单峰混沌系统的相空间均匀化及动力学特性

徐　辉[1,2], 佟晓筠[1†], 张　淼[1], 刘　杨[1], 王　焘[1]

(1. 哈尔滨工业大学 计算机科学与技术学院, 山东 威海 264209; 2. 哈尔滨理工大学 荣成学院, 山东 荣成 264300)

摘要: 由经典一维混沌映射构造密码系统存在短周期轨道、密钥空间小和相空间分布不均匀等安全性缺陷. 为解决经典一维混沌密码的安全性问题, 提出了一种新型的一维单峰混沌系统及其改进的复合形式. 采用普适性均匀化算法来获得等概率分布的混沌序列并给出了概率密度数学证明. 对改进的单峰混沌系统的遍历性、李雅普诺夫指数、相空间和分岔、信息熵和近似熵等动力学和随机特性指标进行了计算和分析. 通过与相关研究的对比可知, 改进的单峰混沌系统具有稳定的李雅普诺夫指数、扩展的相空间、均匀的概率密度和更高的近似熵值. 理论推导和数值计算论证了本方案可以满足密码系统中非线性部件的安全属性要求.

关键词: 混沌系统; 单峰映射; 概率密度; 信息熵

引用格式: 徐辉, 佟晓筠, 张淼, 等. 单峰混沌系统的相空间均匀化及动力学特性. 控制理论与应用, 2019, 36(5): 759 – 765

DOI: 10.7641/CTA.2018.80157

Phase space homogenization and dynamic characteristics of unimodal chaotic system

XU Hui[1,2], TONG Xiao-jun[1†], ZHANG Miao[1], LIU Yang[1], WANG Zhu[1]

(1. School of Computer Science and Technology, Harbin Institute of Technology, Weihai Shandong 264209, China;
2. School of Rongcheng, Harbin University of Science and Technology, Rongcheng Shandong 264300, China)

Abstract: The cryptosystem constructed by classical one-dimensional chaotic mapping has some shortcomings in terms of security such as short-period orbits, small key space and inhomogeneous distribution of phase space. In order to solve the security problem of classical one-dimensional chaotic ciphers, a novel one-dimensional unimodal chaotic system and its improved composite form were proposed. A universal homogenization algorithm was used to transform the chaotic sequence into an equal probability distribution and a probability density mathematical proof was given. The dynamics and random characteristic indicators such as ergodicity, Lyapunov exponents, phase space, bifurcations, information entropy and approximate entropy were calculated and analyzed for the improved unimodal chaotic system. Through comparison with related researches, it can be seen that the improved unimodal chaotic system has stable Lyapunov exponents, extended phase space, uniform probability density and higher approximate entropy. Theoretical derivation and numerical calculation demonstrate that this scheme can meet the security attributes of nonlinear components in cryptosystem.

Key words: chaotic systems; unimodal mapping; probability density; information entropy

Citation: XU Hui, TONG Xiaojun, ZHANG Miao, et al. Phase space homogenization and dynamic characteristics of unimodal chaotic system. *Control Theory & Applications*, 2019, 36(5): 759 – 765

1　引言

混沌映射是一个具有非线性动力学特性的特殊确定性系统. 混沌系统的初始值或参数经过微小改变就会产生完全不同的两条混沌轨道, 在长期的迭代过程中, 混沌系统表现出类随机的特性, 因此从时间维度来看, 预测整个混沌轨道是非常困难甚至不可能的. 混沌系统的许多特性, 如遍历性、初值敏感性和随机行为与Shannon提出的“混淆性”和“扩散性”相一致, 为将混沌系统运用于密码学提供了理论基础[1]. 由于混沌信号固有的连续宽带和类噪声等特性, 使得

收稿日期: 2018−03−07; 录用日期: 2018−06−19.

†通信作者. E-mail: tong_xiaojun@163.com; Tel.: +86 13061181039.

本文责任编委: 张化光.

国家信息保障重点实验室基金项目(KJ–17–004), 2017威海大学共建项目, 国家自然科学基金项目(61702139), 黑龙江省普通高等学校青年创新人才培养计划项目(UNPYSCT–2016036)资助.

Supported by the Foundation of Science and Technology on Information Assurance Laboratory (KJ–17–004), 2017 Weihai University Co-construction Project, National Natural Science Foundation of China (61702139) and the University Nursing Program for Young Scholars with Creative Talents in Heilongjiang Province (UNPYSCT–2016036).

许多学者在混沌控制、混沌密码及保密通信等领域做了大量研究工作[2–5].

