一个一维离散混沌判定定理及其在伪随机数发生器中的应用

臧鸿雁[①] 李 玖[①] 李国东*[②]

[①](北京科技大学数理学院 北京 100083)

[②](新疆财经大学应用数学学院 乌鲁木齐 830012)

摘 要：该文研究了一类取模运算的1维离散动力系统，提出了一个这类离散映射的混沌判据，利用Marotto定理证明了其混沌的存在性。给出了几个满足该判据的特殊形式的系统，分析了其分岔图、Lyapunov指数谱等基本动力学性质，通过模拟结果验证了理论的正确性。基于新系统设计了一个伪随机数发生器(PRNG)，SP800-22随机性检测结果表明了该序列具有良好的伪随机性。进一步给出了一个图像加密方案，其密钥空间可以达到2^{747}。该文提出的新系统的系统参数可以无穷多，所以理论上该加密方案的密钥空间可以无穷大。

关键词：混沌判据；Marotto定理；返回扩张不动点；伪随机数发生器；图像加密

中图分类号：O415.5; TP309.7 **文献标识码**：A **文章编号**：1009-5896(2018)08-1992-06

DOI: 10.11999/JEIT171139

A One-dimensional Discrete Map Chaos Criterion Theorem with Applications in Pseudo-random Number Generator

ZANG Hongyan[①] LI Jiu[①] LI Guodong[②]

[①](*Mathematics and Physics School*, *University of Science and Technology Beijing*, *Beijing* 100083, *China*)

[②](*College of Applied Mathematics*, *Xinjiang University of Finance and Economics*, *Urumchi* 830012, *China*)

Abstract: A novel one-dimensional discrete chaotic criterion is firstly constructed by studying the modular operation of the discrete dynamical systems. The judgement of the Marotto theorem is used to prove that the suggested dynamical systems are chaotic. Secondly, several special chaotic systems satisfied with the conditions of this paper are given, and the bifurcation diagram and Lyapunov exponential spectrum are also analyzed. Numerical simulations show that the proposed chaotic systems have the positive Lyapunov exponent, which indicates the accuracy of the proposed theory. Additionally, a Pseudo-Random Number Generator (PRNG) is also designed based on the given new chaotic system. Using SP800-22 test suit, the results show that the output sequence of PRNG has good pseudorandom. Finally, as an application of the PRNG, an image encryption algorithm is given. The proposed encryption scheme is highly secure Key space of 2^{747} and can resist against the statistical and exhaustive attacks based on the experimental results.

Key words: Chaotic criterion; Marotto theorem; Snap-back repeller; Pseudo-Random Number Generator (PRNG); Image encryption

1 引言

混沌作为非线性动力学中特有的一类复杂行为，广泛存在于自然界中，如物理学、生物学、社会学等各种领域。相比其他确定性动力系统，混沌具有许多复杂的动力行为，如轨道的长期不可预测性，良好的伪随机特性，对初始条件和系统参数的敏感性等。目前判定一个离散动力系统是否存在着混沌行为有一些常用的混沌判据，对1维离散映射的混沌判定，文献[1]提出了“周期三蕴含混沌”即周期三定理。文献[2]通过研究特定的2次多项式形式系统，提出了几类特殊的2次多项式混沌判定。文献[3]通过研究实系数多项式在复数域中的分解问题提出了一般2次多项式的混沌判定定理。文献[4]提出了一类特殊3次多项式混沌系统判定定理。高维离散映射的混沌判定有Marotto 混沌判定定理[5]等。在文献[6]提出的Chen-Lai算法中，通过考虑1维映射$x_{k+1}=f(x_k)+(N+e^c)x_k(\mathrm{mod}\,1)$，研究

收稿日期：2017-12-04；改回日期：2018-05-02；网络出版：2018-06-07

*通信作者： 李国东 lgdzhy@126.com

基金项目：国家自然科学基金(11461063)，新疆维吾尔自治区自然科学基金(2017D01A24)

