度的 Logistic 混沌随机序列的并行计算方法[J]. 中国科学技术大学学报,2011,41(9):837 – 846.
[8] 刘建东,张啸,赵晨,等. 动态整数帐篷映射模型及其性能分析[J]. 计算机科学,2016,43(11):226 – 229.
[9] Ouannas A, Khennaoui A, Bendoukha S, et al. The dynamics and control of the fractional forms of some rational chaotic maps[J]. Journal of Systems Science & Complexity,2020,33(3):584 – 603.
[10] 黄峰,冯勇. 二维混沌映射图像加密安全性分析及改进算法[J]. 哈尔滨工业大学学报,2007(9):1411 – 1414.
[11] Sun Y F, Lv Z W. Digital image encryption with chaotic map lattices[J]. Chinese Physics B,2011,20(4):136 – 142.
[12] 张勇,陈滨. Logistic 映射的有限字长研究[J]. 电子科技大学学报,2006(3):292 – 294,316.
[13] 盛利元,全俊斌. 计算机迭代下混沌序列的周期研究[J]. 计算机应用,2010,30(7):1802 – 1804,1808.
[14] 刘建东. 基于整数耦合帐篷映射的单向 Hash 函数及其性能分析[J]. 计算机研究与发展,2008(3):563 – 569.
[15] 张啸,刘建东,商凯,等. 基于耦合动态整数帐篷映象格子模型的轻量级 Hash 函数[J]. 北京石油化工学院学报,2016,24(1):43 – 48.
[16] 陈飞,刘建东,胡辉辉,等. 二维整数帐篷映射模型设计及安全性仿真分析[J]. 计算机工程与应用,2019,55(1):103 – 108,173.
[17] Nesa N, Ghosh T, Banerjee I. Design of a chaos-based encryption scheme for sensor data using a novel logarithmic chaotic map[J]. Journal of Information Security and Applications,2019,47:320 – 328.
[18] Amigó J M, Kocarev L, Szczepanski J. Theory and practice of chaotic cryptography [J]. Physics Letters A, 2007, 366(3):211 – 216.
[19] Rukhin A, Soto J, Nechvatal J, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications [J]. Applied Physics Letters, 2015, 22(7):1645 – 1679.

(上接第 311 页)

[2] 苏柯文,张永明. 基于改进鸟群算法优化聚类的风电场等值建模[J]. 计算机应用与软件,2021,38(1):266 – 271.
[3] 刘军,张彬彬,赵婷. 基于模糊评价的风电场有功功率分配算法[J]. 电工技术学报,2019,34(4):786 – 794.
[4] Prajapati V, Mahajan V. Congestion management of power system with uncertain renewable resources and plug in electrical vehicle[J]. IET Generation Transmission & Distribution, 2019,13(6):59 – 71.
[5] 张金环,王超群,张彤,等. 基于高斯混合分布模型的风电功率预测误差统计分析研究[J]. 智慧电力,2020,48(7):59 – 64.
[6] Dou F, Cheng J, Wang W, et al. Power system reserve scheduling with wind farm integration considering robust security constraints[J]. Journal of Physics: Conference Series, 2020,16(1):102 – 111.
[7] Li C,Tang G,Xue X, et al. The short-term interval prediction of wind power using the deep learning model with gradient descend optimization[J]. Renewable Energy, 2020,155(6):96 – 108.
[8] 李鉴博,樊小朝,史瑞静,等. 基于互补式集合经验模态分解和 IPSO-LSSVM 的短期风功率预测[J]. 水力发电,2020,46(11):95 – 100.
[9] 孙勇,李宝聚,孙志博,等. 融合 RBF 神经网络和集对分析的风电功率超短期预测[J]. 昆明理工大学学报(自然科学版),2020,45(5):49 – 58.
[10] 薛阳,张宁,俞志程,等. 基于 BiLSTM 和 Bootstrap 方法的风电功率区间预测[J]. 可再生能源,2020,38(8):1059 – 1064.
[11] 熊鸣. 基于 BP 神经网络与非参数核密度估计的短期风电功率概率区间预测[J]. 北京信息科技大学学报(自然科学版),2020,35(4):51 – 56.
[12] 任文凤,冯志亮,杜艳丽. 1 种改进长短期记忆神经网络的风电功率预测[J]. 北华大学学报(自然科学版),2020,21(6):830 – 835.
[13] Hu J,Lin Y,Tang J, et al. A new wind power interval prediction approach based on reservoir computing and a quality-driven loss function[J]. Applied Soft Computing, 2020,92(6):106 – 127.
[14] Wang R,Deng C, et al. Deep learning method based on gated recurrent unit and variational mode decomposition for short-term wind power interval prediction[J]. IEEE transactions on neural networks and learning systems, 2019, 62(6):112 – 123.
[15] Li C,Tang G,Xue X, et al. The short-term interval prediction of wind power using the deep learning model with gradient descend optimization[J]. Renewable Energy, 2020,155(2):114 – 131.