应用于密码体系的混沌系统一般可以分为连续混沌系统和离散混沌系统. 连续混沌系统一般由微分方程的形式来表示, 如Lorenz 系统[6]、Rossler 系统和Chen系统等. 由于连续混沌系统的动力学行为更复杂, 参数空间更大, 因此被许多加密系统所采用[7]. 但连续混沌系统由于需要解微分方程, 因此时间复杂度较高, 不适合大规模实时数据加密.

离散混沌系统, 如Logistic 系统、帐篷映射和Henon映射等都是由差分方程的迭代形式表示的. 这类混沌系统具有计算复杂度低, 软硬件实现便捷等特点, 因此, 越来越多的研究人员开始关注基于离散混沌系统的加密算法[8–9]. 但从密码学的角度来看, 离散混沌系统仍存在许多不可忽视的问题. 以Logistic系统为例, 它是一个典型的离散混沌系统, 然而, 如果将一维Logistic混沌映射直接用作密码系统的核心组件, 其在安全性方面存在密钥空间较小、周期窗口和轨道分布不均匀等缺陷.

为了改进一维离散混沌系统的性能, 许多研究者做了大量工作. Zhou等[10]将两个现有的一维混沌映射相加并取模运算, 尽管在一定程度上提高了随机性, 但取模后的轨道分布仍然是不均匀的. Jeaneth等[11]对Logistic映射进行了改进, 将每一次迭代的状态值去掉前面的k位小数, 只保留接下来的L位, 重新构成新的混沌序列, 随着k的增加, 新的混沌系统表现出了更好的随机特性. 然而, 新的混沌系统的最大李雅普诺夫指数没有显著提高, 混沌轨道在一定程度上仍然呈不均匀分布. 为了让整个混沌轨道在相空间内呈均匀分布, 许多研究将混沌状态值乘以一个较大的整数然后再进行取模操作[12–13], 这一策略尽管使混沌序列近似等概率分布, 但相空间和李雅普诺夫指数没有明显增加. 为了防止动力学特性退化, 也有许多研究人员利用一个混沌系统来扰动或者控制另一个系统的参数和输入状态值, 该方案可以得到更宽的混沌区间, 但序列概率分布仍然是不均匀的[14–15].

混沌系统的本质属性决定了其直接作为密码系统使用会带来安全隐患, 尽管许多研究人员做了大量研究工作来提高混沌系统的安全性, 但是能同时解决相空间扩展、提高李雅普诺夫指数和轨道均匀化3个安全性问题的研究还鲜有报道, 特别是在混沌序列的密度分布问题上, 大多数研究得出的结果都是近似分布, 没有给出严格的数学证明. 同时, 现有混沌系统的混沌参数区间都很窄, 使得李雅普诺夫指数会随着参数的变化剧烈波动, 甚至出现负数, 这不符合密码学的鲁棒性要求. 另外, 现有低维混沌系统的相空间基本上都在区间(0, 1)范围内, 在有限精度的情况下, 容易出现短周期现象. 因此, 为了提高混沌密码系统的安全性, 本文提出了一个新的单峰混沌系统及其改进的复合形式, 同时, 本文也给出了普适性的混沌轨道空间均匀化算法. 经过理论分析和实验测试, 本文提出的混沌系统具有较高的随机性, 可以满足密码算法对非线性部件安全性的要求.

2 单峰混沌系统的动力学特性分析

Logistic系统是一个典型的一维混沌映射, 它是一个具有复杂动力学行为的离散时间动力系统. Logistic系统的数学表达式为

$$x_{n+1} = f(x_n) = \mu \cdot x_n(1 - x_n), \tag{1}$$

$x_n \in (0, 1)$是混沌状态值, μ是控制参数. 当$\mu \in (3.57, 4)$时, 系统处于混沌状态. 这个系统的混沌参数区间和相空间都很小, 混沌轨道分布也不均匀, 因此从密码学角度, 该混沌系统的安全性受到质疑. 为此, 本文提出了一种新的扩展的单峰混沌系统(a novel extended unimodal chaotic system, NUS), 它具有更好的动力学特性. 其数学表达式为

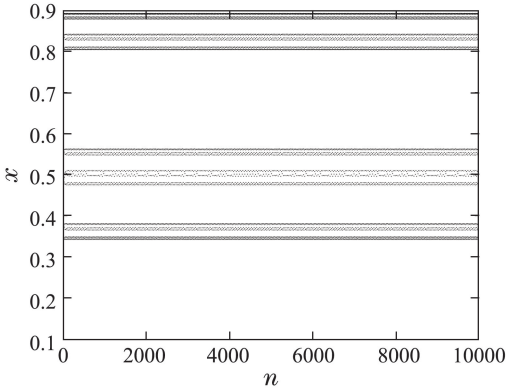
$$x_{n+1} = f(x_n) = -a{x_n}^2 + 4x_n, \tag{2}$$

$x_n \in (0, 4/a)$是混沌状态值, a是控制参数. 这里只要$a > 0$, NUS就处于混沌状态.

