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

王 永[1,2],赵 毅[1],Jerry Gao[3],陈 燕[1]
(1. 重庆邮电大学计算机科学与技术学院,重庆 400065;2. 重庆邮电大学电子商务与物流重点实验室,重庆 400065;
3. 圣何塞州立大学计算机工程系,加利福尼亚州圣何塞 95192)

摘 要: 将分段 Logistic 映射作为局部混沌映射,引入到二维耦合映像格子模型中,构造了一种具有复杂动力学特性的混沌模型. 从密码学应用出发,深入分析了该模型中参数设置对 Lyapunov 指数、分岔、遍历区间和概率密度分布等特性的影响. 分析的结果为将该模型应用于保密通信的参数设置提供了理论依据. 在此基础上,通过引入状态值偏移量,解决了该模型状态值概率密度分布不均的问题,研究结果表明本文模型具有良好的性能,为将其应用于混沌保密通信方案设计提供了基础与条件.

关键词: 时空混沌; 二维耦合映像格子; Lyapunov 指数; 混沌密码; 保密通信
中图分类号: TN918.1; O415.5 **文献标识码:** A **文章编号:** 0372-2112 (2019)03-0657-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.03.020

Cryptographic Feature Analysis on 2D Coupled Map Lattices Based on Piecewise Logistic Map

WANG Yong[1,2], ZHAO Yi[1], Jerry GAO[3], CHEN Yan[1]
(1. *College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*;
2. *Key Laboratory of Electronic Commerce and Logistics, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*;
3. *Computer Engineering Department, San Jose State University, San Jose, California* 95192, *USA*)

Abstract: Using the piecewise logistic map (PLM) as a local chaotic map for the 2D coupled map lattices (CML), this paper proposes a chaotic model with complex dynamic behavior. The influence of some parameters to the model features, such as the Lyapunov exponent (LE), bifurcation, ergodicity, and probability density distribution, is analyzed from the view of cryptographic applications. The analysis results provide the theoretic evidence for the model to configure parameters in the secure communication. Moreover, an offset is introduced to adjust the status value of lattices, which improve the ununiformity of probability density of status value. The research results show that the proposed model has good performance, and provide good foundation and conditions for the research of designing secure communication scheme based on this model.

Key words: spatiotemporal chaos; coupled map lattices; Lyapunov exponent; chaos-based cryptography; secure communication

1 引言

混沌是非线性动力系统中出现的一种确定的、貌似无规则的类随机过程. 已有研究显示混沌系统的演变过程和密码学变换非常类似[1]. 混沌系统在密码学和保密通信中的应用得到越来越多的关注[2]. 混沌模型所具有的与密码学相关的特性是构造保密通信方案的关键. 常用的 Logistic 映射存在序列概率密度分布不均匀,参数取值范围有限等问题. 为此,一些研究者对 Logistic 映射做了分段化处理[3~5]. 在混沌保密通信中,为了避免简单混沌产生的序列被攻击者预测出来[6~8],倾向于选用超混沌或者复杂混沌系统作为核心部件. 耦合映像格子模型是一种常用的复杂混沌系统,在混沌密码算法的设计中得到了一定的应用[9~11]. 然而,当前的研究大多是直接将耦合映像格子用于混沌保密通信系统,很少分析模型本身所固有的加密相关特性,模

收稿日期:2018-01-02;修回日期:2018-05-08;责任编辑:覃怀银
基金项目:国家自然科学基金 (No. 61472464);重庆市基础与前沿项目(No. cstc2015jcyjA0554);国家社会科学基金 (No. 14CTQ026)

型参数的设置缺乏理论指导. 为此,从减少计算量的角度,本文构造了一种二维耦合映像格子模型,然后引入分段 Logsitic 映射(PLM)作为局部混沌映射,分析了该模型所固有的密码学相关的特性. 分析结果可指导耦合映像格子模型的控制参数设置,从而发挥该模型的优势,设计出更安全高效的保密通信系统.

2 混沌系统的密码学相关特性

本文结合密码学应用的需要,选取如下物理特征作为性能评价指标.

(1)Lyapunov 指数(LE):在非线性动力系统中,LE 用于定量描述相空间中相近轨道的平均发散性. 最大 Lyapunov 指数(LLE,Largest Lyapunov Exponent)大于 0 表示在该方向上轨道迅速分离,存在混沌现象. 从密码学应用的角度看,LE 与混沌系统的伪随机性,初值敏感性密切相关,可以量化混沌系统迭代的扩散效果,帮助排除弱密钥.

(2)分岔:可以直观展现非线性方程在临界点附近的突变过程. 在混沌密码算法设计中,通过分岔图能有效观察参数设置对系统行为的影响,指导保密系统中的混沌映射选择和参数设置.

