Computer Science and Application 计算机科学与应用, 2018, 8(11), 1713-1719
Published Online November 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.811189

Hans汉斯

Design of a Stream Cipher Algorithm Based on Time-Varying Symbolic Chaotic Dynamical Systems

Chuanjun Tian*, Jing Lin, Quan Zeng, Xinglin Li

College of Information Engineering, Shenzhen University, Shenzhen Guangdong
Email: *tiancj@szu.edu.cn

Received: Oct. 31st, 2018; accepted: Nov. 12th, 2018; published: Nov. 19th, 2018

Abstract

This paper studies chaos of a class of two-dimensional time-varying generalized symbolic systems, gives a construction example of a special time-varying generalized symbolic chaotic system, and analyses the pseudo-randomicity of solutions of this system. At the same time, based on this system and m sequences, this paper designs a stream cipher algorithm and simulates its encryption effect in digital image. Simulation shows that the designed algorithm has good encryption effects.

Keywords

Two-Dimensional Discrete System, Generalized Symbolic System, Devaney Chaos, Stream Cipher Algorithm

基于二维时变符号混沌系统的流密码算法设计

田传俊*，林　敬，曾　泉，黎杏玲

深圳大学信息工程学院，广东　深圳
Email: *tiancj@szu.edu.cn

收稿日期：2018年10月31日；录用日期：2018年11月12日；发布日期：2018年11月19日

摘　要

本文研究了一类二维时变广义符号动力系统的混沌性，给出了一种特殊混沌系统的构造实例，并对其混沌解序列进行了一些常见的伪随机性能分析。同时，结合m序列和该系统，设计了一种流密码算法，并对该

*通讯作者。

文章引用: 田传俊, 林敬, 曾泉, 黎杏玲. 基于二维时变符号混沌系统的流密码算法设计[J]. 计算机科学与应用, 2018, 8(11): 1713-1719. DOI: 10.12677/csa.2018.811189

算法在数字图像上的加密效果进行了仿真。仿真实验说明了所设计的序列密码算法具有良好的加密效果。

关键词

二维离散系统，广义符号动力系统，Devaney混沌性，流密码算法

1. 引言

普遍认为，密码算法是信息安全领域的重要基础之一，其中，流密码算法是一种常见的密码算法。流密码算法研究的一个关键问题是密钥流序列产生器的设计，通常可用离散系统来产生。当前，混沌流密码算法是流密码算法研究的热点问题之一，其中的关键问题是如何利用离散混沌系统来产生算法中的密钥流序列。本文将先在理论上研究一类新的特殊时变广义符号混沌系统，之后再研究利用这类新系统来设计新的密钥流序列产生器的问题。由于广义符号系统比移位寄存器系统更加广泛，并且能在计算机上准确计算与实现，因此，它们在流密码算法中的应用研究是有理论和实际意义的。

作为特殊离散系统的时变广义符号混沌系统及其在构造伪随机序列方面的应用是一个研究较少的热点问题[1] [2] [3] [4] [5]。因此，本文将讨论如下一种新的二维时变广义符号系统的相关问题：

$$\begin{cases} x_{m+1,n} = f\left(m, x_{m,n}, y_{m,n}, x_{m,n+1}\right) \\ y_{m+1,n} = g\left(m, y_{m,n}, x_{m,n}, y_{m,n+1}\right) \end{cases} \tag{1}$$

其中，$m,n \in N_0 = \{0,1,2,\cdots\}$，$I$ 是实数集 R 的一个有界子集，k 是一个正整数，$f: N_0 \times I^3 \to I$ 和 $g: N_0 \times I^3 \to I$ 是两个多元函数，并将 (f,g) 称为系统(1)的系统函数或生成函数。