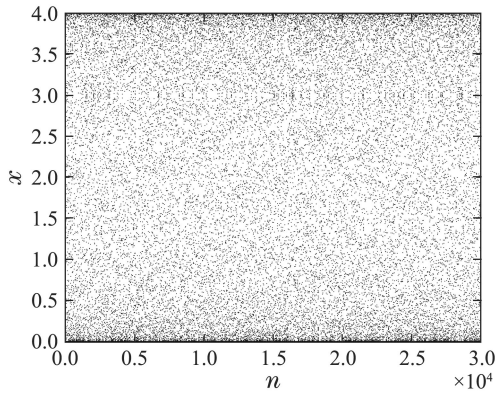
2.1 单峰混沌系统的遍历性

在统计学中, 遍历性描述了一个混沌系统的随机过程, 它体现了序列在长期迭代过程中的分布情况. 通过对混沌遍历范围的分析, 还可以得到混沌系统的相空间大小. 密钥空间的范围在一定程度上取决于相空间的大小. 因此从密码设计角度分析, 遍历性与混沌系统的安全性密切相关.

在图1(a)中, 针对Logistic系统在参数$\mu = 3.57$的情况下, 给出了混沌状态值的空间分布. Logistic系统的相位空间和分布将随着参数的增加而改变. 当参数μ小于4时, 混沌轨道不能覆盖整个相空间(0, 1), 且存在多个密集区域. 在图1(b)中, 针对NUS系统在参数$a = 1$的情况下, 给出了系统的状态空间分布. 从图中可以很明显地发现, 混沌状态值遍历了整个相位空间.



(a) Logistic $\mu = 3.57$



(b) NUS $a = 1$

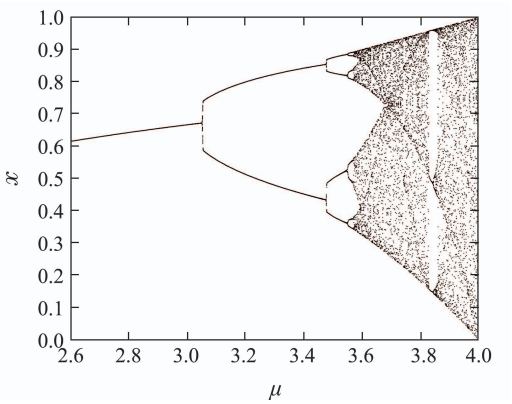
图 1 Logistic和NUS的空间遍历

Fig. 1 Spatial traversal of Logistic and NUS

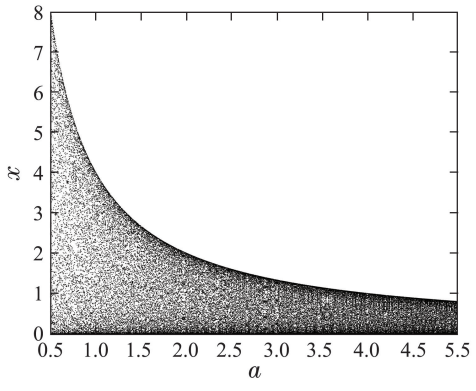
事实上, 只要参数a不等于0, NUS的混沌轨道都会遍历整个相空间. 同时, 随着参数a的减小, 相位空间将增大, 并且NUS的混沌状态值只在两端边界处稠密, 没有明显的周期带和聚集区域. 因此NUS具有更好的遍历性.

2.2 单峰混沌系统的分叉

对于混沌动力系统而言, “分岔”表示当系统参数变化时混沌系统特性的改变. 图2(a)描绘了Logistic系统的倍周期分叉, NUS的分叉如图2(b)所示.



