**Computer Science and Application** 计算机科学与应用, 2020, 10(1), 118-125
Published Online January 2020 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2020.101013

Hans汉斯

# Design of a Stream Cipher Algorithm Based on Latin Square and Time-Varying Symbolic Chaotic System

**Wenjun Tang, Chuanjun Tian**

College of Electronics and Information Engineering, Shenzhen University, Shenzhen Guangdong
Email: tiancj@sina.com.cn

Received: Jan. 1st, 2020; accepted: Jan. 12th, 2020; published: Jan. 19th, 2020

## Abstract

**This paper studies chaos of a class of three-dimensional time-varying generalized symbolic systems, and analyzes the pseudo-randomicity of its solutions. Then, combined with the basic cryptosystem designed by Latin square, a stream cipher algorithm was designed. Finally, the encryption effect of the algorithm on digital image is simulated and compared with the simulation results of the modulo 2 addition stream cipher system. Simulation shows that this algorithm has good encryption effects.**

## Keywords

**Stream Cipher Algorithm, Generalized Symbolic System, Latin Square, Basic Cryptosystem**

# 基于拉丁方与时变符号混沌系统的流密码算法设计

**唐文君，田传俊**

深圳大学电子与信息工程学院，广东 深圳
Email: tiancj@sina.com.cn

收稿日期：2020年1月1日；录用日期：2020年1月12日；发布日期：2020年1月19日

## 摘 要

**本文研究了一类三维时变广义符号动力系统的混沌性，并对它的多种伪随机性能进行了分析。在此基础**

文章引用: 唐文君, 田传俊. 基于拉丁方与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, 2020, 10(1): 118-125. DOI: 10.12677/csa.2020.101013

**上，结合拉丁方构造的基本密码系统，设计了一种多元流密码算法。最后，对该算法在数字图像上的加密效果进行了仿真，并与模2加法流密码系统的仿真结果进行了对比。仿真结果分析表明新流密码算法具有良好的加密效果和较高的安全性。**

## 关键词

**流密码算法，广义符号动力系统，拉丁方，基本密码系统**

Copyright © 2020 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access

## 1. 引言

众所周知，密码学中的加密算法是解决信息安全问题的有效手段之一，流密码作为现代密码学的一个重要分支，已在许多领域得到广泛应用[1] [2] [3]。一般而言，流密码算法直接将密钥流序列与明密文序列模 2 加法进行加解密。但是，最近的文献[2]明确指出流密码算法设计可分为两个部分：一是基本密码系统设计，二是密钥流序列的设计，其中，基本密码系统可利用一组任意阶拉丁方设计，推广了利用模 2 加法或 2 阶拉丁方所设计的基本密码系统。当前，利用高于 2 阶拉丁方来设计基本密码系统的研究还未充分发展。另外，参照现有不少文献[4] [5] [6]知，可直接利用混沌系统生成的伪随机序列作为密钥流序列，因而先讨论一类新的三维时变广义符号系统。

不妨设 $Z$ 为全体整数集，$t\in Z$，$N_t=\{t,t+1,\cdots\}$ 为单边整数集，$I$ 为有界实数集，

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

其中，$m,n\in N_0$，$f:N_0\times I^4\to I$，$g:N_0\times I^4\to I$，$h:N_0\times I^4\to I$ 分别为三个多元函数，并称$(f,g,h)$为系统(1)的系统函数。对任意定义在$\Omega=\{(0,n)\mid n\in N_0\}$上的三个序列$\phi=\{\phi_{0,n}\}$，$\varphi=\{\varphi_{0,n}\}$和$\gamma=\{\gamma_{0,n}\}$，存在三维离散时空序列$x=\{(x_{m,n},y_{m,n},z_{m,n})\}_{m,n=0}^{\infty}$满足(1)，且$x_{m,n}=\phi_{m,n}$，$y_{m,n}=\varphi_{m,n}$，$z_{m,n}=\gamma_{m,n}$，对$(m,n)\in\Omega$。称序列 $x$ 为系统(1)初值为$(\phi,\varphi,\gamma)$的一个解。由文献[4]可知，当$I=Z_q=\{0,1,\cdots,q-1\}$和$q\in N_2$时，可将系统(1)称为三维时变广义符号动力系统。在不混淆时，下面也将列向量写为行向量的形式。