设 $Z = \{\cdots,-1,0,1,\cdots\}$ 和 $N_t = \{t, t+1,\cdots\}$，$t \in Z$。记 $\Omega = \{(0,n) \mid n \in N_0\}$，则对任意定义在 Ω 上的序列 $\phi = \{\phi_{0,n}\}$ 和 $\varphi = \{\varphi_{0,n}\}$，一定存在二维离散时空序列 $(x,y) = \{(x_{m,n}, y_{m,n})\}_{m,n=0}^{\infty}$ 满足(1)，且 $x_{m,n} = \phi_{m,n}$ 和 $y_{m,n} = \varphi_{m,n}$，对任意 $(m,n) \in \Omega$。称 (x,y) 为系统(1)初值为 (ϕ,φ) 的一个解。参照文献[5]，当 $I = Z_q = \{0,1,\cdots,q-1\}$ 和 $q \in N_2$ 时，可将系统(1)称为(二维时变)(广义)符号动力系统。现有文献对时变符号系统研究很少，系统(1)的混沌性还没有文献研究过。

设 $x = \{(x_{m,n}, y_{m,n})\}_{m,n=0}^{\infty}$ 是系统(1)的一个解，其中，$x_{0,n}, y_{0,n} \in I$，$n \in N_0$。记

$$x_m = \{(x_{m,n}, y_{m,n})\}_{n=0}^{\infty},\ m \in N_0, \tag{2}$$

对于任一有界子集 $I \subseteq R = (-\infty,\infty)$，设

$$I_2^{\infty} = \left\{ \{(a_n,b_n)^{\mathrm{T}}\}_{n=0}^{\infty} = \begin{pmatrix} a_0 & a_1 & \cdots & a_n & \cdots \\ b_0 & b_1 & \cdots & b_n & \cdots \end{pmatrix} \middle| a_i, b_i \in I, i = 0,1,\cdots \right\}. \tag{3}$$

参照文献[3] [5]，可在 I_2^{∞} 上定义如下的一种常见形式的度量 $d: I_2^{\infty} \times I_2^{\infty} \to R^+ = [0,\infty)$：

$$d(x,y) = \sum_{n=0}^{\infty} \frac{|x_{1,n} - y_{1,n}| + |x_{2,n} - y_{2,n}|}{2^n}, \tag{4}$$

对任意 $x=\left\{\left(x_{1,n},x_{2,n}\right)^{\mathrm{T}}\right\}_{n=0}^{\infty}, y=\left\{\left(y_{1,n},y_{2,n}\right)^{\mathrm{T}}\right\}_{n=0}^{\infty}\in I_2^{\infty}$，其中，T 表示转置，可省略不写。

对任意 $m=0,1,2,\cdots$，由式(2)，不难发现可将系统(1)等价地改写为无穷维离散系统：

$$x_{m+1}=\left\{\left(f\left(m,x_{m,n},y_{m,n},x_{m,n+1}\right),g\left(m,y_{m,n},x_{m,n},y_{m,n+1}\right)\right)^{\mathrm{T}}\right\}_{n=0}^{\infty}=g_{m+1}\left(x_m\right),\tag{5}$$

其中，$g_1,g_2,\cdots$ 是由 (f,g) 决定的 I_2^{∞} 上的一列映射。为了方便，对任意 $x\in I_2^{\infty}$ 和 $n\in N_1$，记

$$G_n\left(x\right)=g_n\left(g_{n-1}\left(\cdots\left(g_1\left(x\right)\right)\cdots\right)\right)=g_n\circ\cdots\circ g_2\circ g_1\left(x\right),\ G_0\left(x\right)=x.\tag{6}$$

下面介绍一列映射混沌性的相关概念，可参见文献[2] [3] [4] [5]。

定义 1：对于度量空间 $\left(I_2^{\infty},d\right)$ 上的一列映射 $g_1,g_2,\cdots$ 和任意一点 $x_0\in X$，如果 $G=\left\{g_n\right\}_{n=1}^{\infty}$ 的轨道 $O\left(x_0\right)=\left\{x_n\right\}_{n=0}^{\infty}$ 是周期为 p 的周期序列，其中，$x_{n+1}=g_{n+1}\left(x_n\right)$，$n=0,1,2,\cdots$，则称 x_0 为 G 或系统(5)周期为 p 的周期点。如果 G 的所有周期点组成的集合是 X 中的稠密子集，则称 G 或 G 所决定的系统(5)具有周期点的稠密性。