(3)遍历区间:遍历性是指在有限时间内混沌轨道会经历混沌区域内每一个状态点. 遍历区间描述了混沌区域的大小. 在密码学的应用中,遍历区间过小容易被暴力攻击. 所以,在混沌密码算法设计中,应选择具有较宽遍历区间的混沌系统.

(4)概率密度分布:将混沌映射视作以初值和控制参数为种子的随机函数,概率密度分布可描述状态值在相空间的分布情况. 从安全性的角度看,应选用概率密度分布均匀的混沌映射.

3 二维耦合映像格子模型

耦合映像格子是时空混沌模型中的一种常用形式. 二维临近耦合映像格子模型的常用表达式如下[12]:

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

其中,$n=1,2,\cdots$,为时间索引;$i=1,2,\cdots,R$ 为格子的行坐标;$j=1,2,\cdots,L$ 为格子的列坐标;$x_n^{i,j}$ 为第 i 行第 j 列的格子在 n 时刻的状态值;$f(x)$ 为局部混沌映射;$\varepsilon\in(0,1)$ 为耦合系数或耦合强度. 模型的周期边界条件为 $x_n^{R+i,j}=x_n^{i,j}$,$x_n^{i,j+L}=x_n^{i,j}$. 在该模型中,计算任一格子的下一状态值需要运算局部混沌映射 5 次. 为了减少计算量,本文构建如下的临近耦合简化模型:

$$x_{n+1}^{i,j}=(1-\varepsilon)f(x_n^{i,j})+\frac{\varepsilon}{2}[f(x_n^{i+1,j})+f(x_n^{i,j+1})] \tag{2}$$

定理 1 式(2)所表示的二维耦合映像格子模型的 LLE 由局部映射的 LLE 决定.

证明 借鉴文献[12]中的方法,假设式(2)中模型各格子同步,即有为 $x_n^{i,j}=x_n^{i+1,j}=x_n^{i,j+1}=x_n$. 将二维模型看成先行后列排列的一维耦合格子模型,则二维模型可以表示为向量 $\boldsymbol{z}$:

$$\boldsymbol{z}=[x(1),x(2),\cdots,x(R\times L)] \tag{3}$$

它的切向量为 $\delta\boldsymbol{z}=[\delta x(1),\delta x(2),\cdots,\delta x(R\times L)]$,其中:

$$\delta x_{n+1}(i)=(1-\varepsilon)f'(x_n(i))\delta x_n(i)+\varepsilon/2(f'(x_n(k))\delta x_n(k)+f'(x_n(m))\delta x_n(m)) \tag{4}$$

k,m 为二维格子模型中相邻两个格子在一维模型中对应的位置. 由此可以得到 $\delta\boldsymbol{z}_{n+1}=\boldsymbol{J}_n\delta\boldsymbol{z}_n$,其中 $\boldsymbol{J}_n$ 为模型的雅克比矩阵.

设 $\boldsymbol{g}=\begin{pmatrix}\boldsymbol{A}_1 & \boldsymbol{A}_2 & \boldsymbol{A}_3 & \cdots & \boldsymbol{A}_R\\ \boldsymbol{A}_R & \boldsymbol{A}_1 & \boldsymbol{A}_2 & \cdots & \boldsymbol{A}_{R-1}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ \boldsymbol{A}_2 & \boldsymbol{A}_3 & \boldsymbol{A}_4 & \cdots & \boldsymbol{A}_1\end{pmatrix}$,

其中 $\boldsymbol{A}_1=\begin{pmatrix}1-\varepsilon & \varepsilon/2 & 0 & \cdots & 0\\ 0 & 1-\varepsilon & \varepsilon/2 & \cdots & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ \varepsilon/2 & 0 & 0 & \cdots & 1-\varepsilon\end{pmatrix}_{L\times L}$,

$\boldsymbol{A}_2=\begin{pmatrix}\varepsilon/2 & 0 & 0 & \cdots & 0\\ 0 & \varepsilon/2 & 0 & \cdots & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & 0 & \cdots & \varepsilon/2\end{pmatrix}_{L\times L}$,

$\boldsymbol{A}_3=\boldsymbol{A}_4=\cdots=\boldsymbol{A}_R=\boldsymbol{0}$,

则 $\boldsymbol{J}_n$ 可表示为 $\boldsymbol{J}_n=f'(x_n)\boldsymbol{g}$.