Foundation Items: The National Natural Science Foundation of China (11461063), The Xinjiang Uygur Autonomous Region Natural Science Foundation (2017D01A24)

了系统在线性控制项“$(N+e^c)x_k$”的控制下的混沌问题。本文不考虑Chen-Lai算法的线性控制项，仅考虑$x_{k+1}=f(x_k)\,(\bmod 1)$这种结构形式，针对$|f'(x)|>1$的情况，提出了一个1维离散混沌映射的判定定理，并利用返回扩张不动点和Marotto 混沌判据证明了其在Li-Yorke数学意义[1]下混沌的存在性。

伪随机数广泛应用于物理系统模拟、计算机模拟、图像信息加密等领域，如今，伪随机数算法几乎取代了随机数表和基于硬件的伪随机数发生器(PRNG)。而混沌系统的轨道具有长期不可预测性、良好的伪随机特性，适于用来设计PRNG[7,8]。本文提出了几个1维离散混沌系统，并基于这些系统设计了一个伪随机数发生器，采用美国国家标准与技术研究院(NIST)提出的SP800-22检测标准[9]对其进行了随机性检测分析。

2　1 维离散混沌判定定理

以下给出动力系统中返回扩张不动点的定义和Marotto 定理。

定义1[5](返回扩张不动点) 记$B_r(x^*)$以点x^*为中心，半径为r的闭球，如果$\boldsymbol{R}^n$中的可微映射g的不动点x^*满足以下条件：(1)存在实数$r>0$，使得$B_r(x^*)$中任意一点x的雅可比矩阵$\boldsymbol{D}g(x)$的所有特征值的模大于1；(2)存在$B_r(x^*)$中的一个点$x^0\neq x^*$和自然数$m\geq 2$，使得$g^m(x^0)=x^*$，并且点x^0是非退化的，即满足$\det\{\boldsymbol{D}g^m(x^0)\}\neq 0$。则称不动点$x^*$是映射$g$的一个返回扩张不动点。

在返回扩张不动点的定义基础上，有定理1。

定理 1[5](Marotto 定理)　如果n维可微映射g: $\boldsymbol{R}^n\to\boldsymbol{R}^n$具有一个返回扩张不动点，映射$g$具有Li-Yorke意义下的混沌特性。

本文基于Marotto 定理提出了一个有关1维离散系统的混沌判定定理，见定理2。

定理 2　考虑离散动力系统

$$x_{k+1}=f(x_k)\,(\bmod 1) \tag{1}$$

式中，$x_k\in\boldsymbol{R}^1$, $f(x)\in\boldsymbol{C}^1[0,1]$，且$f(0)=0$，若对任意的$x\in[0,1)$, $|f'(x)|>1$恒成立。则动力系统式(1)在Li-Yorke意义下存在着混沌行为。

证明　因$f(0)=0$，得0为系统的不动点。又$f'(x)$为连续函数，且对任意的$x\in[0,1)$，有$|f'(x)|>1$成立，则$f'(x)>1$或$f'(x)<-1$恒成立。以下分两种情况证明0为返回扩张不动点。

先考虑$f'(x)>1$的情况：记$h_1(x)\triangleq f(x)-1$, $x\in[0,1]$，取$x_1=0$时，有

$$h_1(x_1)=f(0)-1=-1<0 \tag{2}$$

取$x_2=1$时，必有

$$h_1(x_2)=f(1)-1>0 \tag{3}$$

由式(2)，式(3)知，根据连续函数的介值性定理，$\exists z_1\in(0,1)$满足$h_1(z_1)=f(z_1)-1=0$，得$f(z_1)=1$，令

$$z_2\triangleq f(z_1)\,(\bmod 1)=0 \tag{4}$$

作辅助函数$h_2(x)\triangleq f(x)-z_1, x\in[0,1]$，

取$x_3=0$时，有

$$h_2(x_3)=f(0)-z_1=-z_1<0 \tag{5}$$

取$x_4=z_1$时，有

$$h_2(x_4)=f(z_1)-z_1=1-z_1>0 \tag{6}$$

由式(5)，式(6)知，$\exists z_0\in(0,z_1)$满足$h_1(z_0)=f(z_0)-z_1=0$，故

$$z_1=f(z_0)\ (\bmod 1) \tag{7}$$

由式(4)，式(7)可得，从z_0开始，当迭代两次后可以使得$z_2=0$。

令$x^*\triangleq 0$, $g(x)\triangleq f(x)\,(\bmod 1)$，那么$g^m(z_0)=x^*$，其中$m=2$且$g$的不动点$x^*$满足以下两个条件：