(a) Logistic



(b) NUS

图 2 混沌动力系统的分叉

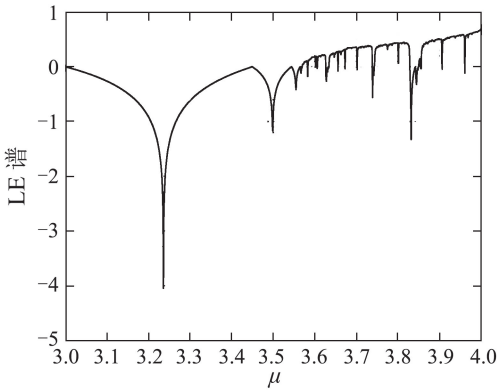
Fig. 2 Bifurcation of chaotic dynamical systems

从图2(a)中可以看出, Logistic映射在参数小于4时有许多周期性窗口, 参数μ只有在(3.57, 4]范围取值时, 系统才处于混沌状态, 这说明系统的混沌参数区间非常窄. 并且只有当参数$\mu = 4$时, 混沌轨道才能够遍历整个相空间(0, 1). 从图2(b)NUS的分岔图中可以发现, 在整个参数区间范围内没有明显的周期性窗口存在. 为了便于分析, 本文只描述了参数a在区间(0.5, 5)的情况. 事实上, 只要a不等于0, NUS就处于混沌状态. 此外, NUS的相位空间不仅局限在(0, 1) 范围内, 而是根据参数的改变而变化, 参数a 越小相位空间范围越大. 因此NUS具有更加稳定的混沌特性和更大的相位空间.

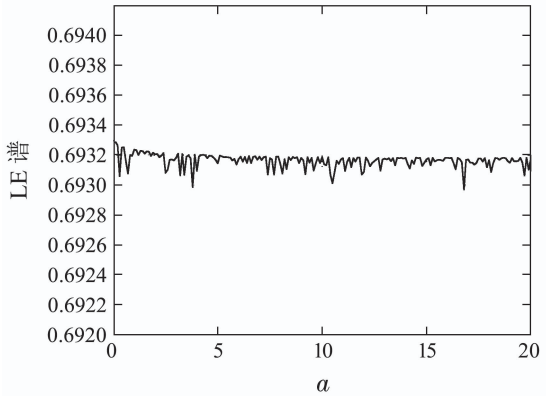
2.3 李雅普诺夫指数分析

李雅普诺夫指数(Lyapunov exponent, LE)表示相空间中动力系统的两个极其紧密的轨道的指数分离程度, 这是一个被广泛接受的表征混沌状态的指标. 如果动力系统处于混沌状态, 则必须至少有一个正的LE. 假设$f(x)$是一个可微函数, LE定义为

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)|.$$



(a) Logistic



(b) NUS

图 3 李雅普诺夫指数谱

Fig. 3 Lyapunov exponent spectrum

图3(a)和图3(b)描绘了Logistic和NUS的LE谱. 从图3(a)中可以看出, 当$\mu = 4$时, Logistic映射的LE最

大值为0.6931, 当$3.57 < \mu < 3.9$时, 存在许多小于0的LE. 当$\mu > 3.9$时, 大多数LE变为正值. 因此, Logistic具有正LE的参数范围很小而且并不连续. 相比之下, 当NUS的参数在0到20变化时, 李雅普诺夫指数始终保持在0.6933左右.

因此, 本文提出的单峰混沌系统具有连续宽泛的混沌参数区间和稳定的动力学特性, 是一个满足密码学安全属性要求的鲁棒性非线性动力系统.

2.4 单峰混沌系统的概率密度

对于Logistic映射, 当参数$\mu = 4$时, 式(1)的密度函数表示为

$$\rho_f(x) = \frac{1}{\pi\sqrt{x(1-x)}},\ x \in (0,1), \tag{3}$$

显然, Logistic映射的密度分布并不均匀, 这意味着该混沌映射直接生成的序列的随机性不能满足密码安全性需求. 但是可以利用式(3)来计算NUS的概率密度.

这里不妨设$F(x) = 4x(1-x), x \in (0,1)$并且$Q(x) = -ax^2 + 4x, a > 0, x \in (0, \frac{4}{a})$,

存在$h(x) = \frac{4}{a}(x)\ \ x \in (0,1)$, 那么有$h(x) \in (0, \frac{4}{a}), a > 0$.

由$h(F(x)) = Q(h(x))$可知$F(x)$和$Q(x)$是拓扑共轭的. 此外, 由拓扑传递性可知, 由于$F(x)$是混沌系统, 因此$Q(x)$也是混沌系统.

