Computer Science and Application 计算机科学与应用, 2018, 8(10), 1582-1588
Published Online October 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.810173

Hans汉斯

Design of One Stream Cipher Algorithm Based on a Time-Varying Generalized Symbolic Chaotic System

Chuanjun Tian, Xingling Li, Jing Lin, Quan Zeng

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

Received: Oct. 8th, 2018; accepted: Oct. 18th, 2018; published: Oct. 25th, 2018

Abstract

Based on the discussion of time-varying generalized symbolic chaotic systems and its construction method, pseudo-randomness of chaotic sequences produced by this system is firstly analyzed. Then, a stream cipher algorithm is designed based on chaotic sequences of this system and JK flip-flop. Finally, the designed algorithm is used in digital image encryption, and encryption and decryption effect is simulated. Simulation shows that the stream cipher algorithm has good effects in image encryption.

Keywords

Discrete System, Time-Varying Generalized Symbolic System, Devaney Chaos, Stream Cipher Algorithm

基于时变双边混沌符号系统的流密码算法设计

田传俊，黎杏玲，林　敬，曾　泉

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8日；录用日期：2018年10月18日；发布日期：2018年10月25日

摘　要

在研究了一类时变广义符号动力系统的混沌性及其构造方法的基础上，首先对这类系统所产生的混沌序

文章引用: 田传俊, 黎杏玲, 林敬, 曾泉. 基于时变双边混沌符号系统的流密码算法设计[J]. 计算机科学与应用, 2018, 8(10): 1582-1588. DOI: 10.12677/csa.2018.810173

列进行了一些伪随机性能分析和测试。然后，再综合现有的JK触发器和该系统混沌解序列设计了一种流密码算法。最后，将该算法用于数字图像加密之中，并对加解密效果进行了仿真。仿真效果说明了所设计的序列密码算法在图像加密上具有良好效果。

关键词

离散系统，时变广义符号动力系统，Devaney混沌性，流密码算法

1. 引言

众所周知，序列密码算法中的密钥流序列一般可利用具有伪随机性的离散系统来产生，而离散混沌系统是用来产生伪随机序列的一种常用方法。考虑到离散时变双边广义符号混沌系统还没有文献研究过，本文将会研究这类特殊系统的混沌性及其在序列密码算法设计上的应用。

设 $Z=\{\cdots,-1,0,1,\cdots\}$ 是一个双边整数集，$N_t=\{t,t+1,\cdots\}$ 是一个单边整数集，对任一 $t\in Z$。文献[1]-[8]讨论了多种时变或时不变单边离散时空系统。本文将讨论一类新的时变双边离散时空系统：

$$x_{m+1,n}=f\left(m,x_{m,n-1},x_{m,n},x_{m,n+1}\right),\quad m=0,1,2,\cdots,\quad n=\cdots,-1,0,1,\cdots \tag{1}$$

其中，I 是实数集 R 的一个有界子集，多元函数 $f:N_0\times I^3\to I$ 是系统(1)的系统函数。

显然，对任意 $\phi=\{\phi_{0,n}\}_{n=-\infty}^{\infty}$，存在一个离散时空序列 $x=\{x_{m,n}\mid m=0,1,2,\cdots,n\in Z\}$ 满足(1)，且 $x_{0,n}=\phi_{0,n}$，$n\in Z$。称 x 为系统(1)初值为 ϕ 的一个解。参照文献[5]，当 $I=Z_q=\{0,1,\cdots,q-1\}$ 时，将系统(1)称为(时变双边)广义符号动力系统，其中，$q\in N_2$。

对于任一有界实数子集 I，记

$$I_{-\infty}^{\infty}=\left\{\{a_n\}_{n=-\infty}^{\infty}=\left(\cdots,a_{-1},a_0,a_1,\cdots\right)\mid a_i\in I,i=\cdots,-1,0,1,\cdots\right\} \tag{2}$$

设 $x=\{x_{m,n}\mid m\in N_0,n\in Z\}$ 是系统(1)的一个解，$x_{0,n}\in I$，$n\in Z$，且

$$x_m=\left(\cdots,x_{m,-1},x_{m,0},x_{m,1},\cdots\right)=\{x_{m,n}\}_{n=-\infty}^{\infty},\quad m\in N_0 \tag{3}$$