(1)取$r\in(z_0,z_1)$，满足$z_0\in B_r(x^*)$，由$(x)>f'1$对$\forall x\in[0,1)$都成立，故得$B_r(x^*)\cap[0,1)$中任意一点x的雅可比矩阵$\boldsymbol{D}g(x)=f'(x)$的所有特征值的模大于1；

(2)$B_r(x^*)$中的点$z_0\in(0,z_1)$和自然数$m=2$，使得$g^m(z_0)=x^*$，又易知$\det\{\boldsymbol{D}g^2(z_0)\}>1\neq 0$，故得$z_0$为非退化的。

综上，$x^*=0$在$f'(x)>1$时为一个返回扩张不动点。

再考虑$f'(x)<-1$的情况：记$h_3(x)\triangleq f(x)+1$, $x\in[0,1]$，取$x_5=0$时，有

$$h_3(x_5)=f(0)+1=1>0 \tag{8}$$

取$x_6=1$时，必有

$$h_3(x_6)=f(1)+1<0 \tag{9}$$

则由式(8)，式(9)，根据连续函数的介值性定理，$\exists w_1\in(0,1)$满足$h_3(w_1)=f(w_1)+1=0$，得$f(w_1)=-1$，令

$$w_2\triangleq f(w_1)\,(\bmod 1)=0 \tag{10}$$

作辅助函数$h_4(x)\triangleq f(x)+1-w_1, x\in[0,1]$，取$x_7=0$时，有

$$h_4(x_7)=f(0)+1-w_1=1-w_1>0 \tag{11}$$

取$x_8=w_1$时，有

$$h_4(x_8)=f(w_1)+1-w_1=-w_1<0 \tag{12}$$

同理，由式(11)，式(12)知，$\exists w_0\in(0,w_1)$满足$h_4(w_0)=f(w_0)+1-w_1=0$，故

$$w_1=f(w_0)\ (\bmod 1) \tag{13}$$

由式(10)，式(13)可得，从w_0开始，当迭代两次后可以使得$w_2=0$。

令$x^*\triangleq 0, g(x)\triangleq f(x)\,(\bmod 1)$，那么$g^m\left(x^0\right)=x^*$，其中$m=2$且$g$的不动点$x^*$满足以下两个条件：

(1)取$r\in(w_0,w_1)$，满足$w_0\in B_r(x^*)$，由$f'(x)<-1$对$\forall x\in[0,1)$都成立，故得$B_r(x^*)\cap[0,1)$中任意一点x的雅可比矩阵$\boldsymbol{D}g(x)=f'(x)$的所有特征值的模大于1；

(2)$B_r(x^*)$中的点$w_0\in(0,w_1)$和自然数$m=2$，使得$g^m(w_0)=x^*$，又知$\det\left\{\boldsymbol{D}g^2(w_0)\right\}>1\neq 0$，故知$w_0$为非退化的。

综上，$x^*=0$在$f'(x)<-1$时为一个返回扩张不动点。总之，$x^*=0$在$|f'(x)|>1$时为一个返回扩张不动点，即系统式(1)在Li-Yorke意义下存在着混沌。 定理2得证。

作为动力系统式(1)的特殊形式，本文进一步给出了满足定理2条件的混沌系统。

推论1 考虑如式(14)多项式形式系统：

$$x_{k+1}=a_nx_k^n+a_{n-1}x_k^{n-1}+\cdots+a_1x_k^1\,(\bmod 1)\quad(14)$$

式中，$x_k\in\boldsymbol{R}^1$，记$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x$，对任意的$x\in[0,1)$, $|f'(x)|>1$恒成立。在此定义下，动力系统式(14)在Li-Yorke意义下存在着混沌行为。