同时，如果任意两个非空开子集 $U,V\subseteq I_2^{\infty}$，存在整数 $n>0$，使得 $G_n\left(U\right)\bigcap V$ 非空，则称 G 或系统(5)具有(拓扑)传递性。另外，如果存在 $\delta>0$，使得对任一 $x\in X$ 和 x 的邻域 U，存在 $y\in U$ 和整数 $n>1$，使得 $d\left(G_n\left(x\right),G_n\left(y\right)\right)>\delta$，则称 G 或 G 决定的系统(5)具有初值敏感依赖性。

定义 2：对于度量空间 $\left(I_2^{\infty},d\right)$ 上的一列映射 $g_1,g_2,\cdots$，如果 $G=\left\{g_n\right\}_{n=1}^{\infty}$ 或 G 决定的系统(5)具有传递性、周期点的稠密性和初值敏感依赖性，则称 $G=\left\{g_n\right\}_{n=1}^{\infty}$ 或系统(5)是 Devaney 混沌的，也称与系统(5)等价的相应系统(1)在 $\left(I_2^{\infty},d\right)$ 上是 Devaney 混沌的。

2. 一类二维时变广义符号混沌系统

下面将通过例子来说明如何去构造具体的时变广义符号混沌系统。

设 $I=Z_q=\left\{0,1,\cdots,q-1\right\}$，$q=2,3,\cdots$，$f:N_0\times I^3\to I$ 和 $g:N_0\times I^3\to I$ 定义如下：

$$f\left(m,x_0,y_0,x_1\right)=a_{0,m}x_0+a_{1,m}y_0+ax_1\bmod q=a_{0,m}x_0\oplus a_{1,m}y_0\oplus ax_1,\tag{7}$$

$$g\left(m,y_0,x_0,y_1\right)=b_{0,m}y_0\oplus b_{1,m}x_0\oplus by_1,\ x_0,x_1,y_0,y_1\in I\text{ 和 }m\in N_0,\tag{8}$$

其中，$\left\{a_{i,m}\right\}_{m=0}^{\infty}$ 和 $\left\{b_{i,m}\right\}_{m=0}^{\infty}$ 是两个周期非负整数列，即存在整数 $p>0$，使得对任一 $i=0,1$ 和 $m\in N_0$，有 $a_{i,m}=a_{i,m+p}$ 和 $b_{i,m}=b_{i,m+p}$，a 和 b 是两个正整数，且 a 与 q 互素，以及 b 与 q 互素。

显然，利用式(7)和(8)所定义的函数 f 和 g 可以生成如下二维时变广义符号动力系统

$$\begin{cases}x_{m+1,n}=f\left(m,x_{m,n},y_{m,n},x_{m,n+1}\right)=a_{0,m}x_{m,n}\oplus a_{1,m}y_{m,n}\oplus ax_{m,n+1}\\ y_{m+1,n}=g\left(m,y_{m,n},x_{m,n},y_{m,n+1}\right)=b_{0,m}y_{m,n}\oplus b_{1,m}x_{m,n}\oplus by_{m,n+1}\end{cases}\tag{9}$$

其中，$x_{m,n},y_{m,n}\in Z_q$，对任意 $m,n\in N_0$。下面将系统(9)所等价的无穷维离散系统设为

$$x_{m+1}=g_{m+1}\left(x_m\right),\ x_0\in I_2^{\infty},\ x_m=\left\{\left(x_{m,n},y_{m,n}\right)\right\}_{n=0}^{\infty},\ m\in N_0,\tag{10}$$

其中，$g_{m+1}:I_2^{\infty}\to I_2^{\infty}$ 是由 f 和 g 所导出的唯一映射，即对任意 $\alpha=\left\{\left(u_n,v_n\right)\right\}_{n=0}^{\infty}\in I_2^{\infty}$，有

$$g_{m+1}\left(\alpha\right)=\left\{\left(a_{0,m}u_n\oplus a_{1,m}v_n\oplus au_{n+1},b_{0,m}v_n\oplus b_{1,m}u_n\oplus bv_{n+1}\right)\right\}_{n=0}^{\infty}.\tag{11}$$