则系统(1)等价于如下的无穷维离散系统

$$x_{m+1}=\left\{f\left(m,x_{m,n-1},x_{m,n},x_{m,n+1}\right)\right\}_{n=-\infty}^{\infty}=g_{m+1}\left(x_m\right),\quad m\in N_0 \tag{4}$$

其中，该系统映射列 $g_1,g_2,\cdots$ 或 $G=\{g_m\}_{m=1}^{\infty}$ 是由 f 决定或导出的 $I_{-\infty}^{\infty}$ 上的一列映射。

上面介绍了本文所要研究的离散时空系统的基本知识，后续内容安排如下：第 2 节将介绍与 Devaney 混沌相关的基本概念；第 3 节将会构造出一类具体的时变双边广义符号混沌系统，将对该系统解序列的伪随机性进行一些常见的仿真分析，并将对所构造的一种混沌序列密码算法进行仿真。

2. 几个定义

一般地，利用度量空间 (X,d) 上的一列映射 $g_1,\cdots,g_n,\cdots$ 都能产生如下形式的时变离散系统

$$x_{m+1}=g_{m+1}(x_m),\quad x_0\in X,\quad m\in N_0 \tag{5}$$

给定任一点 $x_0\in X$，都存在一个序列 $O(x_0)=\{x_m\}_{m=0}^{\infty}$ 满足(5)。将 $O(x_0)$ 称为系统(5)初值为 x_0 的一个解或映射列 $G=\{g_n\}_{n=1}^{\infty}$ 的一条轨道。对任意 $x\in X$ 和 $m=0,1,\cdots$，记

$$G_m(x)=g_m\left(g_{m-1}\left(\cdots\left(g_1(x)\right)\cdots\right)\right)=g_m\circ\cdots\circ g_1(x),\quad G_0(x)=x \tag{6}$$

对任一有界实数集 I，设 $I_{-\infty}^{\infty}$ 由式(2)定义。可定义如下度量 d_1 而得到度量空间 $\left(I_{-\infty}^{\infty},d_1\right)$：

$$d_1(x,y)=\sum_{n=-\infty}^{\infty}\frac{|x_n-y_n|}{2^{|n|}},\ \text{对任意}\ x=\{x_n\}_{n=-\infty}^{\infty},y=\{y_n\}_{n=-\infty}^{\infty}\in I_{-\infty}^{\infty} \tag{7}$$

下面将给出一列映射与混沌相关的几个概念，可参见文献[4] [5] [6]。

定义 1. 如果 $G=\{g_n\}_{n=1}^{\infty}$ 的一条轨道 $O(x_0)=\{x_m\}_{m=0}^{\infty}$ 是周期性的，即存在正整数 p，使得 $x_{m+p}=x_m$，$m\in N_0$，则称 x_0 为 G 或系统(5)的周期点，称 p 为 x_0 或 $O(x_0)$ 的周期。如果 G 的所有周期点组成的集合在 X 中是稠密的，则称 G 或系统(5)具有周期点的稠密性。

定义 2. 对于度量空间 (X,d) 上的一列映射 $g_1,g_2,\cdots$，如果对 X 的任意两个非空开子集 U 和 V，都存在正整数 n，使得 $G_n(U)\cap V$ 不是空集，则称 $G=\{g_n\}_{n=1}^{\infty}$ 或系统(5)具有传递性。

另外，如果存在 $\delta>0$，使得对任意 $x\in X$ 和 x 的任一邻域 U，都存在一个正整数 m 和 $y\in U$，使得 $d\left(G_m(x),G_m(y)\right)>\delta$，则称 $G=\{g_m\}_{m=1}^{\infty}$ 或系统(5)具有对初值的敏感依赖性。

定义 3. 称度量空间 (X,d) 上的一列映射 $G=\{g_m\}_{m=1}^{\infty}$ 或时变离散系统(5)在 Devaney 意义下是混沌的，简称为 Devaney 混沌，如果 1) G 或系统(5)具有传递性；2) G 或系统(5)具有周期点的稠密性；(*iii*) G 或系统(5)具有对初值的敏感依赖性。