对任一有界实数集 $I$，记

$$I_3^{\infty}=\left\{\left\{(a_n,b_n,c_n)^{\mathrm{T}}\right\}_{n=0}^{\infty}=\begin{pmatrix} a_0 & a_1 & \cdots & a_n & \cdots \\ b_0 & b_1 & \cdots & b_n & \cdots \\ c_0 & c_1 & \cdots & c_n & \cdots \end{pmatrix}\middle| a_i,b_i,c_i\in I,i=0,1,\cdots\right\} \tag{2}$$

则在 $I_3^{\infty}$ 上可定义如下度量，

$$d_1(x_1,x_2)=\sum_{n=0}^{\infty}\frac{|x_{1,n}-x_{2,n}|+|y_{1,n}-y_{2,n}|+|z_{1,n}-z_{2,n}|}{2^n} \tag{3}$$

对任意 $x_i=\{(x_{i,n},y_{i,n},z_{i,n})\}_{n=0}^{\infty}\in I_3^{\infty}$，$i=1,2$。易知$(I_3^{\infty},d_1)$是度量空间。

设 $x=\left\{\left(x_{m,n},y_{m,n},z_{m,n}\right)\right\}_{m,n=0}^{\infty}$ 是系统(1)的一个解， $x_{0,n},y_{0,n},z_{0,n}\in I$ ， $n\in N_0$ ，且

$$x_m=\left\{\left(x_{m,n},y_{m,n},z_{m,n}\right)\right\}_{n=0}^{\infty},m\in N_0, \tag{4}$$

记 $\Delta_{1m,n}=f\left(m,x_{m,n},y_{m,n},z_{m,n},x_{m,n+1}\right)$ ， $\Delta_{2m,n}=g\left(m,y_{m,n},x_{m,n},z_{m,n},y_{m,n+1}\right)$ ，$\Delta_{3m,n}=h\left(m,z_{m,n},x_{m,n},y_{m,n},z_{m,n+1}\right)$ ，则系统(1)等价于式(5)中给出的无穷维离散系统：

$$x_{m+1}=\left\{\left(\Delta_{1m,n},\Delta_{2m,n},\Delta_{3m,n}\right)\right\}_{n=0}^{\infty}=F_{m+1}\left(x_m\right),\ m\in N_0 \tag{5}$$

其中， $F_1,F_2,\cdots$ 是 $I_3^{\infty}$ 上由 $\left(f,g,h\right)$ 决定的一列映射。称系统(5)或映射列 $F=\left\{F_m\right\}_{m=1}^{\infty}$ 是由系统(1)或系统函数 $\left(f,g,h\right)$ 所导出的。

## 2. 新混沌系统的构造和伪随机性分析

设 $I=Z_q=\left\{0,1,\cdots,q-1\right\}$ ，对任意 $a,b\in Z_q$ ，记 $a\oplus b=\left(a+b\right)\bmod q$ ，则 $f:N_0\times I^4\to I$ ， $g:N_0\times I^4\to I$ ，$h:N_0\times I^4\to I$ 定义如下

$$\begin{aligned}f\left(m,x_0,y_0,z_0,x_1\right)&=a_{0,m}x_0\oplus a_{1,m}y_0\oplus a_{2,m}z_0\oplus ax_1\\g\left(m,y_0,x_0,z_0,y_1\right)&=b_{0,m}y_0\oplus b_{1,m}x_0\oplus b_{2,m}z_0\oplus by_1\\h\left(m,z_0,x_0,y_0,z_1\right)&=c_{0,m}z_0\oplus c_{1,m}x_0\oplus c_{2,m}y_0\oplus cz_1\end{aligned} \tag{6}$$

其中， $\left\{a_{i,m}\right\}_{m=0}^{\infty}$ ， $\left\{b_{i,m}\right\}_{m=0}^{\infty}$ 和 $\left\{c_{i,m}\right\}_{m=0}^{\infty}$ 为周期整数数列，即存在正整数 $p$，使得 $a_{i,m}=a_{i,m+p}$ ， $b_{i,m}=b_{i,m+p}$ ，$c_{i,m}=c_{i,m+p}$ ，对一切 $i=0,1,2$ 和 $m\in N_0$ 成立， $a,b,c$ 是三个与 $q$ 互素的正整数。