特别地 当$a_i\geq 0\,(i=2,3,\cdots,n;n\in N^+)$，$a_1>1$成立时，系统式(14)在Li-Yorke意义下存在着混沌行为。事实上，由$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x, x\in[0,1]$，则$f'(x)=na_nx^{n-1}+\cdots+a_1\geq a_1>1$。由推论1知，在该条件下系统式(14)在Li-Yorke意义下存在混沌行为。

3 实验模拟仿真

在定理2中，令系统式(1)中函数$f(x)$的形式为$f(x)=\dfrac{1}{2}x^2-2a\ln(1+x), x\in[0,1]$，则系统式(1)变成如式(15)形式：

$$x_{k+1}=\left(\frac{1}{2}x_k^2-2a\ln(1+x_k)\right)(\bmod 1), x_k\in[0,1]\quad(15)$$

其中，a为系统参数。利用定理2得$|f'(x)|=\left|x-\dfrac{2a}{1+x}\right|>1$。即$a>2$或$a<-0.5$时，系统式(15)呈现出混沌特性。

选取初始条件$x_0=0.0385$。图1给出了系统式(15)随参数a变化的分岔图。图2给出了系统式(15)随参数a变化的Lyapunov指数图。

由图1可知，当参数$a>1$或$a<0$时，迭代的取值几乎平均地分布于整个$[0,1]$值域；图2的模拟结果显示参数为$a>2$或$a<-0.5$时，其Lyapunov指数为正值；表明了此时系统式(15)在该条件下呈现出混沌特性。

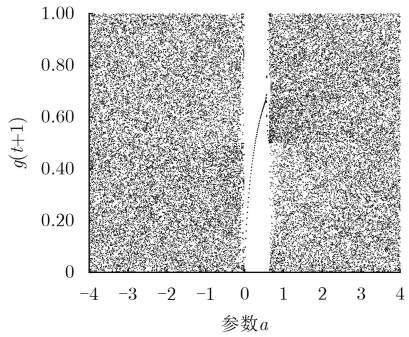


图 1 系统式(15)的分岔图

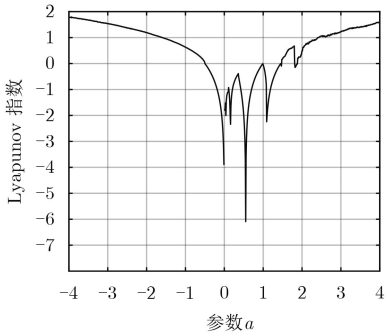


图 2 系统式(15)的Lyapunov指数谱

在推论1中，考虑系统式(14)中函数$f(x)$的形式为$f(x)=x^3+3ax^2+ax, x\in[0,1]$，则系统式(14)变成式(16)形式：

$$x_{k+1}=x_k^3+3ax_k^2+ax_k\,(\bmod 1), x_k\in[0,1]\quad(16)$$

其中，a为系统参数。利用推论1得$|f'(x)|=\left|3x^2+6ax+a\right|>1$。因此，当参数$a>1$或$a<-\dfrac{4}{7}$且$a\neq -1$时，系统呈现混沌特性。

图3和图4分别给出了在给定初值$x_0=0.0385$下系统式(16)随系统参数a变化的分岔图和Lyapunov指数谱。

由图3可见，当参数$a>1$或$a<-0.6$时，迭代的取值几乎取遍了$[0,1]$值域；图4显示当参数$a>1$或$a<-0.6$时，其Lyapunov指数为正值；表明了在该条件下系统式(16)呈现出混沌特性。