令 $\boldsymbol{K}=\boldsymbol{J}_1\times\boldsymbol{J}_2\times\cdots\times\boldsymbol{J}_n=\boldsymbol{g}^n\prod_{i=1}^{n}f'(x_i)$,再设 $\boldsymbol{g}$ 的特征值为 λ,则 $\boldsymbol{K}$ 的特征值为 $\lambda^n\prod_{i=1}^{n}f(x_i)$,对其取模,得到系统的 Lyapunov 指数为

$$\begin{aligned}\mathrm{LE}&=\lim_{n\to\infty}\frac{1}{n}\ln\left|\,|\lambda|^n\prod_{i=1}^{n}f(x_i)\right|\\&=\lim_{n\to\infty}\frac{1}{n}\ln\left|\prod_{i=1}^{n}f(x_i)\right|+\ln||\lambda||\end{aligned} \tag{5}$$

由于 $\boldsymbol{g}$ 为分块循环矩阵,因此其特征多项式为 $\prod_{k=1}^{R}|\boldsymbol{A}_1+\boldsymbol{A}_2\omega_k-\lambda E|$ 其中 ω_k 为 k 个互异的 k 次单位根,$\boldsymbol{E}$ 为单位矩阵. 又因为 $\boldsymbol{A}_1+\boldsymbol{A}_2\omega_k-\lambda\boldsymbol{E}$ 为 $L\times L$ 阶循环矩阵,因此可解得 $\boldsymbol{g}$ 的特征根为:$1-\varepsilon+\frac{\varepsilon}{2}\omega_k+\frac{\varepsilon}{2}\mu_l$,其中 μ_l 为 l 个互异的 l 次单位根,$k=1,2,\cdots,R$;$l=1,2,\cdots,L$. 取模后带入式(5)得到系统的 Lyapunov 指数谱的解析式为:

$$\mathrm{LE}=\lambda_{f(x)}+\frac{1}{2}\ln\left|1+\frac{3}{2}\varepsilon^2-2\varepsilon+\varepsilon(1-\varepsilon)\cdot\left(\cos\frac{2k\pi}{R}+\cos\frac{2l\pi}{L}\right)+\frac{\varepsilon^2}{2}\cos\left(\frac{2k\pi}{R}-\frac{2l\pi}{L}\right)\right| \tag{6}$$

其中 $\lambda_{f(x)}$ 为局部映射 $f(x)$ 的 LE. 在 $k=R, l=L$ 时,式(6)取得最大值 $\lambda_{f(x)}$. 所以,二维耦合映像格子模型的 LLE 由局部混沌映射的 LLE 决定.

由于 PLM 具有比 Logistic 映射更大的 LE,且兼顾了计算效率与混沌序列的复杂性[5],所以选用该映射作为二维耦合映像格子模型的局部映射,其表达式为:

$$x_{m+1}=\mathrm{PLM}(x_m)=\begin{cases}N^2\mu x_m\left(\frac{1}{N}-x_m\right), & 0<x_m<\frac{1}{N}\\ 1-N^2\mu\left(x_m-\frac{1}{N}\right)\left(\frac{2}{N}-x_m\right), & \frac{1}{N}<x_m<\frac{2}{N}\\ N^2\mu\left(x_m-\frac{i-1}{N}\right)\left(\frac{i}{N}-x_m\right), & \frac{i-1}{N}<x_m<\frac{i}{N}\\ 1-N^2\mu\left(x_m-\frac{i}{N}\right)\left(\frac{i+1}{N}-x_m\right), & \frac{i}{N}<x_m<\frac{i+1}{N}\\ \vdots & \\ N^2\mu\left(x_m-\frac{N-2}{N}\right)\left(\frac{N-1}{N}-x_m\right), & \frac{N-2}{N}<x_m<\frac{N-1}{N}\\ 1-N^2\mu\left(x_m-\frac{N-1}{N}\right)(1-x_m), & \frac{N-1}{N}<x_m<1\\ x_m+\frac{1}{100N}, & x_m=0,\frac{1}{N},\frac{2}{N}\cdots,\frac{N-1}{N}\\ x_m-\frac{1}{100N}, & x_m=1\end{cases} \tag{7}$$

其中,N 为分段数;μ 为控制参数;x_m 为 PLM 在时刻 m 的状态值.

此外,依据定理 1,容易得到如下两个推论:

推论 1　模型的 LLE 与模型的尺寸无关.

推论 2　模型的 LLE 与耦合强度 ε 无关.

4　二维耦合映像格子模型的特性分析

从增强局部映射的混沌特性出发,利用格子模型的时空耦合与混合,本文构造了高维的具有复杂时空行为的二维耦合映像格子模型. 该模型中的参数包括二维格子维数 R 和 L,耦合强度 ε 以及局部混沌映射 PLM 中的参数 μ 和 N. 本节中,模型特性分析的目的是确定如何设置参数能够让模型具有更好的密码学性能. 为了避免参数之间的相互影响,采用“变化某个参数,同时保持其他参数不变”的策略,对模型进行分析.