不难发现，由式(6)定义的映射 $\left(f,g,h\right)$ 可产生三维时变广义符号系统如下

$$\begin{cases}x_{m+1,n}=f\left(m,x_{m,n},y_{m,n},z_{m,n},x_{m,n+1}\right)=a_{0,m}x_{m,n}\oplus a_{1,m}y_{m,n}\oplus a_{2,m}z_{m,n}\oplus ax_{m,n+1}\\y_{m+1,n}=g\left(m,y_{m,n},x_{m,n},z_{m,n},y_{m,n+1}\right)=b_{0,m}y_{m,n}\oplus b_{1,m}x_{m,n}\oplus b_{2,m}z_{m,n}\oplus by_{m,n+1}\\z_{m+1,n}=h\left(m,z_{m,n},x_{m,n},y_{m,n},z_{m,n+1}\right)=c_{0,m}z_{m,n}\oplus c_{1,m}x_{m,n}\oplus c_{2,m}y_{m,n}\oplus cz_{m,n+1}\end{cases} \tag{7}$$

其中， $x_{m,n},y_{m,n},z_{m,n}\in Z_q$ ， $m,n\in N_0$ 。由于系统(7)是系统(1)的特定情形，故根据系统(1)和系统(5)的关系，系统(7)等价于如下系统(8)

$$x_{m+1}=F_{m+1}\left(x_m\right),\ x_0\in I_3^{\infty},\ m\in N_0 \tag{8}$$

上式中， $x_m=\left\{\left(x_{m,n},y_{m,n},z_{m,n}\right)\right\}_{n=0}^{\infty}\in I_3^{\infty}$ ， $F_{m+1}:I_3^{\infty}\to I_3^{\infty}$ 是由 $\left(f,g,h\right)$ 所导出的映射，且对任意 $\alpha=\left\{\left(u_n,v_n,w_n\right)\right\}_{n=0}^{\infty}\in I_3^{\infty}$ ，记 $\tilde{u}_{m,n}=a_{0,m}u_n\oplus a_{1,m}v_n\oplus a_{2,m}w_n$ ， $\tilde{v}_{m,n}=b_{0,m}v_n\oplus b_{1,m}u_n\oplus b_{2,m}w_n$ ，$\tilde{w}_{m,n}=c_{0,m}w_n\oplus c_{1,m}u_n\oplus a_{2,m}v_n$ ，则有

$$F_{m+1}\left(\alpha\right)=\left\{\left(\tilde{u}_{m,n}\oplus au_{n+1},\tilde{v}_{m,n}\oplus bv_{n+1},\tilde{w}_{m,n}\oplus cw_{n+1}\right)\right\}_{n=0}^{\infty} \tag{9}$$

参照文献[4] [5] [6] [7]，易得如下引理及推论。

**引理 1**：对式(8)中的映射列 $F=\left\{F_n\right\}_{n=1}^{\infty}$ ，存在正整数周期 $p$，使得 $F_m=F_{m+p}$ ， $m\in N_1$ 。

**推论 1**：设 $F=\left\{F_n\right\}_{n=1}^{\infty}$ 是式(8)的系统映射，则对一切 $m,s,t\in N_1$ ，都有

$$F_{s+mp-1}\circ F_{s+mp-2}\circ\cdots\circ F_s=F_{t+mp-1}\circ F_{t+mp-2}\circ\cdots\circ F_t$$

记式(8)定义的映射列 $F=\left\{F_n\right\}_{n=1}^{\infty}$ 所确定的复合映射为：

$$G_m=F_m\circ F_{m-1}\circ\cdots\circ F\ ,\ m\in N_1 \tag{10}$$

**引理 2**：对 $m\in N_1$ 和 $a,b,r\in I=Z_q$，存在 $s\in I$，使 $a\oplus r^m s=b$ 成立。

**定义 1**：若式(1)的系统函数 $(f,g,h)$ 所确定的映射列 $F=\{F_n\}_{n=1}^{\infty}$ 或系统(5)在度量空间 $\left(I_3^{\infty},d_1\right)$ 上具有传递性、周期点的稠密性和初值敏感依赖性，则称 $F=\{F_n\}_{n=1}^{\infty}$ 或系统(5)是 *Devaney* 混沌的，也称与系统(5)相应等价的系统(1)在 $\left(I_3^{\infty},d_1\right)$ 上是 *Devaney* 混沌的。