4 伪随机数发生器及随机性分析

4.1 基于新离散混沌系统的伪随机数发生器

为设计一个新的伪随机数发生器(PRNG)，本文依据系统式(14)的结构形式提出了3个1维离散混沌系统，构成式(17)所示的3维系统，设其动力系统的数学表达式为

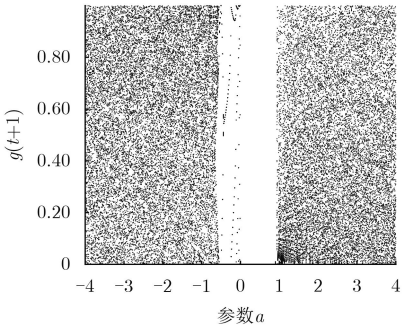


图 3 系统式(16)的分岔图

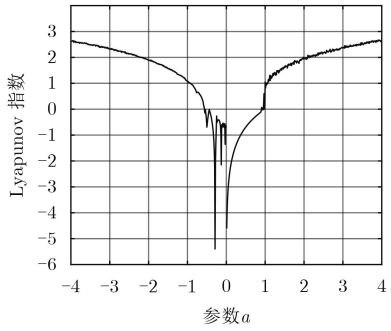


图 4 系统式(16)的Lyapunov指数谱

$$\left.\begin{aligned} y_1(k+1) &= a_4 y_1(k)^4 + a_3 y_1(k)^3 + a_2 y_1(k)^2 \\ &\quad + a_1 y_1(k) \ (\mathrm{mod}\ 1) \\ y_2(k+1) &= b_4 y_2(k)^4 + b_3 y_2(k)^3 + b_2 y_2(k)^2 \\ &\quad + b_1 y_2(k) \ (\mathrm{mod}\ 1) \\ y_3(k+1) &= c_4 y_3(k)^4 + c_3 y_3(k)^3 + c_2 y_3(k)^2 \\ &\quad + c_1 y_3(k) \ (\mathrm{mod}\ 1) \end{aligned}\right\} \quad (17)$$

其中， $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4, c_1, c_2, c_3, c_4$均为系统参数。

据推论1知，当系统参数取如下值：

$$a_1 = 1.115, a_2 = 1.195, a_3 = 0.500, a_4 = 0.210$$
$$b_1 = 1.359, b_2 = 5.995, b_3 = 0.285, b_4 = 0.400$$
$$c_1 = 2.250, c_2 = 0.130, c_3 = 0.200, c_4 = 0.256$$

初始条件为

$$\boldsymbol{y}_1(1) = 0.387, \boldsymbol{y}_2(1) = 0.778, \boldsymbol{y}_3(1) = 0.395$$

时系统式(17)产生混沌轨迹。

令 $\boldsymbol{Y} = \boldsymbol{y}_1 + \boldsymbol{y}_2 + \boldsymbol{y}_3$，首先定义变换 T_1[10]：

$$\boldsymbol{Z}(k) = T_1(\boldsymbol{Y}(k)) = \mathrm{mod}\left(\mathrm{round}\left(\frac{L(\boldsymbol{Y}(k) - \min(\boldsymbol{Y}))}{\max(\boldsymbol{Y}) - \min(\boldsymbol{Y})}\right), 256\right) \quad (18)$$

其中，$\min(\boldsymbol{Y}) = \min|\boldsymbol{Y}(k)|, \max(\boldsymbol{Y}) = \max \boldsymbol{Y}|(k)|$, $k = 1, 2, \cdots, n$ ， L 为一个比较大的实数。则 $\boldsymbol{Z}(k) \in \{0, 1, 2, \cdots, 255\}$ 。

再定义变换 T_2：

$$\tilde{\boldsymbol{Z}} = T_2(\boldsymbol{Z}) \quad (19)$$

该变换将 $\boldsymbol{Z}$ 变换成相应的二进制数，得到0, 1序列。 即得到对应的PRNG。

4.2 随机性检验

本文采用NIST在FIPS标准的基础上建立的SP800-22检测标准[9]对设计的PRNG进行随机性测试。该检测一共包括16项随机性检测，式(18)中选取 $L = 2.55 \times 10^{12}$，对式(19)的生成序列进行SP800-22检测，检测见表1第2列第3列，由第3列可知所有的检测项都通过。对参数扰动进行100次检测见表1第4列第5列，其通过率见第5列。