4.1　Lyapunov 指数谱

推论 1 的结果表明了 LLE 与 L 和 R 的取值无关,所以可根据密码算法设计需要(比如便于硬件布置)自由设置 R 和 L 的大小. 从易于硬件实现的角度,此处将其设置为 $L=R=8$.

推论2 的结果虽然表明了 ε 对 LLE 没有影响. 但是 ε 对其他维度上的 LE 有影响. 当 $L=R=8$ 时,在式(6)中对 ε 求导,可得:

$$\mathrm{LE}'=\frac{\left(3-2\left(\cos\left(\frac{k\pi}{4}\right)+\cos\left(\frac{l\pi}{4}\right)\right)+2\cos\left(\frac{k\pi}{4}-\frac{j\pi}{4}\right)\right)\varepsilon+\cos\left(\frac{k\pi}{4}\right)+\cos\left(\frac{l\pi}{4}\right)-2}{2\left(1+\frac{3}{2}\varepsilon^2-2\varepsilon+\varepsilon(1-\varepsilon)\left(\cos\left(\frac{k\pi}{4}\right)+\cos\left(\frac{l\pi}{4}\right)+\frac{\varepsilon^2}{2}\cos\left(\frac{k\pi}{4}-\frac{l\pi}{4}\right)\right)\right)} \tag{8}$$

其中 $k=1,2,\cdots,8; l=1,2,\cdots,8$.

在式(8)中,令分母为 0. 在满足 $\varepsilon\in(0,1)$ 的条件下,仅在 $k=4, l=4$ 时有解,即 $\varepsilon=0.5$. 分母为 0 意味着对应的 Lyapunov 指数为 $-\infty$,为了让模型有好的混沌特性,ε 应避免取 0.5.

令导数为 0,则解得:

$$\varepsilon=\frac{2-\cos\frac{k\pi}{4}-\cos\frac{l\pi}{4}}{3-2\cos\frac{k\pi}{4}-2\cos\frac{l\pi}{4}+\cos\left(\frac{k\pi}{4}-\frac{l\pi}{4}\right)} \tag{9}$$

由于:

$$\varepsilon=\frac{2-\cos\frac{k\pi}{4}-\cos\frac{l\pi}{4}}{3-2\cos\frac{k\pi}{4}-2\cos\frac{l\pi}{4}+\cos\left(\frac{k\pi}{4}-\frac{l\pi}{4}\right)}$$

$$\geq\frac{2-\cos\frac{k\pi}{4}-\cos\frac{l\pi}{4}}{4-2\cos\frac{k\pi}{4}-2\cos\frac{l\pi}{4}}=0.5$$

又因为式(6)可视作 ε 的二次函数,因此无论 k,l 取何值,LE 取得最小值点时,对应的 ε 均大于 0.5. 又由 $\varepsilon\in(0,1)$ 和二次函数的性质可得:欲使 LE 值最大 ε 的取值应该趋近于 0. 同时,为了保持模型内格子之间必要的耦合强度,ε 取值不宜过小,所以建议 ε 取值为 0.1.

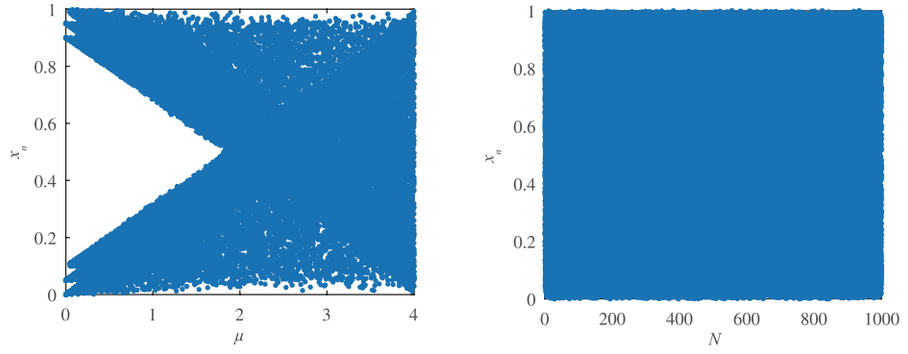
定理 1 表明 LLE 的取值仅与 PLM 的 Lyapunov 指数有关. 因此根据文献[5]中的研究结果,PLM 的 Lyapunov 指数随着 μ 和 N 的增大而增大,但是 N 越大 PLM 在各分段内的非线性特性会越小,所以,在综合 PLM 非线性变换和 LLE 增长效率的条件下,设置 $\mu=4$ 和 $N=64$.