**定理 1**：在上述条件下，系统(7)在度量空间 $\left(I_3^{\infty},d_1\right)$ 上是 *Devaney* 混沌的。

证明：由定义 1，只需证明系统(8)在 $\left(I_3^{\infty},d_1\right)$ 上是 *Devaney* 混沌的。

设 $U,V\subseteq I_3^{\infty}$ 且 $U,V\neq\varnothing$，对 $\chi=\{(r_n,s_n,t_n)\}_{n=0}^{\infty}\in U$ 和 $\beta=\{(u_n,v_n,w_n)\}_{n=0}^{\infty}\in V$，存在 $\theta>0$，使得 $B_\theta(\chi)=\left\{x=\{(x_n,y_n,z_n)\}_{n=0}^{\infty}\mid d(x,\chi)<\theta\right\}\subseteq U$ 和 $B_\theta(\beta)\subseteq V$。根据 $d_1$ 的定义知，存在 $M\in N_1$，满足

$$\begin{aligned}&\left\{x=\{(x_n,y_n,z_n)\}_{n=0}^{\infty}\mid x_i=r_i,y_i=s_i,z_i=t_i,i\in Z_M;x_j,y_j,z_j\in I,j\notin Z_M\right\}\subseteq B_\theta(\chi)\\&\left\{y=\{(o_n,p_n,q_n)\}_{n=0}^{\infty}\mid o_i=u_i,p_i=v_i,q_i=w_i,i\in Z_M;o_j,p_j,q_j\in I,j\notin Z_M\right\}\subseteq B_\theta(\beta)\end{aligned}\tag{11}$$

对 $x=\{(x_n,y_n,z_n)\}_{n=0}^{\infty}\in I_3^{\infty}$，记

$$G_1(x)=\{(f_0\oplus ax_{n+1},g_0\oplus by_{n+1},h_0\oplus cz_{n+1})\}_{n=0}^{\infty}=\left\{\left(x_n^{(1)},y_n^{(1)},z_n^{(1)}\right)\right\}_{n=0}^{\infty}=x^{(1)},$$

其中 $f_0,g_0,h_0$ 分别满足：$f_0(x_n,y_n,z_n)=a_{0,0}x_n\oplus a_{1,0}y_n\oplus a_{2,0}z_n$，

$g_0(x_n,y_n,z_n)=b_{0,0}y_n\oplus b_{1,0}x_n\oplus b_{2,0}z_n$，$h_0(x_n,y_n,z_n)=c_{0,0}z_n\oplus c_{1,0}x_n\oplus c_{2,0}y_n$.

由递推法可知，对 $m\in N_1$，$x=\{(x_n,y_n,z_n)\}_{n=0}^{\infty}\in I_3^{\infty}$，有

$$G_m(x)=F_m\left(x^{(m-1)}\right)=F_m\left(\cdots\left(F_1(x)\cdots\right)\right)=\left\{\left(x_n^{(m)},y_n^{(m)},z_n^{(m)}\right)\right\}_{n=0}^{\infty}=x^{(m)},\quad x^{(0)}=x,$$

其中 $G_m$ 定义由式(10)给出，且有

$$x^{(m)}=\left\{\left(f_{m-1}(\rho_n)\oplus a^m x_{n+m},g_{m-1}(\rho_n)\oplus b^m y_{n+m},h_{m-1}(\rho_n)\oplus c^m z_{n+m}\right)\right\}_{n=0}^{\infty}=\left\{x_n^{(m)}\right\}_{n=0}^{\infty}\tag{12}$$

上式中 $m,n\in N_0$，$\rho_n=(x_n,\cdots,x_{n+m-1},y_n,\cdots,y_{n+m-1},z_n,\cdots,z_{n+m-1})=\{(x_n,y_n,z_n)\}_n^{n+m-1}$，$G$ 决定了映射列 $f_{m-1}:I^{3m}\to I$、$g_{m-1}:I^{3m}\to I$ 和 $h_{m-1}:I^{3m}\to I$。

根据引理 2，对任意 $m\in N_1$ 和 $\xi\in I$，存在整数 $r,s,t\in I$，满足：

$$f_{m-1}(\rho_n)\oplus a^m r=\xi,\quad g_{m-1}(\rho_n)\oplus b^m s=\xi,\quad h_{m-1}(\rho_n)\oplus c^m t=\xi\tag{13}$$

已知 $\chi=\{(r_n,s_n,t_n)\}_{n=0}^{\infty}\in U$，$\beta=\{(u_n,v_n,w_n)\}_{n=0}^{\infty}\in V$，由式(11)、(12)、(13)知，存在 $\eta=\{(\tau_n,\sigma_n,\varsigma_n)\}_{n=0}^{\infty}\in I_3^{\infty}$，使 $\tau_n=r_n$，$\sigma_n=s_n$，$\varsigma_n=t_n$，其中 $n\in Z_M$，且 $\tau_M,\sigma_M,\varsigma_M,\cdots$ 依次满足：

$$f_{M-1}(\zeta_n)\oplus a^M\tau_{n+M}=u_n,\quad g_{M-1}(\zeta_n)\oplus b^M\sigma_{n+M}=v_n,\quad h_{M-1}(\zeta_n)\oplus c^M\varsigma_{n+M}=w_n,\quad n\in N_0$$