表 1　SP800-22随机性检验结果

检测项目	给定初始值		参数扰动100次	
	P-值	检测结果	拟合优度P-值	通过率
频率测试	0.1493	通过	0.8978	0.97
块内频率测试	0.6436	通过	0.3041	0.99
向前累积和测试	0.2777	通过	0.3191	0.97
向后累积和测试	0.1971	通过	0.8832	0.98
游程测试	0.3875	通过	0.1453	0.97
块内最长连续1测试	0.5564	通过	0.4559	1.00
二元矩阵秩测试	0.0523	通过	0.9463	1.00
离散傅里叶变换测试	0.1445	通过	0.4373	0.99
非重叠模板匹配测试	0.5761	通过	0.7598	0.99
重叠模板匹配测试	0.2961	通过	0.1719	0.98
全局通用统计测试	0.2253	通过	0.9963	0.99
近似熵检测	0.5118	通过	0.6579	1.00
随机偏移测试	0.0246	通过	0.7598	1.00
随机偏移变量测试	0.5542	通过	0.0072	0.98
线性复杂度测试	0.4339	通过	0.2023	0.99
串行测试	0.9780	通过	0.4190	0.98

表1的随机性检验结果表明，基于本文提出的混沌系统设计的伪随机数发生器产生的随机序列具有良好的伪随机性。

5　图像加密方案及安全性分析

5.1 图像加解密算法描述

以下基于PRNG式(19)设计了一个图像加密方案。

图像加密算法为：假设甲方需要通过Internet向乙方发送一幅 $m \times n$ 的彩色图像，其中 m 和 n 分别表示图像像素的行数和列数，像素值为[0, 255]之间的整数，表示像素的灰度值。甲、乙双方共享系统式(17)和密钥集

$$\mathrm{keys} = \{a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4, c_1, c_2, c_3, c_4, \boldsymbol{y}_1(1), \boldsymbol{y}_2(1), \boldsymbol{y}_3(1)\} \quad (20)$$

(1)利用系统式(17)和密钥集式(20)生成混沌序

列$\{\boldsymbol{y}_1(k),\boldsymbol{y}_2(k),\boldsymbol{y}_3(k)|k=1,2,\cdots,m\times n\}$；

(2)甲方生成加密序列。由于像素值为0 ~255之间的整数，为加强密文中加密序列的作用以及数据范围的需要需利用变换T_1对混沌序列作如式(21)处理(L为一个比较大的实数)：

$$\boldsymbol{z}=\bmod\left(\mathrm{round}\left(L\left(\boldsymbol{y}_1+\boldsymbol{y}_2+\boldsymbol{y}_3\right)\right),256\right) \tag{21}$$

(3)甲方从生成的序列$\boldsymbol{z}$中分别选出$m\times n\times 3$个数，并将其重新排成$m\times n$的矩阵得到矩阵$\boldsymbol{t}_1,\boldsymbol{t}_2,\boldsymbol{t}_3$；

(4)读取彩色图像，$\boldsymbol{M}_1,\boldsymbol{M}_2,\boldsymbol{M}_3$分别代表图像的红绿蓝3层。甲方取生成的$\boldsymbol{t}_1,\boldsymbol{t}_2,\boldsymbol{t}_3$对原始图像的像素值进行加密得到密文($i=1,2,3$)：

$$\boldsymbol{C}_i=\bmod\left(\mathrm{round}\left(\boldsymbol{M}_i+\boldsymbol{t}_i\right),256\right) \tag{22}$$

