Logistic 混沌映射性能分析与改进

陈志刚[①③] 梁涤青[*②③④] 邓小鸿[③⑤] 张 颖[⑥]
[①](中南大学软件学院 长沙 410075)
[②](中南大学信息科学与工程学院 长沙 410083)
[③](中南大学“移动医疗”教育部—中国移动联合实验室 长沙 410075)
[④](长沙理工大学信息化建设与管理处 长沙 410114)
[⑤](江西理工大学应用科学学院 赣州 341000)
[⑥](长沙理工大学电气与信息工程学院 长沙 410114)

摘 要：混沌系统是基于混沌的数据加密领域的一个重要研究对象，Logistic 混沌映射是最简单和有效的混沌系统，被广泛应用在大多数混沌加密算法中，Logistic 映射的安全性成为研究的热点。针对 Logistic 序列存在的吸引子与空白区问题，该文提出一种基于初始值和分形控制参数之间关系的 Logistic 映射改进方法。利用两者之间关系对映射自变量区间进行合理分段，扩大了混沌控制参数区域，将满射范围扩大到整个控制参数区间，使产生的序列分布更均匀，解决了“稳定窗”与空白区等问题。通过将改进 Logistic 与其它分段 Logistic 映射进行仿真对比，实验结果表明改进后的映射产生的序列混沌特性得到显著加强，分布更均匀，具有更好的随机性能测试指标。另外，改进 Logistic 映射计算复杂度低，实现简单，在扩频通信与混沌密码等领域有广阔的应用前景。

关键词：数据加密；Logistic 映射；混沌序列；安全性
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2016)06-1547-05
DOI: 10.11999/JEIT151039

Performance Analysis and Improvement of Logistic Chaotic Mapping

CHEN Zhigang[①③] LIANG Diqing[②③④] DENG Xiaohong[③⑤] ZHANG Ying[⑥]
[①](*College of Software*, *Central South University*, *Changsha* 410075, *China*)
[②](*School of Information Science and Engineering*, *Central South University*, *Changsha* 410083, *China*)
[③](“*Mobile Health*” *Ministry of Education-China Mobile Joint Laboratory*, *Central South University*, *Changsha* 410075, *China*)
[④](*Informatization Construction and Management Department*, *Changsha University of Science and Technology*, *Changsha* 410114, *China*)
[⑤](*College of Applied Science*, *Jiangxi University of Science and Technology*, *Ganzhou* 341000, *China*)
[⑥](*College of Electrical and Information Engineering*, *Changsha University of Science and Technology*, *Changsha* 410114, *China*)

Abstract: Chaotic system is an important research object in the field of data encryption based on the chaos. The logistic chaotic mapping is the simplest and efficient chaotic system and is usually used by many encryption methods based on the chaos, thus the security of Logistic mapping becomes an important research point. To deal with the issue of attractors and blank area of the presence of the Logistic sequence, an improved Logistic mapping based on the relationship between initial value and the fractal control parameters is proposed. The variables interval of chaotic mapping is reasonable subsection by using this relationship, so the chaos control parameter region can be expanded, and the onto mapping range is extended to the entire control parameter interval. The improved Logistic mapping makes the chaotic sequence distribution more uniform, and solves the problem of “stability window”and the blank area etc. Compared with the improved Logistic and piecewise chaotic Logistic, the experimental results show that the chaotic characteristics of sequence generated by the improved mapping is significantly strengthened, has more uniform distribution, and better random performance index. In addition, the improved Logistic mapping has low computational complexity and is prone to implement. The improved Logistic mapping has broad application prospects in the fields of spread spectrum communication and chaotic cipher.