定义 4. 设 I 是有界实数集，$f:N_0\times I^3\to I$ 是一个四元函数，且 $G=\{g_n\}_{n=1}^{\infty}$ 是由系统(1)所导出的度量空间 $\left(I_{-\infty}^{\infty},d_1\right)$ 上的一列映射。如果系统(4)或映射列 $G=\{g_n\}_{n=1}^{\infty}$ 在 $\left(I_{-\infty}^{\infty},d_1\right)$ 上具有传递性或周期点的稠密性或对初值的敏感依赖性，则相应地称系统(1)或 f 在 $\left(I_{-\infty}^{\infty},d_1\right)$ 上具有传递性或周期点的稠密性或对初值的敏感依赖性。特别地，如果系统(4)或 $G=\{g_n\}_{n=1}^{\infty}$ 在 $\left(I_{-\infty}^{\infty},d_1\right)$ 上是 Devaney 混沌的，则称系统(1)在 $\left(I_{-\infty}^{\infty},d_1\right)$ 上是 Devaney 混沌的。

3. 广义符号混沌系统的构造

设 $I=Z_q=\{0,1,\cdots,q-1\}$，$f:N_0\times I^3\to I$ 定义如下：对任意 $x_{-1},x_0,x_1\in I$ 和 $m\in N_0$，

$$f(m,x_{-1},x_0,x_1)=ax_{-1}+c_mx_0+bx_1 \bmod q=ax_{-1}\oplus c_mx_0\oplus bx_1 \tag{8}$$

其中，$q>1$ 是一个正整数，$a,b\in Z_q$ 是两个正整数，$\{c_m\}_{m=-\infty}^{\infty}$ 是一个周期为 p 的周期整数数列，即对一切 $m\in N_0$，有 $c_m=c_{m+p}\in Z$，以及 a 与 q 互素，且 b 与 q 互素。

不难发现，利用式(8)所定义的函数 f 可以生成如下的时变广义符号动力系统

$$x_{m+1,n}=f\left(m,x_{m,n-1},x_{m,n},x_{m,n+1}\right)=ax_{m,n-1}\oplus c_mx_{m,n}\oplus bx_{m,n+1},\quad x_{m,n}\in I,\quad m,n\in N_0 \tag{9}$$

显然，系统(9)是系统(1)的特殊情形，因而它会等价于如下的一个无穷维离散系统：

$$x_{m+1}=g_{m+1}(x_m),\quad x_0\in I_{-\infty}^{\infty},\quad m\in N_0 \tag{10}$$

其中，$x_m=\{x_{m,n}\}_{n=-\infty}^{\infty}\in I_{-\infty}^{\infty}$ 和 $g_{m+1}:I_{-\infty}^{\infty}\to I_{-\infty}^{\infty}$ 是由 f 所导出的一个映射，$m\in N_0$，且对任意 $\alpha=\{u_n\}_{n=-\infty}^{\infty}\in I_{-\infty}^{\infty}$，都有 $g_{m+1}(\alpha)=\{au_{n-1}\oplus c_mu_n\oplus bu_{n+1}\}_{n=-\infty}^{\infty}\in I_{-\infty}^{\infty}$，$m\in N_0$。

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 $g_m=g_{m+p}$，$m\in N_1$。

事实上，由已知条件和式(9)和(10)，对任一 $m\in N_0$ 和任意 $u=\{u_n\}_{n=-\infty}^{\infty}\in I_{-\infty}^{\infty}$，有

$$g_{m+1}(u)=\{au_{n-1}\oplus c_m u_n\oplus bu_{n+1}\}_{n=-\infty}^{\infty}=\{au_{n-1}\oplus c_{m+p}u_n\oplus bu_{n+1}\}_{n=-\infty}^{\infty}=g_{m+1+p}(u)。$$

推论 1. 设 $G=\{g_n\}_{n=1}^{\infty}$ 是由系统(10)的一列系统映射，则对一切 $m,s,t\in N_1$，都有

$$g_{s+mp-1}\circ g_{s+mp-2}\circ\cdots\circ g_s=g_{t+mp-1}\circ g_{t+mp-2}\circ\cdots\circ g_t \tag{11}$$

利用自然数性质，容易证明如下结果。

引理 2. 对任一正整数 m 和 $u,v\in I=Z_q$，存在 $s,t\in I$，使得 $u\oplus b^m s=v$ 和 $a^m t\oplus u=v$。