不妨设$Q(y) = -ay^2 + 4y,\ a > 0,\ y \in (0, \frac{4}{a})$, 根据点数守恒定律$\rho_{\rm F}(x){\rm d}x = \rho_{\rm Q}(y){\rm d}y$, 变形后得到

$$\rho_{\rm F}(x) = \rho_{\rm Q}(y)|\frac{{\rm d}y}{{\rm d}x}|. \tag{4}$$

把式(3)和$y = h(x)$代入式(4)中得到$\rho_{\rm Q}(\frac{4}{a}x) = \frac{a}{4\pi\sqrt{x(1-x)}}$, 则NUS的概率密度

$$\rho_{\rm Q}(x) = \frac{a}{\pi\sqrt{4ax - a^2x^2}},\ a > 0,\ x \in (0, \frac{4}{a}). \tag{5}$$

从式(5)可以得出结论: NUS的概率分布也是不均匀的. 因此, NUS不能直接用于设计密码系统. 为了获得高安全性的混沌序列, 必须对NUS进行均匀化处理.

3 单峰混沌系统相空间的均匀化

在上节中给出了NUS的概率密度函数, 从中可以推断NUS是呈非均匀分布的, 这不满足安全性要求, 因此在本节中, 提出了针对单峰混沌映射的一般性均匀化方法. 这里设NUS产生的混沌序列为x_n, 为了使其呈均匀分布, 本文对该序列的每一个状态值进行变换, 有$Y_n = \frac{4}{a\pi}\arcsin(\frac{a}{2}x_n - 1) + \frac{2}{a},\ a > 0,\ x \in (0, \frac{4}{a})$. 随机变量$Y$的分布函数为

$$F_{\rm Y}(y) = P(\frac{4}{a\pi}\arcsin(\frac{a}{2}X - 1) + \frac{2}{a} \leqslant y) =$$

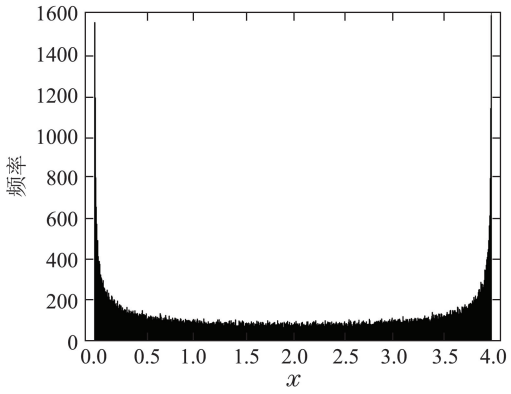
$$P(X \leqslant \frac{2}{a}\sin(\frac{a}{4}\pi y - \frac{\pi}{2}) + \frac{2}{a}) =$$

$$\int_{-\infty}^{\frac{2}{a}\sin(\frac{a}{4}\pi y - \frac{\pi}{2}) + \frac{2}{a}} \rho_{\rm X}(x){\rm d}x.$$

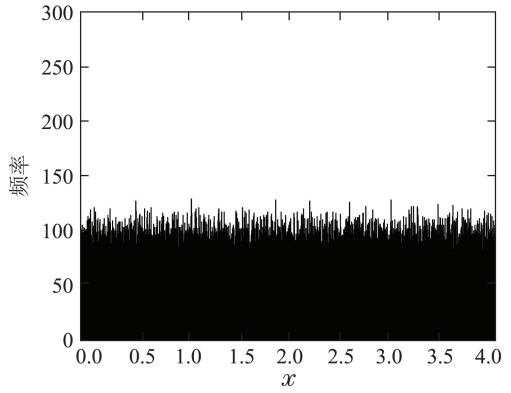
对等式两边求导得到随机变量Y的概率密度函数为

$$\rho_{\rm Y}(y) = \begin{cases} \dfrac{a}{4},\ 0 < y < \dfrac{4}{a}, \\ 0,\ \ \text{其他}. \end{cases} \tag{6}$$

由于参数a是常量, 因此Y的概率密度为常数, 即Y服从均匀分布. 图4描述的是NUS均匀化变换前后当$a = 1$时的统计特性直方图. 由图4(a)可以看出, 在均匀化之前NUS的分布是呈“U”型的, 通过均匀化处理, 在图4(b)中, NUS的统计结果呈均匀分布, 从而验证了该均匀化变换的有效性.



(a) 均匀化前



(b) 均匀化后

图 4 NUS统计直方图

Fig. 4 Statistics histogram for NUS

4 单峰混沌系统的改进方案

在第2.3节中, NUS的李雅普诺夫指数的计算值为

0.6933. 虽然该值是恒定为正的, 但仍然很低. 为了进一步增强系统的混沌特性, 增大李雅普诺夫指数, 本文给出了一个针对NUS的改进方案(improvement for unimodal chaotic system, IUS).