4.2 分岔图

依据4.1中的分析结果,固定 $R=L=8$,$\varepsilon=0.1$,分析局部映射参数 μ 和 N 对模型分岔的影响. 由于模型中格子数目众多,受篇幅限制,仅以第一个格子(即 $i=1$,$j=1$)为代表展示模型的分岔图结果. 同时,测试的结果还发现各格子在分岔图上的特性类似,故可用模型中的任一格子作为代表.

对局部映射 PLM,设置 $N=64$,分析当 μ 变化时格子的分岔情况,格子(1,1)的分岔如图1(a)所示. 同样的设置 $\mu=4$. 变化 N 的值,绘制模型中各个格子的分岔图. 格子(1,1)随 N 变化的分岔情况如图1(b)所示.

从图1(a)中可以看出,参数 μ 的取值对格子的分岔图影响显著,且 μ 为4时模型格子的分岔最充分,有最好的混沌特性. 因而模型在整体上也获得了最好的分岔特性. 同时由图1(b)可以看出,N 的变化对分岔的结果几乎没有影响.



(a) 格子(1,1)的分岔图随μ变化的情况　　(b) 格子(1,1)的分岔图随N变化情况

图1　格子(1,1)分岔图的随参数的变化情况

4.3 遍历区间

与分岔图类似,遍历区间也是针对单个格子而言的. 此处,仍然以第一个格子($i=1$,$j=1$)为代表,分析其遍历区间. 同时,实验也测试了模型中其他格子的遍历区间,测试结果显示各格子在遍历区间上的特性是类似的. 因此,可用模型中的任一格子作为代表来展示模型的遍历区间. 依次设置 $\mu=0.5$,1.5,2.5 和4,同时变化 $N=8$,32,64,得到的格子(1,1)的遍历区间如图2所示. 由图2知,μ 对格子的遍历区间有显著的影响. 随着 μ 值增大,格子遍历区间随之增大,当 $\mu=4$ 时,格子有最大的遍历区间(0,1). 同时,当系统未进入混沌状态时,N 的变化对系统的遍历区间有一定的影响. 但是,当系统处于混沌状态后,N 的增加并不会改变系统的遍历区间.

4.4 概率密度

根据分岔图和遍历区间的分析结果知,$\mu=4$ 时,模型进入完全的分岔状态,遍历区间最大且与值域区间重合. 所以,在概率密度分布的分析中,固定 $\mu=4$,测试概率密度随 N 的变化情况.

设置 $N=2$,8,32,64,得到模型的概率密度分布如图4所示. 由图3可得无论 N 如何取值,模型的概率密度分布是不均匀的,均为两边高,中间低. 同时概率密度取值的峰值出现在(0,0.2)和(0.8,1)两个区间内,出现此情况的原因是为了保证模型的混沌性能,在设置 ε 的取值时采取了较小的取值,所以模型的概率密度分布类似于 PLM 的概率密度分布情况,而与 N 的取值关系不大.

5 模型概率密度分布的均匀化

由于模型状态值的概率密度分布不均匀,从密码学应用的角度看,不利于保证模型状态值的伪随机性. 为此,有必要对模型状态值做均匀化处理.

根据4节中的分析结果,设置模型参数为:$R=8$,$L=8$,$\varepsilon=0.1$,$\mu=4$,$N=64$. 绘制模型中各格子的概率密度分布,如图4所示. 由于各格子的概率密度峰值重合,导致了模型整体的概率密度分布不均. 为此,在模型中每个格子完成一次迭代后,对其状态值添加一个不同幅度的偏移量,以便将各格子的概率密度峰值错开,使其均匀分布到(0,1)区间.

每次迭代后,模型中各格子状态值的变化式如下:

$$y_n^{i,j}=(x_n^{i,j}+((i-1)\times L+j)/(R\times L))\bmod 1 \quad (8)$$

式中,$x_n^{i,j}$ 和 $y_n^{i,j}$ 分别为格子(i,j)的状态值和增加偏离量后的值.

由式(8)知,状态值的偏移量与模型中的格子数相关,所以状态值的概率密度分布均匀性也与模型中格子的个数是相关的. 图5中绘制了格子数为10和12时的模型概率密度分布. 从图中可以看出,当格子数为12时,模型的概率密度分布基本均匀.

对上述 8×8 的二维耦合映像格子模型,格子总数为64,具有更好的概率密度分布均匀性,它的状态值概率分布如图6所示. 图中状态值概率分布的方差为 4.342×10^{-12},进一步验证了模型的概率密度分布有很好的均匀性.