Key words: Data encryption; Logistic mapping; Chaotic sequence; Security

1 引言

混沌理论研究被认为继量子力学与相对论之后的第 3 大科学发现，混沌现象是非线性动力映射的复杂动力学主要表现形式之一，具有良好的类随机、非周期、对初始值敏感、历经各态并可确定等特性，被信息安全、扩频通信及工业控制等领域的研究者们广泛关注[1−3]。

混沌映射中 Logistic 虽然形式简单，但有非常复杂的动力学特性。经研究发现[4,5]，Logistic 映射存在如下问题：(1)存在无穷不动点。当 Logistic 控制参数 μ 与初始值 x_0 存在 $x_0\mu=1$ 或 $x_0\mu=\mu-1$ 关

收稿日期：2015-09-14；改回日期：2016-02-29；网络出版：2016-04-07
*通信作者：梁涤青 billldq@163.com
基金项目：国家自然科学基金(61272494, 61350011)，江西省教育厅科研项目(GJJ151522)
Foundation Items: The National Natural Science Foundation of China (612724494, 61350011), Educational Commission Science Foundation of Jiangxi Province of China (GJJ151522)

系时，其相空间中存在无数的不动点；(2)稳定窗问题与空白区问题。控制参数 μ 在(0,4)取值时，Logistic 迭代点取值分布过于集中，形成点聚集区域，而相空间其它区域出现空白带。(3)使映射处于满映射状态的参数区域过小，只有当参数取值为 4 时，Logistic 才处于满映射状态。而当 μ 在(3.570,4)之间时，Logistic 处于混沌区间，但其均匀分布特性较差。如将其应用于混沌加密中时将产生密钥空间过小，存在大量弱密钥，产生的混沌序列分布不均匀等安全隐患[6]。

为改善 Logistic 映射产生序列的混沌特性，文献[7,8]将 Logistic 映射从 1 维扩展到 2 维，将分岔提前，但增加了计算复杂度，且混沌序列均匀分布性降低。文献[9]利用分段进行扩展，但没有考虑参数与初始值特定条件下存在的吸引子问题。文献[10]利用 Logistic 跟其它非线性映射结合，Logistic 原有均匀性被破坏；文献[11]给出了针对分段线性函数数字化混沌映射进行扰动的方案，改进了序列的随机性能，但计算量增大。文献[12]提出利用扰动间隔动态变化的扰动方法，其扰动量依赖于被扰动映射的李雅谱诺夫指数和当前的扰动间隔，效率比较低；文献[13]采用可扩展精度并行方法对 Logistic 映射分步计算，利用动态数组保存计算结果，映射空间得到扩大。但该方法增大计算复杂度，且计算环境不具有普适性。

上述方法只可部分地解决 Logistic 映射中存在的问题，本文提出的改进方法在充分考虑 μ 与 x_0 关系的前提下对变量区间进行分段，在不增加计算复杂的情况下，使 Logistic 处于混沌状态下的分形参数范围扩大到(0,6)区域，在整个参数范围内 Logistic 映射连续无间断地无限接近满映射状态。

2 Logistic 映射性能分析

经典 Logistic 映射数学表达形式为

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

其中控制参数 $\mu\in(0,4]$，$x\in(0,1)$，Logistic 映射经历的状态跟控制参数 μ 密切相关。

定理 1 $x_{n+1}=\mu x_n(1-x_n)$ 的最大值为 $\mu/4$，最小值为 $\mu^2/4-\mu^3/16$。

证明 设 $f(x)=\mu x(1-x)$，因为 $f(x)$ 在 $x\in(0,1)$ 上为连续可导函数，故 $f(x)$ 的最大值或最小值存在其极值之中。当 $f'(x)=df(x)/dx=0$，即 $\mu-2\mu x=0$ 时可得到 $f(x)$ 极值，解方程可得 $x=1/2$，故 $f(x)$ 可能的极值点分别到 $x=1/2$，$x=0$ 和 $x=1$ 时。分别将 x 的取值代入到式(1)中得 $f(0)=f(1)=0$，$f(1/2)=\mu/4$。所以 $f(x)$ 最大值为 $\mu/4$。根据抛物线最大值与最小值性质可知：当 $x_n=\mu/4$ 时，则 $f(x)$ 取得最小值，将 $x_n=\mu/4$ 代入式(1)中得最小值为 $\mu^2/4-\mu^3/16$。 证毕