参照文献[6] [7]，并利用已知条件，容易证明如下的两个引理及其推论，其证明过程省略。

引理 1：式(10)所定义的 $G=\{g_n\}_{n=1}^{\infty}$ 是周期为 p 的一列映射，即 $G_m=G_{m+p}$， $m\in N_1$。

推论 1：设 $G=\{g_n\}_{n=1}^{\infty}$ 是由式(10)所确定的一列映射，则对一切 $m,s,t\in N_1$，都有

$$g_{s+mp-1}\circ g_{s+mp-2}\circ\cdots\circ g_s=g_{t+mp-1}\circ g_{t+mp-2}\circ\cdots\circ g_t. \tag{12}$$

引理 2：对任一 $u\in\{a,b\}$、正整数 m 和 $r,v\in Z_q$，一定存在 $s\in Z_q$，使得 $r\oplus u^m s=v$。

定理 1：时变广义符号系统(9)在度量空间 $\left(I_2^{\infty},d\right)$ 上是 Devaney 混沌的，其中， $I=Z_q$。

证明：由定义 2，显然只需要证明系统(10)是 $\left(I_2^{\infty},d\right)$ 上的 Devaney 混沌系统就行了。

首先，将证明系统(10)在 $\left(I_2^{\infty},d\right)$ 上具有传递性。

对任意两个非空开子集 $U,V\subseteq I_2^{\infty}$，以及对任一 $\alpha=\{(s_n,t_n)\}_{n=0}^{\infty}\in U$ 和 $\beta=\{(u_n,v_n)\}_{n=0}^{\infty}\in V$，存在 $\theta>0$，使得 $B_\theta(\alpha)=\left\{x=\{(x_n,y_n)\}_{n=0}^{\infty}\in I_2^{\infty}\mid d(x,\alpha)<\theta\right\}\subseteq U$ 和 $B_\theta(\beta)\subseteq V$。因此，根据式(4)所定义的度量 d 的性质可知，存在一个正整数 M，使得

$$\left\{x=\{(x_{1,n},y_{1,n})\}_{n=0}^{\infty}\mid x_{1,i}=s_i,y_{1,i}=t_i,i\in Z_M;x_{1,j},y_{1,j}\in I,j\notin Z_M\right\}\subseteq B_\theta(\alpha),$$

$$\left\{y=\{(x_{2,n},y_{2,n})\}_{n=0}^{\infty}\mid x_{2,i}=u_i,y_{2,i}=v_i,i\in Z_M;x_{2,j},y_{2,j}\in I,j\notin Z_M\right\}\subseteq B_\theta(\beta). \tag{13}$$

对任意一点 $x=\{(x_n,y_n)\}_{n=0}^{\infty}\in I_2^{\infty}$，记

$$G_1(x)=\{(a_{0,0}x_n\oplus a_{1,0}y_n\oplus ax_{n+1},b_{0,0}y_n\oplus b_{1,0}x_n\oplus by_{n+1})\}_{n=0}^{\infty}=\{x_n^{(1)}\}_{n=0}^{\infty}=x^{(1)},$$

其中， $x^{(1)}=\{x_n^{(1)}=(f_0(x_n,y_n)\oplus ax_{n+1},h_0(x_n,y_n)\oplus by_{n+1})\}_{n=0}^{\infty}$，且函数 $f_0:I^2\to I$ 和 $h_0:I^2\to I$ 满足 $f_0(x_n,y_n)=a_{0,0}x_n\oplus a_{1,0}y_n$ 和 $h_0(x_n,y_n)=b_{0,0}y_n\oplus b_{1,0}x_n$。