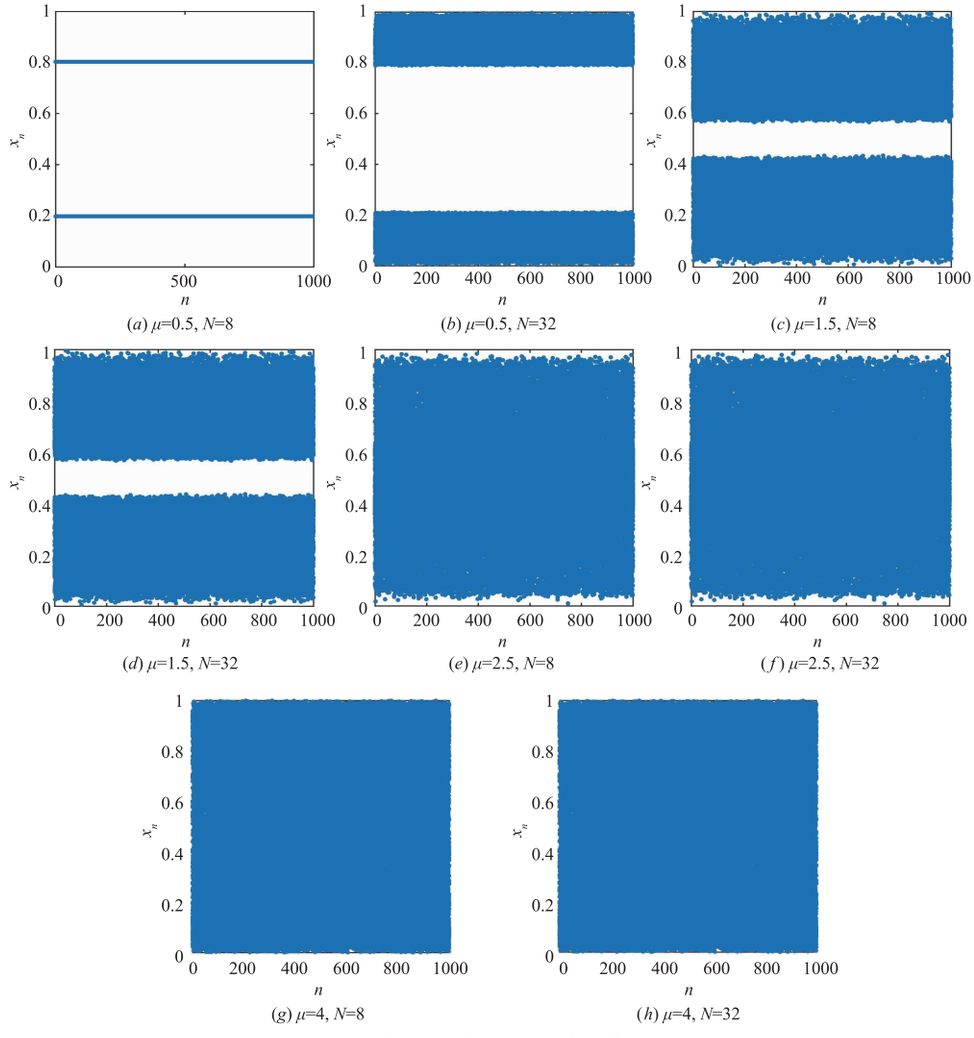


图2　格子(1,1)的遍历区间变化情况

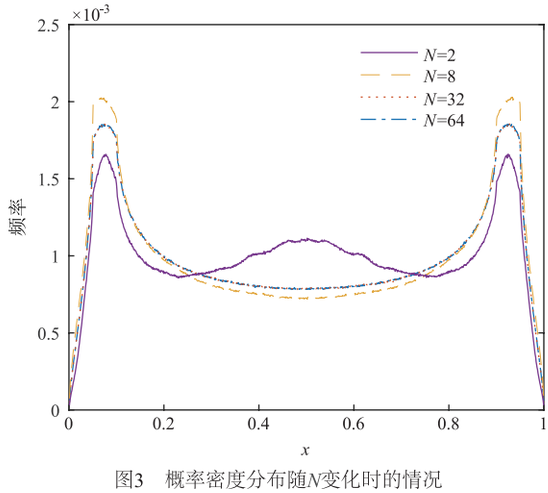


图3　概率密度分布随N变化时的情况

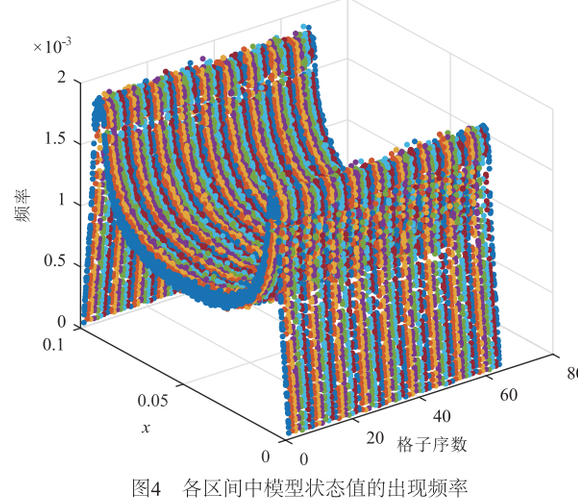


图4　各区间中模型状态值的出现频率

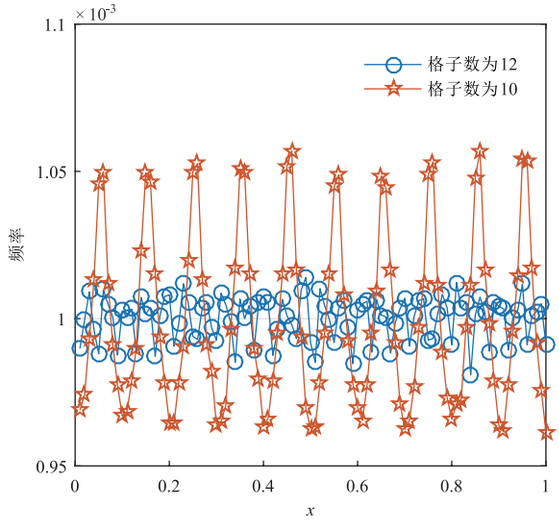


图5 格子数为10和12时的概率密度分布

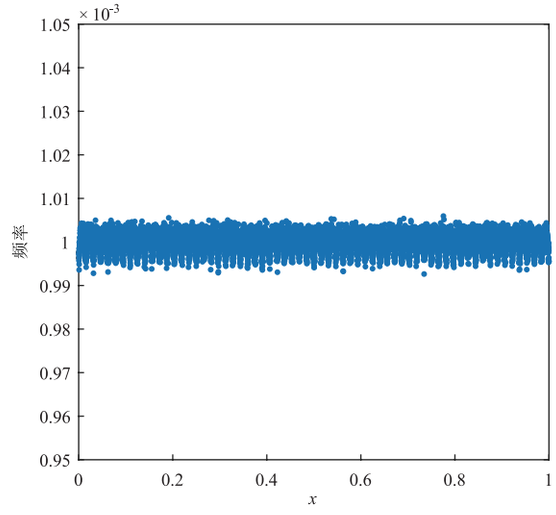


图6 8×8二维映像格子模型的状态值概率密度分布

6 对比分析

近年来,一些基于耦合映像格子模型的加密算法被提出[9,11,13,14]. 计算这些文献中混沌模型的最大 Lyapunov 指数、参数 μ 的取值范围,并与本文模型进行对比,结果如表 1 和表 2 所示. 从表 1 和 2 中可得,本文模型具有更大的 LLE 值,且参数 μ 的取值范围更大,说明本文模型更适合应用于加密算法的设计.

表 1 LLE 的对比结果

	本文模型	本文模型(偏移处理)	文献[9]	文献[11]	文献[13]	文献[14]
LLE	4. 7414	4. 7228	0. 5911	0. 4088	0. 4589	0. 6029