推论 1 由定理 1 可推出：x_n 的取值与控制参数 μ 相关。随着参数 μ 的增大，序列取值范围越大，分布越均匀。当 $\mu=4$ 时，Logistic 映射趋向满映射，分布最均匀。$\mu\in(0,4)$ 时混沌序列分布不均匀。

定理 2 ε 为任意小的正实数，在混沌区域中 Logistic 映射初始取值范围在 $[(\mu-1)/2\mu,(\mu+1)/2\mu]$ 时，生成的迭代值为 $\mu/4-\varepsilon$ (往上界 $\mu/4$ 附近压缩)。当 Logistic 映射初始值取值接近上界 $\mu/4$ 时，下一轮迭代值为 $\mu^2/4-\mu^3/16-\varepsilon$ (无限接近下界 $\mu^2/4-\mu^3/16$)。

证明 令 $x_n=(\mu-1)/2\mu$，则 $x_{n+1}=(\mu^2-1)/4\mu$；令 $x_n=(\mu+1)/2\mu$，则 $x_{n+1}=(\mu^2-1)/4\mu$；令 $x_n=1/2$，由定理 1 知 $x_{n+1}=\mu/4$。由上述 3 个等式可推导出：当 x_n 取值 $[(\mu-1)/2\mu,(\mu+1)/2\mu]$ 时，则 x_{n+1} 的值域为 $\left[(\mu^2-1)/4\mu,\mu/4\right]$。即 Logistic 映射初始值取值范围在 $[(\mu-1)/2\mu,(\mu+1)/2\mu]$ 时，初值的区间宽度为 $1/2\mu$，下一轮迭代值接近上界 $\mu/4$，区间宽度压缩至 $1/4\mu$。

综上所述，Logistic 不断迭代将会在上界附近形成点聚集区域。设 $x_n=\mu/4-\varepsilon$ 且其取值范围为 $[(\mu^2-1)/4\mu,\mu/4]$，其中 ε 为任意小的正实数，则 $x_{n+1}=(\mu^2/4-\mu^3/16)+\mu[(\mu/2-1)\varepsilon-\varepsilon^2]$，由此得知，当 Logistic 映射初始值取值接近上界 $\mu/4$ 时，下一轮迭代无限接近下界 $\mu^2/4-\mu^3/16$。

推论 2 从定理 2 可推出 μ 在某些取值范围内时相空间形成点聚集区和空白区。Logistic 映射只有在控制参数 $\mu=4$ 时才能达到满映射，其分布相对较为均匀。如 μ 取值为 3.735 时，序列在区间(0,0.2153)呈现空白区，在区间(0.66,0.9)形成聚集区。

3 Logistic 映射性能改进

由上述分析可以得知，当初值取 $\left[\frac{\mu-1}{2\mu},\frac{\mu+1}{2\mu}\right]\cup\left[\frac{\mu}{4}-\varepsilon,\frac{\mu}{4}\right]\cup\left[\frac{\mu^2}{4}-\frac{\mu^3}{16},\frac{\mu^2}{4}-\frac{\mu^3}{16}+\varepsilon\right]$ 时，映射容易陷入吸引子问题，改进 Logistic 映射避免 μ 落于该区，当取值落在上述区段时，使用控制参数为 4。方程式如式(2)所示。

$$x_{n+1}=\begin{cases}4x_n(1-x_n), & \dfrac{1}{2}-\sqrt{\dfrac{1}{4}-\dfrac{\lfloor\mu/4\rfloor}{\mu}}\le x_n\le\dfrac{1}{2}+\sqrt{\dfrac{1}{4}-\dfrac{\lfloor\mu/4\rfloor}{\mu}}\\ 1-\mu x_n(1-x_n), & \text{其它}\end{cases} \tag{2}$$