其中 $\zeta_n=\{(\tau_n,\sigma_n,\varsigma_n)\}_n^{n+M-1}$。故 $G_M(\eta)=F_M\circ\cdots\circ F_1(\eta)=\beta\in V$，且 $\eta\in U$。由此可见系统(8)在 $\left(I_3^{\infty},d_1\right)$ 上是传递的。同理，可以类似方法证明系统(8)在 $\left(I_3^{\infty},d_1\right)$ 上具有周期点的稠密性和初值敏感依赖性，因而系统(8)在 $\left(I_3^{\infty},d_1\right)$ 上是 Devaney 混沌的。证毕。

**例1**：设 $q=16$ 和时变离散时空系统为

$$\begin{aligned} x_{m+1,n} &= a_{0,m}x_{m,n} \oplus a_{2,m}z_{m,n} \oplus x_{m,n+1} \\ y_{m+1,n} &= b_{0,m}y_{m,n} \oplus b_{1,m}x_{m,n} \oplus 3y_{m,n+1} \\ z_{m+1,n} &= c_{0,m}z_{m,n} \oplus c_{1,m}x_{m,n} \oplus c_{2,m}y_{m,n+1} \oplus 7z_{m,n+1} \end{aligned} \tag{14}$$

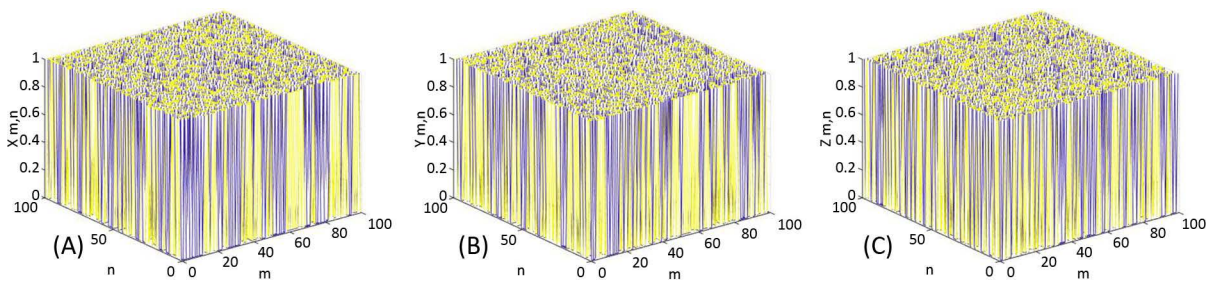
其中，$x_{0,n} \in I = \{0,1\}$，$a_{0,m} = 1+(-1)^{m \bmod 3}$，$a_{2,m} = 3+2\times(-1)^{m}$，$b_{0,m} = 1+(-1)^{(m+1) \bmod 3}$，$b_{1,m} = (m+1) \bmod 2$，$c_{0,m} = 1+(-1)^{(m+2) \bmod 3}$，$c_{1,m} = (2m) \bmod 3$，$c_{2,m} = 5+2\times\left(1+(-1)^{\bmod(m,3)}\right)$，对任意 $m,n \in N_0$。

根据现有文献无法判断系统(14)是否具有*Devaney*混沌性。但由于系统(14)是(7)的特殊情形，根据定理1，系统(14)是$\left(I_3^{\infty}, d_1\right)$上的*Devaney*混沌系统。

现对系统(14)的混沌解序列进行混乱性和自相关性仿真，图1(A)~(C)分别显示了解序列 $X,Y,Z$ 在三维空间上的混乱程度，图1(D)~(F)分别显示解序列 $X,Y,Z$ 的自相关程度。通过图1，不难发现，系统(14)的解序列都具有复杂的混乱性和良好的自相关性。同时，使用NIST推出的SP800-22软件检测包来测试解序列的伪随机性，从表1可知，均通过检测。由此可得，新系统的解序列具有良好伪随机性，可将其用于密钥流序列和流密码算法的设计之中。