定理 1. 系统(9)在度量空间 $(I_{-\infty}^{\infty},d_1)$ 上是 Devaney 混沌的，其中，度量 d_1 由式(7)定义。

证明：由定义 4，只需要证明系统(10)是 $(I_{-\infty}^{\infty},d_1)$ 上的 Devaney 混沌系统。

首先，将证明系统(10)在 $(I_{-\infty}^{\infty},d_1)$ 上具有传递性。

设 U 和 V 是 $I_{-\infty}^{\infty}$ 中任意两个非空开子集，则对任一 $\alpha=\{s_n\}_{n=-\infty}^{\infty}\in U$ 和 $\beta=\{t_n\}_{n=-\infty}^{\infty}\in V$，存在常数 $\theta>0$，使得 $B_\theta(\alpha)=\left\{x=\{x_n\}_{n=0}^{\infty}\in I_{-\infty}^{\infty}\mid d_1(x,\alpha)<\theta\right\}\subseteq U$ 和 $B_\theta(\beta)\subseteq V$。因此，由式(7)可知，存在一个正整数 M，使得

$$\begin{aligned}&\left\{x=\{x_n\}_{n=-\infty}^{\infty}\mid x_i=s_i,|i|=0,1,\cdots,M-1;x_j\in I;|j|\ge M\right\}\subseteq B_\theta(\alpha)\\&\left\{y=\{y_n\}_{n=-\infty}^{\infty}\mid y_i=t_i,|i|=0,1,\cdots,M-1;y_j\in I;|j|\ge M\right\}\subseteq B_\theta(\beta)\end{aligned} \tag{12}$$

对任一 $x=\{x_n\}_{n=-\infty}^{\infty}\in I_{-\infty}^{\infty}$，记

$$G_1(x)=g_1(x)=\{ax_{n-1}\oplus c_0x_n\oplus bx_{n+1}\}_{n=-\infty}^{\infty}=\{x_n^{(1)}\}_{n=-\infty}^{\infty}=x^{(1)},$$

其中，$x^{(1)}=\{x_n^{(1)}=f_0(x_{n-1},x_n)\oplus bx_{n+1}\}_{n=-\infty}^{\infty}=\{x_n^{(1)}=ax_{n-1}\oplus h_0(x_n,x_{n+1})\}_{n=-\infty}^{\infty}$，且 $f_0(x_{n-1},x_n)=ax_{n-1}\oplus c_0x_n$，$h_0(x_n,x_{n+1})=c_0x_n\oplus bx_{n+1}$。

一般地，利用递推法，对任意 $m=1,2,\cdots$ 和 $x=\{x_n\}_{n=-\infty}^{\infty}\in I_{-\infty}^{\infty}$，都有

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

其中，G_m 由式(6)定义，且

$$x^{(m)}=\{x_n^{(m)}=f_{m-1}(x_{n-m},\cdots,x_{n+m-1})\oplus b^m x_{n+m}=a^m x_{n-m}\oplus h_{m-1}(x_{n-m+1},\cdots,x_{n+m})\}_{n=-\infty}^{\infty} \tag{13}$$

以及 $f_{m-1}:I^{2m}\to I$ 和 $h_{m-1}:I^{2m}\to I$ 是由式(8)定义的函数 f 唯一决定的两个函数，$m\in N_1$。

由引理 2 可知，对任一给定的 $m\in N_1$ 和整数 $w\in I$，都存在整数 $u,v\in I$，使得

$$f_{m-1}(x_{n-m},\cdots,x_{n+m-1})\oplus b^m u=w,\quad a^m v\oplus h_{m-1}(x_{n-m+1},\cdots,x_{n+m})=w \tag{14}$$

对于 $\alpha=\{s_n\}_{n=-\infty}^{\infty}\in U$ 和 $\beta=\{t_n\}_{n=-\infty}^{\infty}\in V$，由式(12)，(13)和(14)，存在 $\eta=\{z_n\}_{n=-\infty}^{\infty}\in I_{-\infty}^{\infty}$，满足 $z_n=s_n$，对 $n=-M,\cdots,0,1,\cdots,M-1$，且依次选取 $z_M,z_{M+1},\cdots$ 和 $z_{-M-1},z_{-M-2},\cdots$ 满足

$$f_{M-1}(z_{n-M},\cdots,z_{n+M-1})\oplus b^M z_{n+M}=t_n,\quad n=0,1,2,\cdots,$$

$$a^M z_{n-M}\oplus h_{M-1}(z_{n-M+1},\cdots,z_{n+M})=t_n,\quad n=-1,-2,\cdots。$$

因此，$G_M(\eta)=g_M\circ\cdots\circ g_1(\eta)=\beta\in V$，且 $\eta\in U$。于是，系统(10)在 $(I_{-\infty}^{\infty},d_1)$ 上是传递的。