定理 3 式(2)的取值范围为(0,1)。

证明

$$f(x)=\begin{cases}4x_n(1-x_n), \\ \quad \dfrac{1}{2}-\sqrt{\dfrac{1}{4}-\dfrac{\lfloor \mu/4 \rfloor}{\mu}} \le x_n \le \dfrac{1}{2}+\sqrt{\dfrac{1}{4}-\dfrac{\lfloor \mu/4 \rfloor}{\mu}} \\ 1-\mu x(1-x), \qquad \text{其它}\end{cases}$$

因为 $f(x)$ 在 $x\in(0,1)$ 上为连续可导函数，所以 $f(x)$ 的最值存在于其极值之中，当 $f'(x)=df(x)/dx=0$，即 $\mu-2\mu x=0$ 或 $8x-4=0$ 时可得到 $f(x)$ 极值，可解得一个极值点 $x=1/2$。故 $f(x)$ 可能的极值点分别到 x=1/2，x=0 和 $x=\dfrac{1}{2}-\sqrt{\dfrac{1}{4}-\dfrac{\lfloor \mu/4 \rfloor}{\mu}}$ 和 $x=\dfrac{1}{2}+\sqrt{\dfrac{1}{4}-\dfrac{\lfloor \mu/4 \rfloor}{\mu}}$ 时。分别将可能极值点按照分段范围代入式(1)中得 $f(x)$ 为 0 或 1，故得证。

由定理 3 知，改进 Logistic 映射分布范围比原始 Logistic 映射大，其遍历性也比原始 Logistic 映射好。改进 Logistic 的初始值为 0.001，控制参数分别为 0.001, 0.8, 1.0, 4.0，其相空间与时间序列分布如图 1 所示。不同的控制参数与初始值函数每次迭代 50000 次，选其中间连续的 10000 个(第 20001 个至第 30000 个)。

从图 1 中可以看出，改进 Logistic 的混沌控制参数区域得以扩展，在所有控制参数的范围内均处于混沌状态，满映射区域扩大。

4　性能对比分析

在时间性能上，改进 Logistic 映射只多了一次取值范围的比对，通过将两种映射分别迭代 50000 次，相差时间在 0.002 s。另外，空间复杂度也没有变化。下面重点对两种 Logistic 映射的初值敏感度和随机性进行对比。

4.1 初始值敏感度

将初始值相差微小的两列混沌序列进行符号化，统计 0 与 1 的在相应位置的变化个数，计算位变化率：$T=n'/n$。其中，n 表示混沌序列长度。初始值微小变化后产生的二值序列与原二值序列进行对比，n' 为两序列对应位置数值不同的个数。位变化率接近 0.5，敏感度越强，敏感度对比结果如表 1 所示。根据不同初始值与控制参数，3 种不同函数每次迭代 50000 次，取连续的 10000 个点(即第 30001 个至第 40000 个)。

表 1 表明，Logistic 控制参数影响到 Logistic 映射对初始参数的敏感度，控制参数为 4 时其敏感度比控制参数为 3.8 时更强。改进 Logistic 位变化率更接近于 0.5，其敏感度总体上比 Logistic 与分段 Logistic 强。

4.2 随机性能比较

本文采用最常用的方法 NIST 测试法比较序列的随机性能。为使分析更客观，使用常见的均值静态法将实数转化为 0 与 1。每次迭代 20000 次，去掉序列前面的 10000 次迭代值，消除混沌序列的暂态效应。当伪随机序列的实际测试通过率超过最小值 P_α 时，被认为通过 NIST 测试。P_α 定义为