**Table 1.** NIST pseudo-random sequence detection results
**表1.** NIST伪随机序列检测结果

| 检测方法 | 本符号系统*X*序列*P*值 | 本符号系统*Y*序列*P*值 | 本符号系统*Z*序列*P*值 | 检测结果 |
|---|---|---|---|---|
| Monobit test | 0.8969 | 0.1339 | 0.7609 | 通过 |
| Frequency within block test | 0.8868 | 0.0719 | 0.5109 | 通过 |
| Runs test | 0.3645 | 0.6961 | 0.0930 | 通过 |
| Longest run ones in a block test | 0.8729 | 0.7641 | 0.6173 | 通过 |
| Binary matrix rank test | 0.1412 | 0.0799 | 0.3188 | 通过 |
| Dft test | 0.9810 | 0.2139 | 0.7165 | 通过 |
| Non overlapping template matching test | 1.0000 | 1.0000 | 0.9999 | 通过 |
| Maurers universal test | 0.9997 | 0.9991 | 0.9996 | 通过 |
| Linear complexity test | 0.0114 | 0.0230 | 0.0354 | 通过 |
| Serial test | 0.5830 | 0.3818 | 0.7361 | 通过 |
| Approximate entropy test | 0.7293 | 0.3830 | 0.7341 | 通过 |
| Cumulative sums test | 0.8050 | 0.1354 | 0.8199 | 通过 |
| Random excursion test | 0.3876 | 0.3643 | 0.1665 | 通过 |
| Random excursion variant test | 0.0725 | 0.0252 | 0.2185 | 通过 |



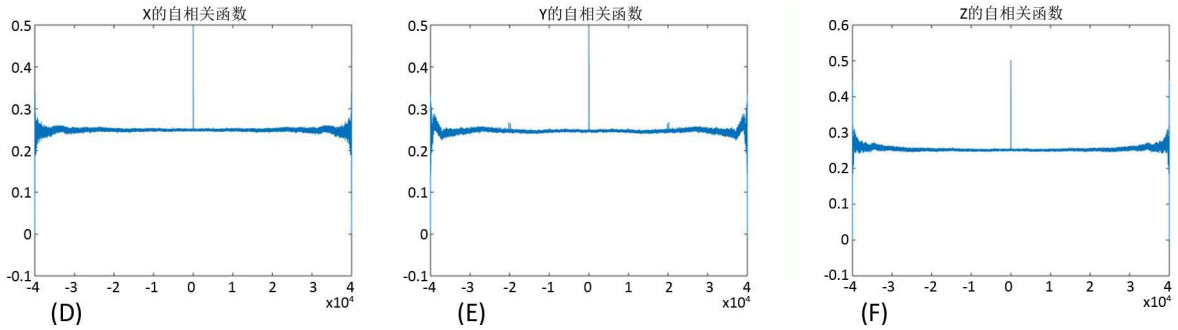



**Figure 1.** Confusion and correlation of solutions
**图 1.** 解的混乱性和自相关性

## 3. 基于拉丁方的多元流密码算法

### 3.1. 算法描述

若 $Z_n=\{0,1,\cdots,n-1\}$ 中的 $n$ 个元素在 $n$ 阶方阵 $L$ 的每行每列中都出现，则称 $L$ 为 $n$ 阶拉丁方。显然，式(15)中的矩阵是一个 16 阶拉丁方。

$$L=\begin{bmatrix} 9 & 11 & 8 & 10 & 13 & 15 & 12 & 14 & 1 & 3 & 0 & 2 & 5 & 7 & 4 & 6 \\ 11 & 9 & 10 & 8 & 15 & 13 & 14 & 12 & 3 & 1 & 2 & 0 & 7 & 5 & 6 & 4 \\ 10 & 8 & 11 & 9 & 14 & 12 & 15 & 13 & 2 & 0 & 3 & 1 & 6 & 4 & 7 & 5 \\ 8 & 10 & 9 & 11 & 12 & 14 & 13 & 15 & 0 & 2 & 1 & 3 & 4 & 6 & 5 & 7 \\ 1 & 3 & 0 & 2 & 5 & 7 & 4 & 6 & 13 & 15 & 12 & 14 & 9 & 11 & 8 & 10 \\ 3 & 1 & 2 & 0 & 7 & 5 & 6 & 4 & 15 & 13 & 14 & 12 & 11 & 9 & 10 & 8 \\ 2 & 0 & 3 & 1 & 6 & 4 & 7 & 5 & 14 & 12 & 15 & 13 & 10 & 8 & 11 & 9 \\ 0 & 2 & 1 & 3 & 4 & 6 & 5 & 7 & 12 & 14 & 13 & 15 & 8 & 10 & 9 & 11 \\ 5 & 7 & 4 & 6 & 1 & 3 & 0 & 2 & 9 & 11 & 8 & 10 & 13 & 15 & 12 & 14 \\ 7 & 5 & 6 & 4 & 3 & 1 & 2 & 0 & 11 & 9 & 10 & 8 & 15 & 13 & 14 & 12 \\ 6 & 4 & 7 & 5 & 2 & 0 & 3 & 1 & 10 & 8 & 11 & 9 & 14 & 12 & 15 & 13 \\ 4 & 6 & 5 & 7 & 0 & 2 & 1 & 3 & 8 & 10 & 9 & 11 & 12 & 14 & 13 & 15 \\ 13 & 15 & 12 & 14 & 9 & 11 & 8 & 10 & 5 & 7 & 4 & 6 & 1 & 3 & 0 & 2 \\ 15 & 13 & 14 & 12 & 11 & 9 & 10 & 8 & 7 & 5 & 6 & 4 & 3 & 1 & 2 & 0 \\ 14 & 12 & 15 & 13 & 10 & 8 & 11 & 9 & 6 & 4 & 7 & 5 & 2 & 0 & 3 & 1 \\ 12 & 14 & 13 & 15 & 8 & 10 & 9 & 11 & 4 & 6 & 5 & 7 & 0 & 2 & 1 & 3 \end{bmatrix}=\begin{bmatrix} T_0 \\ T_1 \\ T_2 \\ T_3 \\ T_4 \\ T_5 \\ T_6 \\ T_7 \\ T_8 \\ T_9 \\ T_{10} \\ T_{11} \\ T_{12} \\ T_{13} \\ T_{14} \\ T_{15} \end{bmatrix} \tag{15}$$