表 2 μ 的取值范围对比结果

	本文模型	本文模型(偏移处理)	文献[9]	文献[11]	文献[13]	文献[14]
参数范围	[0. 1,4]	[0. 1,4]	(0,1)	[3. 57,4]	[3. 57,4]	[3. 57,4]

计算文献[9,11,13,14]中模型的状态值概率密度分布,结果显示这些模型的状态值的概率密度分布都是不均匀的. 本文模型在通过偏移化处理之后,状态值的概率密度分布是均匀的. 因此,从密码学的统计角度看,本文模型具有更好的性能.

选取观测区间数目 M 为 1000,序列的长度为 100,000,测量本文模型和文献[9,11,13,14]中模型产生的序列的信息熵[15],所得到的结果如表 3 所示.

表 3 信息熵对比结果

	本文模型	本文模型(偏移处理)	文献[9]	文献[11]	文献[13]	文献[14]
信息熵	9. 8816	9. 9657	9. 7832	9. 6973	9. 7191	9. 7277

理想状态下随机序列的最大信息熵为 $\log_2 M$ 即 9. 9658. 由表 3 可得到本文模型的信息熵大于文献[9,11,13,14]中的信息熵,且模型经过偏移化处理之后,其信息熵非常接近理论最大值,说明模型具有非常好的随机性,能更好的满足保密通信的需要.