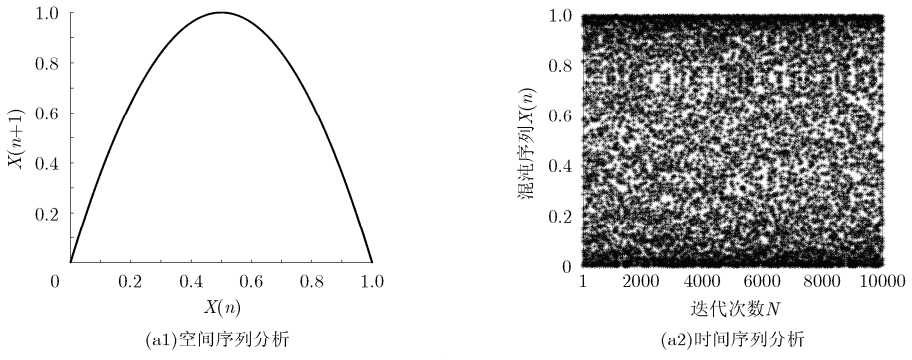
$$P_\alpha=(1-\alpha)\pm 3\sqrt{\alpha(1-\mathrm{a})/M} \tag{3}$$

其中，$\alpha\in[0.001,0.01]$。取 $\alpha=0.001$，序列总数 $M=100$，则 $P_\alpha\approx 0.9602$。用原始 Logistic 与改进 Logistic 进行迭代，各取 100 条长度为 10000 的混沌序列用于检验，当通过率大于 P_α 时，说明混沌序列具有良好的随机性和相应的应用价值。

实验中 Logistic 控制参数取最佳参数值 4，改进 Logistic 控制参数取(0,4)以内的任意数，因其在此区间上的控制参数产生的序列均匀性基本一致，这里取 0.7。3 种映射产生的序列都能通过 NIST 测试，并且在测试项目频数、分组频数、最长游程测试、矩阵秩、Maurer 通用统计、线性复杂度、近似熵、前向累加和、后向累加和、随机游走和随机游走指标上都均达到 100%，其他具有差异的 NIST 测试结果如表 2 所示。改进 Logistic 测试通过率比原始 Logistic 及文献[9]方案更高，说明改进 Logistic 映射产生序列随机性能更好。

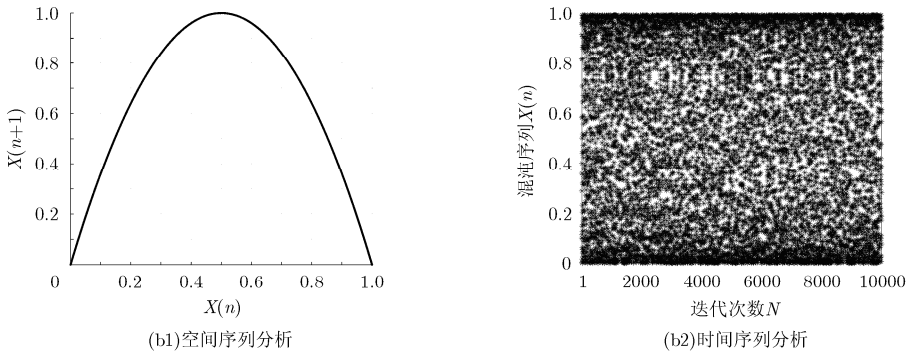
表 1 对初始值的敏感度比较

混沌映射初始值	0.1	0.2	0.3	0.4
变化后的初始值	0.100001	0.200001	0.300001	0.400001
Logistic($\mu=3.8$)	0.5112	0.48887	0.5232	0.4798
Logistic($\mu=4$)	0. 5038	0. 5013	0. 4983	0. 5012
文献[9] Logistic($\mu=3.9$)	0.5087	0.5016	0.5021	0.5032
改进 Logistic($\mu=1$)	0.5008	0.5003	0.5007	0.5001