定理 1　$f(x)$和$g(x)$是相空间$\mathbb{R}^n$中的两个混沌系统, λ_1和λ_2是两个混沌系统的李雅普诺夫指数, 则复合函数$f(g(x))$的李雅普诺夫指数为$\lambda_1+\lambda_2$.

证　根据李雅普诺夫指数的定义, 复合函数$f(g(x))$的李雅普诺夫指数可表示为

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|[f(g(x_i))]'\right|=$$

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|\frac{\mathrm{d}f(g(x_i))}{\mathrm{d}g(x_i)}\right|+\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|\frac{\mathrm{d}g(x_i)}{\mathrm{d}(x_i)}\right|=$$

$\lambda_1+\lambda_2$.

证毕.

设$f(x)=-ax^2+4x$且$g(x)=\dfrac{4}{a}\sin(\dfrac{a}{4}\pi x)$, $a>0,\ x\in(0,\ \dfrac{4}{a})$.

$f(x)$是NUS系统, 它的LE为0.6933, $g(x)$是一个扩展的正弦混沌映射, 最大LE为0.6911. $f(x)$和$g(x)$具有相同的定义域和值域, 因此改进的复合系统IUS可以表示为

$$f(g(x_{n+1}))=$$
$$-a(\frac{4}{a}\sin(\frac{a}{4}\pi x_n))^2+4(\frac{4}{a}\sin(\frac{a}{4}\pi x_n)).$$

根据定理1, IUS的最大李雅普诺夫指数计算结果为1.3844. 为了进一步验证定理1的可靠性, 计算了不同参数下的IUS的李雅普诺夫指数, 如图5所示. 根据图5的曲线, 发现IUS的李雅普诺夫指数在1.3844附近波动, 理论分析与实验结果是一致的.

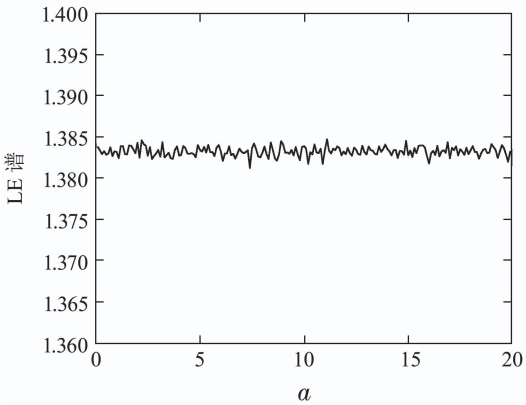


图 5　IUS李雅普诺夫指数谱

Fig. 5　Lyapunov exponent spectrum for IUS

通过数值计算, 笔者发现IUS序列的不变分布与NUS均匀化前近似相等, 皆为图4(a)中呈现的“U”型分布. 因此, 采用第3节中的变换方法对IUS进行均匀化处理. 由IUS定义可得

$$x_{n+1}=-a(\frac{4}{a}\sin(\frac{a}{4}\pi x_n))^2+4(\frac{4}{a}\sin(\frac{a}{4}\pi x_n)).$$

对序列x_n进行均匀化变换:

$$y_{n+1}=\frac{4}{a\pi}\arcsin(\frac{a}{2}x_{n+1}-1)+\frac{2}{a},$$

$a>0,\ y\in(0,\ \dfrac{4}{a})$, 则序列$y_{n+1}$即为IUS均匀化后的混沌序列.

图6为均匀化后的IUS的统计直方图(参数$a=0.5$), 从图中也可以发现, 均匀化后的混沌序列基本呈等概率分布.

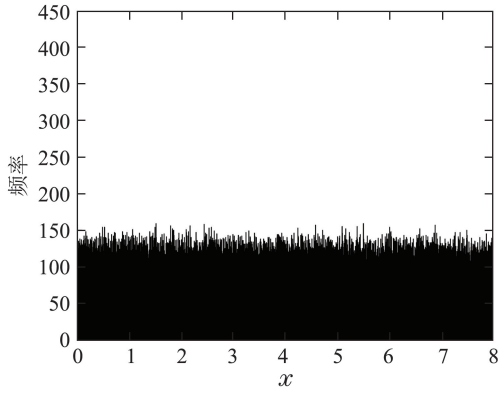


图 6　均匀化后的IUS统计直方图

Fig. 6　Statistics histogram for IUS after homogenization

5　性能指标分析

5.1　信息熵

信息熵用于描述与随机性特征相关的信息冗余程度, 如果一个序列的信息熵较大, 那么该序列具有更好的随机性和不确定性. 设混沌序列的长度为N, 落在每个统计区间内的混沌值的个数为$n_i(i=1,2,3,\cdots,M$, M为统计区间个数). 区间统计概率为$p_i=n_i/N$, 则由信息熵的定义有$H=-\sum_{i=1}^{M}p_i\log_2 p_i$. 根据信息熵的极值性原理, 当信源在统计区间内呈等概率分布时, 熵函数具有极大值, 其极大值可表示为$\max(H)=\log_2 M$. 当设定统计区间个数M为2^8时, 得到序列信息熵的最大值为8.