7 结论

从减少计算量的角度提出了一种二维耦合映像格子模型,给出了该模型 Lyapunov 指数谱的解析式. 从理论上得到了模型的 LLE 与模型尺寸和耦合强度无关,仅由局部映射决定的结论. 然后,以 PLM 作为局部函数,分析了该模型的密码学相关特性. 分析结果能够有效指导该模型在保密通信应用中的参数设置. 针对模型状态值的概率密度分布不均匀问题,引入不同的偏移量,实现了模型状态值的均匀化,提升了混沌序列的信息熵. 数值实验分析和对比结果表明,本文构造的二维耦合映像格子模型具有很好的密码学特性,在混沌保密通信中有很好的应用潜力.

参考文献

[1] 廖晓峰,肖迪,陈勇,等. 混沌密码学原理及其应用[M]. 北京:科学出版社,2009. 37 – 39.

[2] 禹思敏,吕金虎,李澄清. 混沌密码及其在多媒体保密通信中应用的进展[J]. 电子与信息学报,2016,38(3):735 – 752.
YU Si-min,LÜ Jin-hu,LI Cheng-qing. Some progresses of chaotic cipher and its applications in multimedia secure communications[J]. Journal of Electronics & Information Technology,2016,38(3):735 – 752. (in Chinese)

[3] 张雪锋,范九伦. 一种新的分段非线性混沌映射及其性能分析[J]. 物理学报,2010,59(4):2298 – 2304.
ZHANG Xue-feng,FAN Jiu-lun. A new piecewise nonliner chaotic map and its performance[J]. Acta Physica Sinica,2010,59(4):2298 – 2304. (in Chinese)

[4] 范九伦,张雪锋. 分段 Logistic 混沌映射及其性能分析[J]. 电子学报,2009,37(4):720 – 725.
FAN Jiu-lun,ZHANG Xue-feng. Piecewise logistic chaotic map and its performance analysis[J]. Acta Electronica Sinica,2009,37(4):720 – 725. (in Chinese)

[5] WANG Y,LIU Z,MA J,et al. A pseudorandom number generator based on piecewise logistic map[J]. Nonlinear Dynamics,2016,83(4):2373 – 2391.

[6] MAGUIRE L P,ROCHE B,MCGINNITY T M,et al. Predicting a chaotic time series using a fuzzy neural network[J]. Information Sciences,1998,112(1 – 4):125 – 136.

[7] LI D,MIN H,WANG J. Chaotic time series prediction based on a novel robust echo state network[J]. IEEE Transactions on Neural Networks & Learning Systems,2012,23(5):787 – 799.

[8] HAMILTON F,BERRY T,SAUER T. Predicting chaotic time series with a partial model[J]. Physical Review E,2015,92(1):10902 – 12015.

[9] WANG Y,WONG K W,LIAO X,et al. A new chaos-based fast image encryption algorithm[J]. Applied Soft Computing,2011,11(1):514 – 522.

[10] ZHANG H,WANG X Y,WANG S W,et al. Application of coupled map lattice with parameter q in image encryption[J]. Optics & Lasers in Engineering,2017,88:65 – 74.

[11] ZHANG Y Q,WANG X Y. A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice[J]. Information Sciences,2014,273(8):329 – 351.

[12] DING M,YANG W. Stability of synchronous chaos and on-off intermittency in coupled map lattices[J]. Physical Review E,1997,56(4):4009 – 4016.

[13] WANG Y,LIAO X,XIAO D,et al. One-way hash function construction based on 2D coupled map lattices[J]. Information Sciences,2008,178(5):1391 – 1406.

[14] WANG X Y,ZHANG Y Q,BAO X M. A novel chaotic image encryption scheme using DNA sequence operations[J]. Optics & Lasers in Engineering,2015,73:53 – 61.

[15] 刘先省,申石磊,潘泉,等. 基于信息熵的一种传感器管理算法[J]. 电子学报,2000,28(9):39 – 41.
LIU Xian-sheng,SHEN Shi-lei,PAN Quan,et al. An algorithm of sensor management based on information[J]. Acta Electronica Sinica,2000,28(9):39 – 41. (in Chinese)

作者简介

王　永(通信作者)　男,1977 年生于四川自贡. 现为重庆邮电大学教授、博士. 主要研究方向为信息安全,混沌密码,信息管理.
E-mail:wangyong1@cqupt.com

赵　毅　男,1993 年生于山东泰安. 现为重庆邮电大学计算机科学与技术硕士研究生. 主要研究方向为混沌密码.
E-mail:zy199303@qq.com

Jerry Gao　男,现为美国圣何塞州立大学教授. 主要研究方向为云安全、大数据分析、智慧城市.
E-mail:jerry.gao@sjsu.edu

陈　燕　女,1991 年生于河南许昌. 现为重庆邮电大学计算机科学与技术硕士研究生. 主要研究方向为混沌密码.
E-mail:2671182178@qq.com