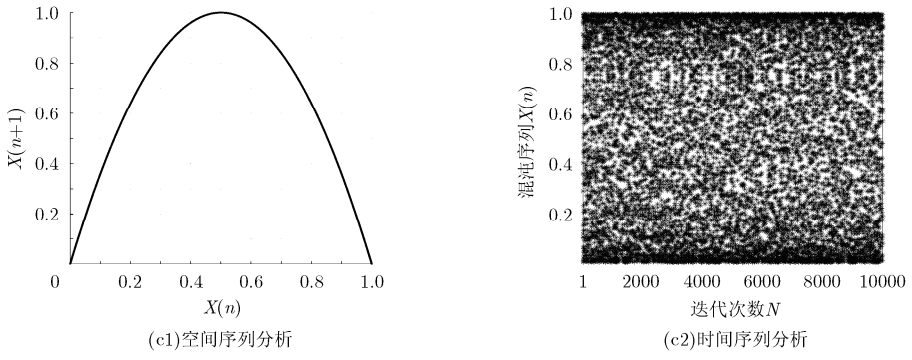
(a1)空间序列分析 (a2)时间序列分析

(a) μ=0.001



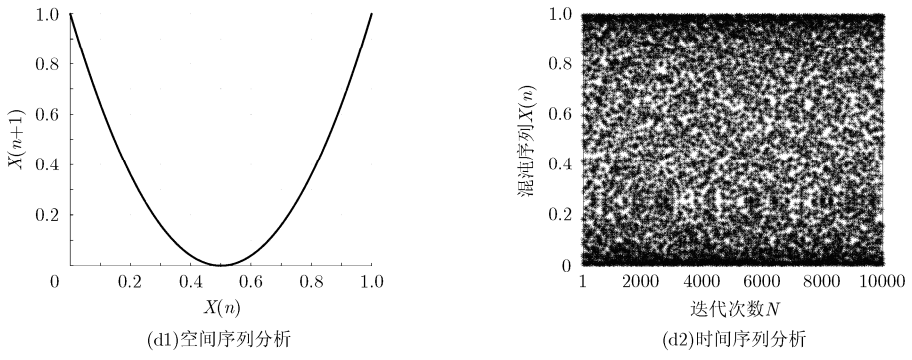
(b1)空间序列分析 (b2)时间序列分析

(b) μ=0.8



(c1)空间序列分析 (c2)时间序列分析

(c) μ=1.0



(d1)空间序列分析 (d2)时间序列分析

(d) μ=4.0

图 1 改进 Logistic 选取 4 个不同控制参数形成的空间序列与时间序列图

5 结束语

改进 Logistic 映射基于初始值与控制参数之间存在的关系对变量域进行分段处理，扩大了映射的混沌控制参数区域；整个控制参数区域内映射无限接近满映射；产生的混沌序列具有很好的均匀分布特性，解决了“稳定窗”、空白区及不动点等吸引子问题，改进 Logistic 混沌映射具有更好的随机性和广泛的应用前景。后续研究明确界定改进 Logistic 的控制参数范围，简化初始值与控制参数之间的关系，平衡映射整体与局部均匀分布，基于并行计算与浮点数等技术提高映射序列产生效率，进一步降低计算复杂度。

表 2　NIST 测试结果对比

测试项目	NIST 测试项目通过率(%)		
	原始 Logistic	文献[9]分段 Logistic	改进 Logistic
游程测试	98	98	100
频谱测试	98	98	99
非重叠模式匹配测试	97	98	98
重叠模式匹配测试	98	98	100
串行测试	99	100	100

参 考 文 献

[1] LEE Tianfu. Enhancing the security of password authenticated key agreement protocols based on chaotic maps[J]. *Information Sciences*, 2015, 290(1): 63–71. doi: 10.1016/j.ins.2014.08.041.

[2] TONG Xiaojun. Design of an image encryption scheme based on a multiple chaotic map[J]. *Communications in Nonlinear Science and Numerical Simulation*, 2013, 18(7): 1725–1733. doi:10.1016/j.asoc.2015.08.008.