分别在不同的参数a下计算了IUS在均匀化前后的信息熵值, 结果如表1所示. 从表1结果可以发现, 均匀化过程明显提高了IUS的信息熵值, 此外, 均匀化后的信息熵并没有随着参数a的改变而发生较大波动, 皆近似等于理论最大值. 这说明均匀化后的IUS系统可以产生具有强随机特性的混沌序列.

表 1 IUS信息熵

Table 1 Information entropy of IUS

a	均匀化前	均匀化后
0.5	7.6876	7.9997
1	7.6871	7.9997
2	7.6857	7.9998
3	7.6879	7.9998
4	7.6811	7.9998

5.2 近似熵

近似熵是用于测量信号复杂度的非线性动力学指标. 这里引入它来评估混沌系统的随机性. 本节中按照文献[16]的方法计算了一些经典混沌映射和相关研究的近似熵值, 结果如表2所示.

表 2 近似熵对比分析

Table 2 Comparison analysis for approximate entropy

混沌系统	参数取值	近似熵
Logistic映射	$u=4$	0.6528
Tent映射	$u=2$	0.6342
文献[10]	LTS $r=u=a=4$	0.6416
文献[17]	$a=-1.5,\ b=2.8,\ c=0.96$	0.6504
IUS	$a=0.5$	1.2403

从表2可以看出, 本文提出的IUS系统的近似熵值为1.2403, 比两个经典的混沌映射和两个相关文献的结果要高很多. 这说明本文提出的IUS系统具有更好的随机特性.

5.3 对比分析

为进一步将本文的研究与相关文献进行对比, 表3列出了相关研究的结果. 针对低维离散混沌系统, 李雅普诺夫指数、轨道分布和相空间是从密码学角度考量一个非线性系统的3个重要指标.

表 3 相关研究比较分析

Table 3 Comparative analysis of relevant researches

混沌系统	李雅普诺夫指数	均匀化处理	相空间
文献[11]	0.6931	否	(0,1)
文献[13]	10.7	否	(0,1)
文献[15]	0.5434	否	(0,1)
文献[17]	0.6931	是	$(-0.5, 0.5)$
本文IUS	1.3844	是	(0, 4/a)

由于低维混沌的相空间概率分布不均匀, 许多文献都提出了一些改进方法, 但除了文献[17]以外绝大多数研究没有对混沌序列进行均匀化处理. 相空间与密钥空间密切相关, 但在表3中并没有相关研究对相空间进行扩展. 尽管表3中显示的所有研究的最大李雅普诺夫指数都是正的, 但其并不具有稳定性, 不能在整个参数区间都保持恒定. 本文的方案具有稳定的正李雅普诺夫指数、扩展的相空间, 并对混沌轨道进行了均匀化处理. 通过对比分析可以发现本文提出的单峰混沌系统的改进形式具有更好的动力学特性和随机特性.

6 结论

为了构造一个更加安全的非线性密码部件, 本文提出了一个新的一维单峰混沌系统及其改进的复合形式. 通过比较分析可知NUS具有更好的遍历性, 更稳定的李雅普诺夫指数, 更大的相空间和混沌参数范围. 为了实现混沌序列的均匀分布, 本文提出了一种普适性的均匀化方法, 并给出了严格的证明过程. 通过复合迭代的形式使得系统的动力学特性和随机特性进一步增强. 数值分析和对比分析结果表明本文提出的混沌系统在鲁棒性、随机性和安全性方面具有明显优势, 可以作为密码系统的非线性部件来使用.

参考文献:

[1] WANG Chuanfu, DING Qun. SM4 key scheme algorithm based on chaotic system. *Acta Physica Sinica*, 2017, 66(2): 020504.
(王传福, 丁群. 基于混沌系统的SM4密钥扩展算法. 物理学报, 2017, 66(2): 020504.)