一般地，利用递推法，对任意 $m=1,2,\cdots$ 和 $x=\{(x_n,y_n)\}_{n=0}^{\infty}\in I_2^{\infty}$，都有

$$G_m(x)=g_m\left(x^{(m-1)}\right)=g_m\left(\cdots(g_1(x)\cdots)\right)=\{x_n^{(m)}\}_{n=0}^{\infty}=x^{(m)},\ x^{(0)}=x,$$

其中， G_m 由式(6)定义，且

$$x^{(m)}=\{x_n^{(m)}=(f_{m-1}(x_n,\cdots,y_{n+m-1})\oplus a^m x_{n+m},h_{m-1}(x_n,\cdots,y_{n+m-1})\oplus b^m y_{n+m})\}_{n=0}^{\infty}, \tag{14}$$

$f_m:I^{2(m+1)}\to I$ 和 $h_m:I^{2(m+1)}\to I$ 是按递推方式由 G 唯一决定的两列函数，对任意 $m,n\in N_0$。

由引理 2 可知，对任一整数 $m\in N_1$ 和 $c\in I$，都存在 $r,h\in I$，使得

$$f_{m-1}(x_n,\cdots,y_{n+m-1})\oplus a^m r=c,\ \ h_{m-1}(x_n,\cdots,y_{n+m-1})\oplus b^m h=c. \tag{15}$$

对于 $\alpha=\{(s_n,t_n)\}_{n=0}^{\infty}\in U$ 和 $\beta=\{(u_n,v_n)\}_{n=0}^{\infty}\in V$，由式(13)，(14)和(15)，可找到一点 $\eta=\{(r_n,k_n)\}_{n=0}^{\infty}\in I_2^{\infty}$，满足 $r_n=s_n$ 和 $k_n=t_n$，对 $n=0,1,\cdots,M-1$，且依次可选取的 $r_M,r_{M+1},\cdots$ 和 $k_M,k_{M+1},\cdots$，使得如下等式成立：

$$f_{M-1}(r_n,\cdots,k_{n+M-1})\oplus a^M r_{n+M}=u_n,\ \ h_{M-1}(r_n,\cdots,k_{n+M-1})\oplus b^M k_{n+M}=v_n,\ \ n=0,1,2,\cdots.$$

因此， $G_M(\eta)=\beta\in V$ 和 $\eta\in U$。这样，系统(10)在 $\left(I_2^{\infty},d\right)$ 上具有传递性。

其次，利用与上面传递性的相似证明方法，不仅可证明系统(10)具有周期点的稠密性，而且也能证明系统(10)具有初值敏感依赖性。由于证明过程是类似的，因此，省略它们的证明过程。这样，综合上面的证明过程可知，系统(10)在 $\left(I_2^{\infty},d\right)$ 上是 Devaney 混沌的。证毕。

例 1：考虑如下时变离散时空系统

$$x_{m+1,n}=a_{0,m}x_{m,n}\oplus a_{1,m}y_{m,n}\oplus x_{m,n+1},\quad y_{m+1,n}=b_{0,m}y_{m,n}\oplus b_{1,m}x_{m,n}\oplus 3y_{m,n+1}, \tag{16}$$

其中，$x_{0,n}\in I=\{0,1\}$，$q=2$，$a_{0,m}=2+(-1)^m$ 和 $a_{1,m}=(3m)\bmod(2)$，$b_{0,m}=2+(-1)^{m+1}$，$b_{1,m}=(m+1)\bmod(2)$，对任意 $m,n\in N_0$，$\oplus$ 和 $\bmod(2)$ 表示模 2 加法运算。

由于系统(16)是时变广义符号系统，因此，现有的判断方法不能判断系统(16)是否具有 Devaney 混沌性。但是，由于 $\{a_{i,n}\}_{n=0}^{\infty}$ 和 $\{b_{i,n}\}_{n=0}^{\infty}$ 都是周期数列，对任一 $i=0,1$，且 2 与 1、2 和 3 都是互素的，因此，由定理 1 可知，系统(16)在 (I_2^{∞},d) 上是 Devaney 混沌的。