文献[2]举例说明了利用 4 阶拉丁方构造基本密码系统的方法。目前还没有利用更高阶拉丁方来设计基本密码系统的相关研究。下面将利用式(15)中的 16 阶拉丁方 $L$ 设计一个基本密码系统。将所有基本明文从小到大排列为一个行向量，并将拉丁方每一行作为其加密后的相应结果。例如，$L$ 的第一行所决定的置换 $T_0: M\leftrightarrow C$ 为 $0\leftrightarrow 9$、$1\leftrightarrow 11$、$2\leftrightarrow 8$、$3\leftrightarrow 10$、$\cdots$、$15\leftrightarrow 6$。

不难验证：对任意 $m=m_1m_2m_3m_4\in Z_2^4$，$T_0$、$T_3$ 的代数计算公式为

$$T_0(m)=\left(8+\left(m_3m_4+m_3+m_4+1 \bmod 4\right)+4\times m_2+8\times m_1\right) \bmod 16$$

$$T_3(m)=\left(8+m_4m_3+4\times m_2+8\times m_1\right) \bmod 16$$

类似地，$T_0\sim T_{15}$ 均能以代数式表示，它们所决定的相应基本密码系统为 $\left(M=C=K=Z_2^4,E,D\right)$，并将相应的加解密具体步骤设计如下：

1) 设任一明文$m$为二元序列$m=m_1m_2\cdots$，$m_j\in Z_2$，将该二元序列按每4比特进行分组，将分组后所得到的明文单位序列设为$\tilde{m}=\tilde{m}_1\tilde{m}_2\cdots$，其中$\tilde{m}_1=m_1m_2m_3m_4\in Z_{16}$，等等。必要时可对$m$的最后一个分组填充1而组成一个4比特分组。

2) 加密变换$E:\tilde{c}_j=E\left(k_j,\tilde{m}_j\right)$，$j=1,2,\cdots$，其中，取系统(14)的一个解序列作为16元密钥流序列$k=k_1k_2\cdots$，可得到密文单元序列$\tilde{c}=\tilde{c}_1\tilde{c}_2\cdots$。

3) 解密变换$D:\tilde{m}_j=D\left(k_j,\tilde{c}_j\right)$，$j=1,2,\cdots$，可得到明文16元序列$\tilde{m}=\tilde{m}_1\tilde{m}_2\cdots$。然后将每个明文单元$\tilde{m}_j$表示为4比特明文就得到解密后的原始二元明文序列$m=m_1m_2\cdots$。