其次，将证明系统(10)在 $(I_{-\infty}^{\infty},d_1)$ 上具有稠密的周期点集。

对任一 $\alpha=\{s_n\}_{n=-\infty}^{\infty}\in I_{-\infty}^{\infty}$ 和 α 的任意邻域 U，都存在正数 ε_0 和某个充分大整数 $M>0$，使得 $B_{\varepsilon_0}(\alpha)\subseteq U$ 和

$$\left\{y=\{x_n\}_{n=-\infty}^{\infty}\in I_{-\infty}^{\infty}\mid x_i=s_i;x_j\in I,|i|=0,1,\cdots,M-1;|j|\ge M\right\}\subseteq B_{\varepsilon_0}(\alpha) \tag{15}$$

类似于上面传递性证明，一定存在 $\rho=\{z_n\}_{n=-\infty}^{\infty}\in B_{\varepsilon_0}(\alpha)$，使得

$$f_{M-1}(z_{n-M},\cdots,z_{n+M-1})\oplus b^M z_{n+M}=z_n,\quad n=0,1,2,\cdots,$$

$$a^M z_{n-M}\oplus h_{M-1}(z_{n-M+1},\cdots,z_{n+M})=z_n,\quad n=-1,-2,\cdots。$$

因此，$\rho\in U$ 和 $G_M(\rho)=g_M\circ\cdots\circ g_1(\rho)=\rho\in U$。

由式(11)，可得 $G_{2M}(\rho)=g_{2M}\circ\cdots\circ g_{M+1}\circ\left(g_M\circ\cdots\circ g_1(\rho)\right)=\rho\in U$。利用归纳法可证：对任意 $s\in N_1$，都有 $G_{sM}(\rho)=g_{sM}\circ\cdots\circ g_1(\rho)=\rho$。因此，$\rho\in U$ 和 ρ 是系统(10)或映射列 $G=\{g_n\}_{n=1}^{\infty}$ 的一个周期点。于是，系统(10)在 $\left(I_{-\infty}^{\infty},d_1\right)$ 上具有周期点的稠密性。

最后，将证明系统(10)在 $\left(I_{-\infty}^{\infty},d_1\right)$ 上具有对初值的敏感依赖性。

设 $\delta=0.1$，$\alpha=\{s_n\}_{n=-\infty}^{\infty}\in I_{-\infty}^{\infty}$，且 U 是 α 的任一邻域，则存在 $\varepsilon_0>0$ 和充分大整数 $M\in N_1$，使得 $B_{\varepsilon_0}(\alpha)\subseteq U$ 和式(15)成立。因此，类似于上面证明，存在 $\lambda=\{t_n\}_{n=-\infty}^{\infty}\in B_{\varepsilon_0}(\alpha)$，使得 $t_i=s_i$，对任意 $i\in\{-M,\cdots,-1,0,1,\cdots,M-1\}$，且依次选取任一 $j\in\{M,M+1,\cdots\}\bigcup\{-M-1,-M-2,\cdots\}$，存在 $t_j\in I$，使得 $\left|t_0^{(m)}-s_0^{(m)}\right|>\delta$，以及

$$t_0^{(M)}=f_{M-1}(t_{-M},\cdots,t_{M-1})\oplus b^M t_M,\quad a_0^{(M)}=f_{M-1}(s_{-M},\cdots,s_{M-1})\oplus b^M t_M。$$

于是，$\gamma\in B_{\varepsilon_0}(\alpha)\subseteq U$ 和

$$d\left(G_M(\alpha),G_M(\gamma)\right)=\sum_{i=-\infty}^{\infty}\frac{\left|t_i^{(M)}-s_i^{(M)}\right|}{2^{|i|}}\geq\left|t_0^{(M)}-s_0^{(M)}\right|\geq\delta=0.1。$$

因此，系统(10)在 $\left(I_{-\infty}^{\infty},d_1\right)$ 上具有对初值的敏感依赖性。

综合上面的证明过程可知，系统(10)在度量空间 $\left(I_{-\infty}^{\infty},d_1\right)$ 上是 Devaney 混沌的。证毕。

例 1. 考虑如下时变离散时空系统

$$x_{m+1,n}=3x_{m,n-1}\oplus r_m x_{m,n}\oplus x_{m,n+1}=3x_{m,n-1}+r_m x_{m,n}+x_{m,n+1}\bmod 2 \tag{16}$$