[3] 刘泉, 李佩玥, 章明朝, 等. 基于可 Markov 分割混沌系统的图像加密算法[J]. 电子与信息学报, 2014, 36(6): 1271–1277. doi:10.3724/SP.J.1146.2013.01246.
LIU Quan, LI Peiyue, ZHANG Mingchao, *et al*. Image encryption algorithm based on chaos system having Markov portion[J]. *Journal of Electronic & Information Technology*, 2014, 36(6): 1271–1277. doi:10.3724/SP.J.1146.2013.01246.

[4] 徐红梅, 郭树旭. 基于符号相对熵的 Logistic 混沌系统时间不可逆性分析[J]. 电子与信息学报, 2014, 36(5): 1242–1246. doi: 10.3724/SP.J.1146.2013.01262.
XU Hongmei and GUO Shuxu. Time irreversibility analysis of logistic chaos system based on symbolic relative entropy[J]. *Journal of Electronics & Information Technology*, 2014, 36(5): 1242–1246. doi:10.3724/SP.J.1146.2013.01262.

[5] ZHENG Pan, MU ChunLai, HU Xuegang, *et al*. Boundedness of solutions in a chemotaxis system with nonlinear sensitivity and logistic source[J]. *Journal of Mathematical Analysis and Applications*, 2015, 424(1): 509–522. doi: 10.1016/j.jmaa.2014.11.031.

[6] WANG Mingxin. The diffusive logistic equation with a free boundary and sign-changing coefficient[J]. *Journal of Differential Equations*, 2015, 258(4): 1252–1266. doi:10.1016/j.jde.2014.10.022.

[7] 王兴元, 王明军. 二维 Logistic 映射的混沌控制[J]. 物理学报, 2008, 57(2): 731–736.
WANG Xingyuan and WANG Ming-jun. Chaotic control of the coupled Logistic map[J]. *Acta Physica Sinica*, 2008, 57(2): 731–736.

[8] 王兴元, 骆超. 二维 Logistic 映射的动力学分析[J]. 软件学报, 2006, 17(4): 729–739.
WANG Xingyuan and LUO Chao. Dynamic analysis of the coupled logistic map[J]. *Journal of Software*, 2006, 17(4): 729–739.

[9] 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 Jiulun and ZHANG Xuefeng. Piecewise logistic chaotic map and its performance analysis[J]. *Acta Electronica Sinica*, 2009, 37(4): 720–725.

[10] HUA Zhongyun, ZHOU Yicong, PUN Chiman, *et al*. 2D sine logistic modulation map for image encryption[J]. *Information Sciences*, 2015, 297(1): 80–94. doi: 10.1016/j.ins.2014.11.018.

[11] 刘建东, 付秀丽. 基于耦合帐篷映射的时空混沌单向 Hash 函数构造[J]. 通信学报, 2007, 28(6): 30–38.
LIU Jiandong and FU Xiuli. Spatiotemporal chaotic one-way hash function construction based on coupled tent maps[J]. *Journal on Communications*, 2007, 28(6): 30–38.

[12] 刘金梅, 丘水生. 基于 Lyapunov 指数改善数字化混沌系统的有限精度效应[J]. 暨南大学学报(自然科学版), 2010, 31(5): 425–430.
LIU Jinmei and QIU Shuisheng. Minimizing finite precision effects of digital chaotic systems by virtue of Lyapunov exponent[J]. *Journal of Jinan University* (*Natural Science Edition*), 2010, 31(5): 425–430.

[13] 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.
LIU Jiahui and ZHANG Hongli. A parallel computing method of chaotic random sequence based on logistic map with scalable precision[J]. *Journal of University of Science and Technology of China*, 2011, 41(9): 837–846.

陈志刚： 男，1964 年生，博士，教授，主要研究方向为分布式计算、网络信息安全等.

梁涤青： 男，1979 年生，博士生，研究方向为混沌加密等.

邓小鸿： 男，1982 年生，博士，讲师，主要研究方向为数字水印、医学图像处理等.

张　颖： 男，1963 年生，博士，教授，主要研究方向为电能质量控制、电力系统数据通信等.