参见文献[6] [7] [8] [9] [10]的研究和分析方法，下面将对系统(16)的解序列伪随机性进行一些分析，并在此基础上，将构造一种流密码算法。

首先，系统(16)是 Devaney 混沌的，因而在理论上其解一般是混乱和几乎不相关的，因而下面就对解序列的混乱性和相关性进行数值计算，并与常用的 Logistic 系统的相应性质进行对比。仿真效果可参见图 1，其中，(a)和(b)、以及(d)和(e)分别为本文符号系统解序列 X 和 Y 的混乱性和自相关函数，而(c)和(f)分别为 Logistic 系统解序列的混乱性和自相关函数。

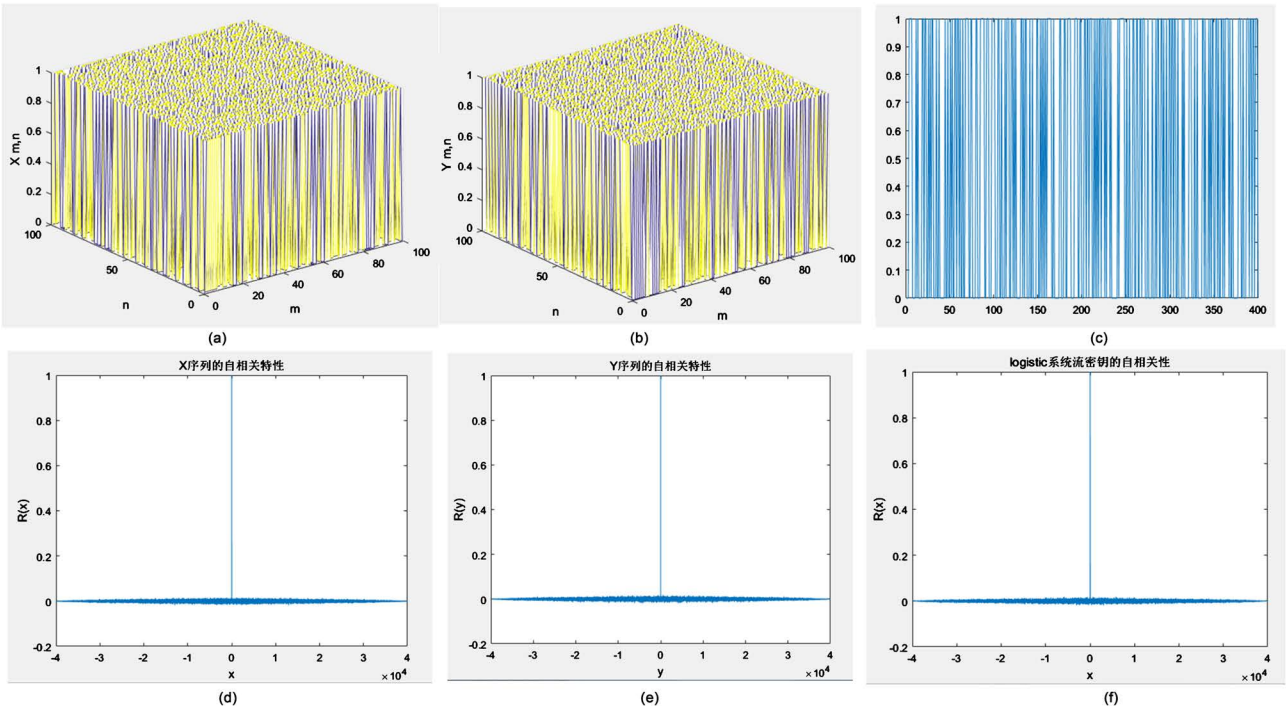

Figure 1. Confusion and correlation diagram of Solutions
图 1. 解的混乱性和相关性图

由图 1 可以看出，系统(16)解具有很好的类随机性。由于广义符号系统解序列在三维空间中都很混乱，这比二维空间中的混乱性更加复杂和难以预测，因此，利用符号系统来设计密钥流序列所具有的安全性比 Logistic 系统就会更好一些。