[2] SHEN Zhiping, WU Yilin. Asymptotic stability of equilibrium points of uncertain unified chaotic systems. *Control Theory & Applications*, 2016, 33(1): 98 – 105.
(沈志萍, 邬依林. 不确定统一混沌系统平衡点的渐近稳定. 控制理论与应用, 2016, 33(1): 98 – 105.)

[3] WEN Heping, YU Simin, LÜ Jinhu. Encryption algorithm based on Hadoop and non-degenerate high-dimensional discrete hyperchaotic system. *Acta Physica Sinica*, 2017, 66(23): 230503.
(温贺平, 禹思敏, 吕金虎. 基于Hadoop大数据平台和无简并高维离散超混沌系统的加密算法. 物理学报, 2017, 66(23): 230503.)

[4] LI Zhenbo, TANG Jiashi. Chaotic synchronization with parameter perturbation and its secure communication scheme. *Control Theory & Applications*, 2014, 31(5): 592 – 600.
(李震波, 唐驾时. 参数扰动下的混沌同步控制及其保密通信方案. 控制理论与应用, 2014, 31(5): 592 – 600.)

[5] LIU Wei, WANG Yanyan, WANG Zhiming. Synchronization for a class of discrete-time chaotic control systems under communication constraints . *Control Theory & Applications*, 2014, 31(8): 1128 – 1132.
(刘伟, 王岩岩, 汪志鸣. 一类离散混沌系统的传输受限同步问题. 控制理论与应用, 2014, 31(8): 1128 – 1132.)

[6] ZHANG F, CHEN R, WANG X, et al. Dynamics of a new 5D hyperchaotic system of lorenz type. *International Journal of Bifurcation and Chaos*, 2018, 28(3): 1850036.

[7] LIU H, WANG X. Triple-image encryption scheme based on one-time key stream generated by chaos and plain images. *Journal of Systems and Software*, 2013, 86(3): 826 – 834.

[8] LIU Y, TANG S, LIU R, et al. Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Systems with Applications*, 2018, 97: 95 – 105.

[9] PARVAZ R, ZAREBNIA M. A combination chaotic system and application in color image encryption. *Optics and Laser Technology*, 2018, 101: 30 – 41.

[10] ZHOU Y, BAO L, CHEN C L P. A new 1D chaotic system for image encryption. *Signal Processing*, 2014, 97(7): 172 – 182.

[11] JEANETH M, ODEMIR M B. Improving the pseudo-randomness properties of chaotic maps using deep-zoom. *Chaos*, 2017, 27(5): 053116.

[12] FATIH O. A novel method to improve the performance of chaos based evolutionary algorithms. *Optik*, 2015, 126(24): 5434 – 5438.

[13] MA M, CRUZ H C, CARDOZA A L, et al. A novel pseudorandom number generator based on pseudo randomly enhanced logistic map. *Nonlinear Dynamics*, 2017, 87(1): 407 – 425.

[14] LIU Y, LUO Y, SONG S, et al. Counteracting dynamical degradation of digital chaotic chebyshev map via perturbation. *International Journal of Bifurcation and Chaos*, 2017, 27(3): 1750033.

[15] HUA Z, ZHOU Y. Dynamic parameter-control chaotic system. *IEEE Transactions on Cybernetics*, 2016, 46(12): 3330 – 3341.

[16] CHEN Xiaojun, LI Zan, BAI Baoming, et al. New complexity metric of chaotic pseudorandom sequences using fuzzy relationship entropy. *Acta Physica Sinica*, 2011, 60(6): 064215.
(陈小军, 李赞, 白宝明, 等. 一种确定混沌伪随机序列复杂度的模糊关系熵测度. 物理学报, 2011, 60(6): 064215.)

[17] ZANG Hongyan, CHAI Hongyu. Homogenization and entropy analysis of a quadratic polynomial chaotic system. *Acta Physica Sinica*, 2016, 65(3): 030504.
(臧鸿雁, 柴宏玉. 一个二次多项式混沌系统的均匀化及其熵分析. 物理学报, 2016, 65(3): 030504.)

作者简介:

徐　辉　博士研究生, 从事混沌密码与多媒体安全研究, E-mail: banmianstudent@163.com;

佟晓筠　教授, 博士生导师, 从事混沌密码与信息安全研究, E-mail: tong_xiaojun@163.com;

张　淼　博士, 讲师, 从事混沌密码与图像加密研究, E-mail: zhangmiaozm209@126.com;

刘　杨　博士, 讲师, 从事密码学和信息安全研究, E-mail: ly_windy@126.com;

王　翥　博士, 教授, 从事无线传感器网络与检测技术研究, E-mail: wangzhu@hit.edu.cn.