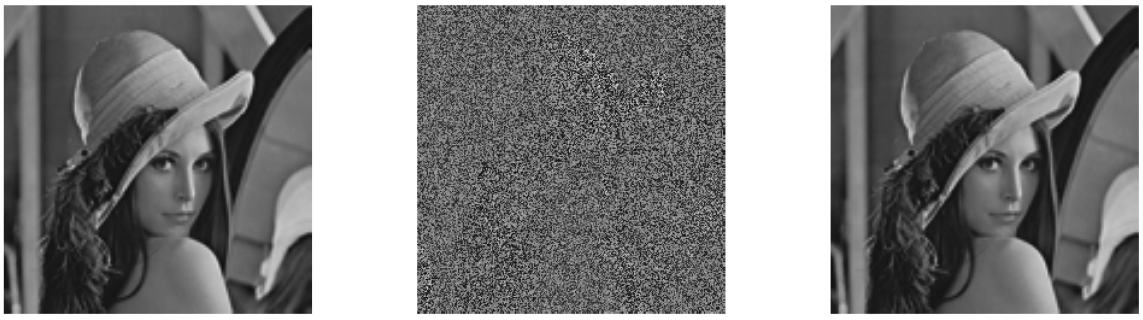
(5)最后乙方利用密钥按照步骤(3)和步骤(4)逆向求解出明文图像。

5.2 加密实验及密钥空间

明文是256 × 256的Lena图像，如图5(a)所示。密钥集式(20)选择为

keys={1.115, 1.195, 0.500, 0.210, 1.359, 5.995, 0.285, 0.400, 2.250, 0.130, 0.200, 0.256, 0.387, 0.778, 0.395}

对明文按照上述图像加解密算法进行加解密，效果如图5(b)，图5(c)所示。



(a) 原始图像　(b) 加密图像　(c) 正确密钥解密图像

图 5 图像的加解密效果图

本文设计的加密方案对系统中所有参数的敏感度均达到了10^{-15}以上，即任何大于10^{-15}的参数扰动均不能正确地解密出原始图像。本文算法对密钥有极强的敏感性。

为了能够有效抵抗穷举攻击等密码攻击，理想的加密方案应尽可能使得密钥空间足够大。在混沌序列的产生过程中，该加密方案的密钥主要取决于混沌系统的系统参数和初始条件，通过对密钥敏感性测试表明了本文的密钥空间为$10^{15\times(12+3)}=10^{225}>2^{747}$。对比文献[11]，文献[12]，文献[13]，文献[14]和文献[15]密钥空间结果见表2。

表 2 密钥空间对比表

	本文	文献[11]	文献[12]	文献[13]	文献[14]	文献[15]
密钥空间	2^{747}	2^{640}	2^{273}	2^{270}	2^{267}	2^{208}

6 结论

本文基于Marotto 混沌判定定理，研究了一类基于取模运算的1维离散动力系统，提出了一个有关1维离散动力系统的混沌判据(定理2)；在此基础上进一步研究了原始函数为一般多项式形式的离散动力系统，给出了推论1；针对几个满足本文混沌判据的离散动力系统进行了数值模拟，模拟结果验证了本文提出的理论的正确性。

根据推论1，本文构造了3个1维离散混沌系统并设计了一个伪随机数发生器(PRNG)，并进行了SP800-22的随机性检验，检验结果显示本文设计的伪随机数发生器具有良好的伪随机性。在此基础上给出了一个图像加密实例，并对该算法进行了安全性分析。本文采用的混沌系统参数较多，密钥空间高达2^{747}；该加密方案对密钥十分敏感，任何超过10^{-15}的密钥扰动都会使解密失效，实验分析均表明本文所设计的图像加密方案具有较高的安全性。

基于本文构造的系统式(14)，理论上可以构造出具有无穷多参数的混沌系统，为进一步设计密钥空间大的加密方案提供了良好的伪随机源。

参 考 文 献

[1] LI T Y and YORKE J A. Period three implies chaos[J]. *American Mathematical Monthly*, 1975, 82(10): 985–992. doi: 10.2307/2318254.

[2] YU Xingmei, MIN Lequan, and CHEN Tianyu. Chaos criterion on some quadric polynomial maps and design for chaotic pseudorandom number generator[C]. Seventh International Conference on Natural Computation,

Shanghai, 2011: 1373–1376.