其中，$x_{0,n}\in I=Z_2=\{0,1\}$ 和 $r_m=2m\bmod(5)$，对任意 $m,n\in N_0$，$\bmod(\bullet)$ 表示模 2 加法运算。

由于系统(16)是时变广义双边符号系统，因此，现有的判断标准无法判断系统(16)是否是 Devaney 混沌的。但是，由于 $\{r_m\}_{m=0}^{\infty}$ 都是周期数列，因而系统(16)是系统(9)的特殊情形，且满足定理 1 中的各项条件。因此，由定理 1，系统(16)在度量空间 $\left(I_{-\infty}^{\infty},d_1\right)$ 上是 Devaney 混沌的。

下面来分析系统(16)解的伪随机性能，并利用它来构造一种序列密码算法。

首先，考虑到系统(16)是 Devaney 混沌的，其解理论上应该是混乱和接近不相关的。下面对系统(16)解序列的混乱性和相关性进行数值计算，并与 Logistic 系统产生的混沌序列的混乱性和相关性作对比，可见图 1，其中(a)和(b)分别为上述符号系统和 Logistic 系统的解的混乱性，(c)和(d)分别为上述符号系统和 Logistic 系统的解的相关性。直观上看，符号系统在三维空间中的混乱性比 Logistic 所在二维空间中的混乱性要更“乱”，且它们的相关性几乎相同。因此，仿真说明本文所研究的符号系统的解序列具有很好的类随机性。

其次，考虑文献[9]曾给出了多种序列随机性能的检测方法，下面再来对上述符号系统解序列进行其中的 3 种最常见随机性检测，即单比特、扑克和游程检验，其中，单比特检测主要用于序列中 0 和 1 的均匀分布性检测，扑克检测用于序列的多个连续比特的均匀分布性检测，游程检测用于游程总数的随机性检测。这些都能从某个方面分析序列的随机性能的好坏，其检测仿真效果见表 1。

最后，再利用系统(16)的解 $z=\left\{x_{m,n}\right\}_{m,n=-\infty}^{\infty}\in I^{\infty}$ 中的数值构造如下的一种流密码系统：