其次，按照常见随机数检测方法[10]，再对解序列进行单比特、扑克和游程检验，参见表 1。

从表 1 中数据可以看出，与 Logistic 系统的相应性能检测相比，本文符号系统大都会更容易通过上述 3 项随机性检测，因而它的解序列在单比特、连续多比特和游程总数的分布上都会接近均匀分布，因

而其类随机性较为理想。

最后，参照现有混沌序列密码算法的设计方法，下面利用系统(16)的解序列来构造一种流密码系统：

1) 选择常见的一副数字灰度图像作为明文，利用 Matlab 语言可以将该图像表示为一个数字矩阵 $I=\left(m_{ij}\right)_{256\times256}$，其中，每个明文数值 $m_{ij}\in Z_{256}=\{0,1,\cdots,255\}$；

2) 先选取某个 JK 触发器序列作为系统(16)的初始值，再利用系统(16)的某个解 $x=\left\{x_{m,n}\right\}_{m,n=0}^{\infty}$ 计算出密钥流序列，其中，需要将二元解序列 $\left\{x_{m,n}\right\}_{m,n=0}^{\infty}$ 转化为在 0~255 中取值的密钥流序列；

3) 加密变换：$c_{ij}=x_{ij}\oplus m_{ij}$，其中，$c_{ij}$ 表示密文数值，$\oplus$ 表示逐比特异或运算；

4) 解密变换：$m_{ij}=x_{ij}\oplus c_{ij}$。

将由上述方法所构造的流密码算法与基于 Logistic 系统所构造的流密码算法进行效果对比，它们的 Matlab 仿真效果可参见图 2。

Table 1. Three common random number test results
表 1. 三种常见随机数检测结果

检测方法	样本数量	本文符号系统 X 序列 P 值	本文符号系统 Y 序列 P 值	logistic 系统 P 值	检测结果
单比特频数检测	40,000 bit	0.5419	0.3681	0.0488	通过
扑克检测	40,000 byte	0.7751	0.7391	0.2545	通过
游程总数检测	40,000 bit	0.4461	0.9156	0.2310	通过

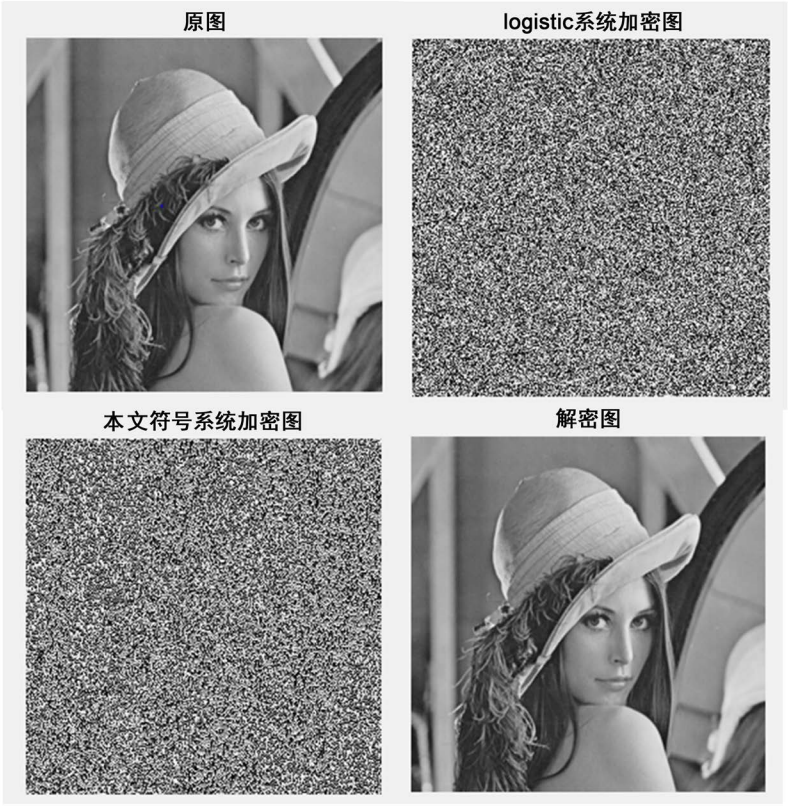

Figure 2. Encryption and decryption effect diagram
图 2. 加解密效果图

直观上，由图 2 可以看出，两种算法都能对原图像进行优良和正确的置乱加解密。下面继续再对图 2 中原图和两种算法加密效果图的 3 种方向的相邻像素值之间的相关性进行仿真计算，可见表 2。