[3] 周海玲, 宋恩彬. 二次多项式映射的3-周期点判定[J]. 四川大学学报(自然科学版), 2009, 46(3): 561–564. doi: 103969/j.issn.0490-6756.2009.03-009.

ZHOU Hailing and SONG Enbin. Discrimination of the 3-periodic points of a quadratic polynomial[J]. *Journal of Sichuan University*(*Natural Science Edition*), 2009, 46(3): 561–564. doi: 103969/j.issn.0490-6756.2009.03-009.

[4] YANG Xiuping, MIN Lequan, and WANG Xue. A cubic map chaos criterion theorem with applications in generalized synchronization based pseudorandom number generator and image encryption[J]. *Chaos*, 2015, 25(5): 053104. doi: 10.1063/1.4917380.

[5] MAROTTO F R. Snap-back repellers imply chaos in R^n[J]. *Journal of Mathematical Analysis and Applications*, 1978, 63: 199–223. doi: 10.1016/0022-247X(78)90115-4.

[6] CHEN Guangrong and LAI Dejian. Feedback control of lyapunov exponents for discrete-time dynamical systems[J]. *International Journal of Bifurcation & Chaos*, 1996, 6(7): 1341–1349. doi: 10.1142/S021812749600076X.

[7] HAN Dandan, MIN Lequan, and CHEN Guangrong. A stream encryption scheme with both key and plaintext avalanche effects for designing chaos-based pseudorandom number generator with application to image encryption[J]. *International Journal Bifurcation & Chaos*, 2016, 26(5): 1650091-1. doi: 10.1142/S0218127416500917.

[8] 韩丹丹, 闵乐泉, 赵耿. 八维广义同步系统在伪随机数发生器中的应用[J]. 电子与信息学报, 2016, 38(5): 1158–1165. doi: 10.11999/JEIT150899.

HAN Dandan, MIN Lequan, and ZHAO Geng. Application of 8-dimensional generalized synchronization system in pseudorandom number generator[J]. *Journal of Electronics & Information Technology*, 2016, 38(5): 1158–1165. doi: 10.11999/JEIT150899.

[9] RUKHIN A, SOTO J, NECHVATAL J, *et al*. A statistical test suite for random and pseudorandom number generators for cryptographic applications[R]. National Institute of Standards and Technology Special Publication, 2010.

[10] LI Pei, MIN Lequan, ZANG Hongyan, *et al*. A generalized chaos synchronization-based pseudo-random generator number and performance analysis[C]. International Conference on Communications Circuits and Systems, Chengdu, China, 2010: 781–785.

[11] WANG Xingyuan, LIU Chuanming, XU Dahai, *et al*. Image encryption scheme using chaos and simulated annealing algorithm[J]. *Nonlinear Dynamics*, 2016, 84(3): 1417–1429. doi: 10.1007/s11071-015-2579-y.

[12] LI Yueping, WANG Chunhua, and CHEN Hua. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation[J]. *Optics & Lasers in Engineering*, 2017, 90: 238–246. doi: 10.1016/j.optlaseng.2016.10.020.

[13] WANG Xingyuan, LIU Chuanming, and ZHANG Huili. An effective and fast image encryption algorithm based on chaos and interweaving of ranks[J]. *Nonlinear Dynamics*, 2016, 84(3): 1595–1607. doi: 10.1007/s11071-015-2590-3.

[14] GUESMI R, FARAH M A B, KACHOURI A, *et al*. A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2[J]. *Nonlinear Dynamics*, 2016, 83(3): 1123–1136. doi: 10.1007/s11071-015-2392-7.

[15] BELAZI A, EL-LATIF A A A, DIACONU A V, *et al*. Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms[J]. *Optics & Lasers in Engineering*, 2017, 88: 37–50. doi: 10.1016/j.optlaseng.2016.07.010.

臧鸿雁：女，1973年生，副教授，研究方向为混沌系统理论及混沌密码学.

李　玖：男，1995年生，硕士生，研究方向为混沌系统理论及图像加密.

李国东：男，1972年生，教授，研究方向为细胞神经网络和混沌密码学.