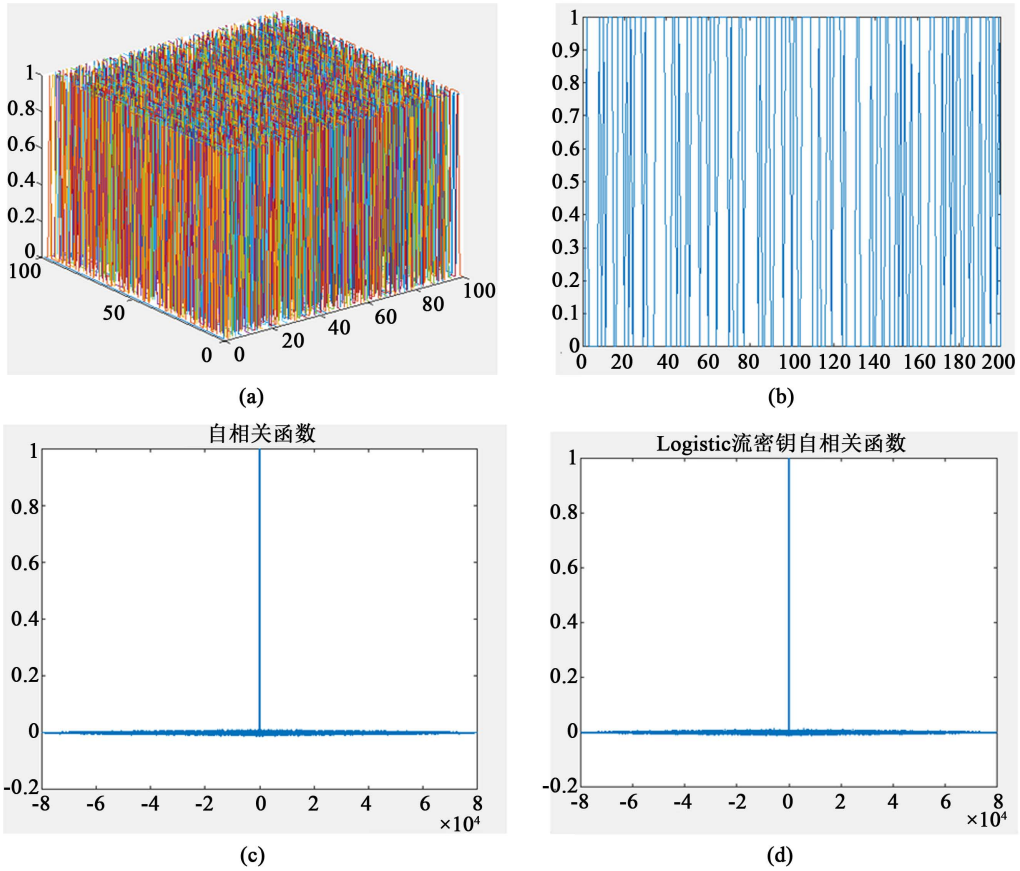

Figure 1. Solution confusion and correlation
图 1. 解的混乱性与相关性

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

	样本数量	本文符号系统 P 值	Logistic 系统 P 值	检测结果
单比特频数检测	80,000 bit	0.0269	0.2793	通过
扑克检测	80,000 byte	0.5962	0.3401	通过
游程总数检测	80,000 bit	0.7816	0.2928	通过

1) 选择一副数字灰度图像作为明文，利用 Matlab 语言将该图像表示为数字矩阵 $I=\left(m_{ij}\right)_{256\times256}$，其中，每个明文数值 $m_{ij}\in Z_{256}=\{0,1,\cdots,255\}$；

2) 先选取一个 JK 序列，以它作为初始值，再利用系统(16)的某个解 $z=\left\{x_{m,n}\right\}$ 来产生密钥流序列，并将该二元密钥流序列转化为值为 0~255 的序列；

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：$m_{ij}=x_{ij}\oplus c_{ij}$。

将上述简单加密算法与基于常见的 Logistic 系统加密算法进行对比，它们的 Matlab 仿真效果可参见图 2。

直观上，由图 2 可以看出，两种算法都能进行正确的加解密。而且，再对图 2 中两种算法加密效果图的 3 种方向的相关性进行仿真计算，计算结果可见表 2。

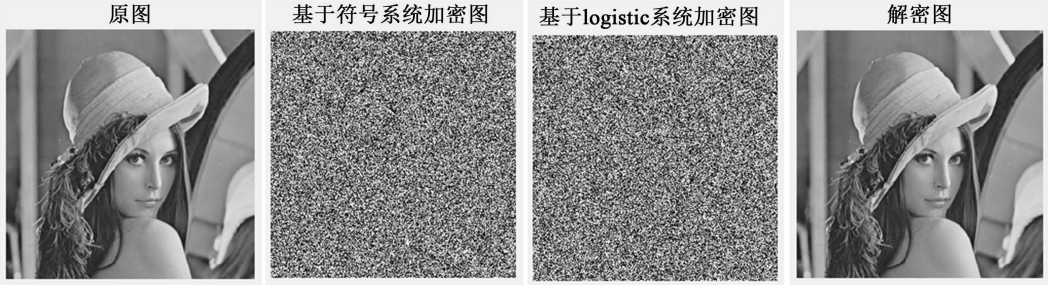

Figure 2. Add and decrypt renderings
图 2. 加解密效果图

Table 2. Correlation coefficient between original image and encrypted image
表 2. 原始图像和加密图像的相关系数

方向	原图	本文符号系统	Logistic 系统
水平	0.9357	−0.0007	−0.0076
垂直	0.9682	0.0011	0.0012
对角线	0.9084	0.0052	0.0039

从表 2 中，可以看出，原始图像在各个方向的相关系数都接近 1，而加密图像各个方向的相关系数则都在 0 左右。而且，利用本文符号系统加密的效果比利用 Logistic 系统加密的效果略有改善。这说明本文符号加密系统更有利于有效抵御统计攻击。

4. 小结

本文研究了时变双边广义符号系统的混沌类随机性，并对该系统所产生的序列进行了多种伪随机性能分析，分析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。本文的研究在混沌序列密码算法研究领域具有一定的指导意义。

参考文献

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

[2] Elaydi, S.N. (2000) Discrete Chaos. Chapman & Hall/CRC.

[3] 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

[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] Shi, Y.M. and Chen, G. (2009) Chaos of Time-Varying Discrete Dynamical Systems. *Journal of Difference Equations and Applications*, **15**, 429-449. https://doi.org/10.1080/10236190802020879

[7] 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]. 信息安全与技术, 2016, 7(9-10): 33-36.

[8] 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.

[9] 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