Table 2. Correlation between adjacent pixels between original and encrypted graphs
表 2. 原图与加密图相邻像素之间各方向的相关性

方向	原图	logistic 加密图	本文符号系统加密图
水平	0.9357	0.0038	0.0053
垂直	0.9682	0.0031	0.0027
对角	0.9084	0.0016	0.0005

从表 2 中，可以看到原图在三个方向上相邻像素之间具有很高的相关性，在各个方向的相关系数都接近 1。而经过加密后，Logistic 加密图和本文符号系统加密图在各个方向的相关系数则都接近 0，说明加密效果良好。而且，还可以看出，利用本文符号系统加密比利用 Logistic 系统加密后在多数方向上的相关性更小，加密效果会更好。

3. 小结

本文研究了二维时变广义符号系统的混沌性，并对该系统所产生的序列进行了多种常见的伪随机性能分析，结果说明系统解序列的伪随机性能优良。在此基础上，构造了一种新的序列密码算法，仿真实验说明了该算法在数字图像加密中具有良好的效果。本文对今后混沌序列密码算法的研究具有一定的参考价值和实际意义。

参考文献

[1] Devaney, R.L. (1989) An Introduction to Chaotic Dynamical Systems. 2nd Edition, Addision-Wesley, New York.

[2] Chen, G., Tian, C.J. and Shi, Y.M. (2005) Stability and Chaos in 2-D Discrete Systems. *Chaos*, *Solitons and Fractals*, **25**, 637-647. https://doi.org/10.1016/j.chaos.2004.11.058

[3] Tian, C.J. (2017) Chaos in the Sense of Devaney for Two-Dimensional Time-Varying Generalized Symbolic Dynamical Systems. *Inter. J. Bifurcation and Chaos*, **27**, 1750060. https://doi.org/10.1142/S0218127417500602

[4] Tian, C.J. and Chen, G. (2006) Chaos of a Sequence of Maps in a Metric Space. *Chaos*, *Solitons and Fractals*, **28**, 1067-1075. https://doi.org/10.1016/j.chaos.2005.08.127

[5] 田传俊, 陈关荣. 广义符号动力系统的混沌性[J]. 应用数学学报, 2008, 31(3): 440-446.

[6] 田传俊, 李佳佳, 曾泉, 刘明刚. 时变广义符号动力系统的混沌性及其在流密码中的应用[J]. 网络空间安全, 2016, 7(9-10): 33-36.

[7] 田传俊, 刘明刚, 郝红建, 李佳佳. 二维时变离散时空系统的混沌性及其在流密码中的应用[J]. 信息安全与技术, 2015(7): 71-75.

[8] Ye, G.D., Pan, G., Huang, X.L., *et al.* (2018) A Chaotic Image Encryptiong Algorithm Based on Information Entropy. *International Journal of Bifurcation and Chaos*, **28**, 1850010. https://doi.org/10.1142/S0218127418500104

[9] Hua, Z.Y. and Zhou, Y.C. (2016) Image Encryption Using 2D Logistic-Adjusted-Sine Map. *Information Sciences*, **339**, 237-253. https://doi.org/10.1016/j.ins.2016.01.017

[10] 李大为, 冯登国, 陈华, 等, 编. 随机性检测规范[S]. 国家密码管理局, 2009.

知网检索的两种方式：

1. 打开知网页面 http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD
   下拉列表框选择：[ISSN]，输入期刊 ISSN：2161-8801，即可查询
2. 打开知网首页 http://cnki.net/
   左侧“国际文献总库”进入，输入文章标题，即可查询

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：csa@hanspub.org