## 3.2. 实验结果及分析

将上述密码算法用于数字图像加解密，并将它与模 2 加法流密码系统进行的比较效果可参见图 2。

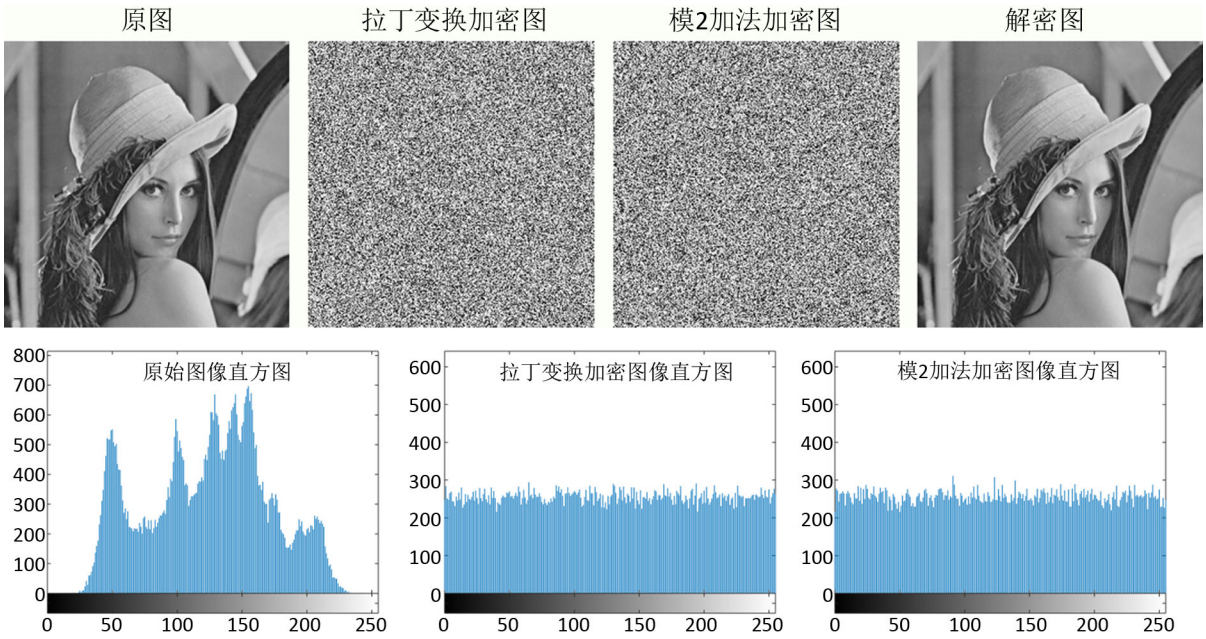



**Figure 2.** Encryption and decryption effect and gray level histogram
**图 2.** 加解密效果及灰度直方图

由图 2 可见，两种算法都能对原始图像进行有效的加解密，密文图像的灰度直方图都接近均匀分布，能抵抗统计分析。对明文图像和两种密文图像的相邻像素相关性做仿真计算，可见表 2。

**Table 2.** Correlation of each direction between adjacent pixels of 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 | 模2加法加密图 | 拉丁变换加密图 |
|---|---|---|---|
| 水平 | 0.9357 | 0.0078 | 0.0011 |
| 垂直 | 0.9682 | 0.0001 | 0.0032 |
| 对角 | 0.9084 | 0.0054 | -0.0021 |

从表中可以看出，两种密文图像相邻像素相关系数都接近 0，几乎不存在相关性。进一步，根据图像 $X$ 信息熵的定义式(16)和最大熵原理知，由于本文所选取的 Lena 图像的灰度取值范围是[0,255]，故图中各像素值等概率出现时最大信息熵达到 8。

$$H(X)=-\sum_{i=1}^{256}P(x_i)\log_2 P(x_i) \tag{16}$$

通过仿真计算，可得到原始图像信息熵为 7.4442，新流密码系统加密图像信息熵为 7.9974，模 2 加法流密码系统加密图像信息熵为 7.9969，两种密文图的熵都比明文图的熵更接近最大理想值。综上所述，拉丁方基本密码系统在实际加密中的加密效果与传统模 2 加法流密码系统加密效果相差无几，且基于拉丁方基本密码系统计算复杂度更高，因而对相应流密码算法的攻击难度更大。这说明利用高阶拉丁方设计的流密码算法具有实用价值。

## 4. 小结

本文研究了一类新时变广义符号混沌系统，基于该系统和高阶拉丁方构造了一种与传统模 2 加法不同的多比特流密码算法，通过对数字图像加解密效果的分析与对比，说明了本文提出的算法具有可行性和较高的安全性。

## 参考文献

[1] 张斌, 徐超, 冯登国. 流密码的设计与分析:回顾、现状与展望[J]. 密码学报, 2016, 3(6): 527-545.

[2] 田传俊. 密钥非均匀分布的完善保密通信系统[J]. 通信学报, 2018, 39(11): 1-9.

[3] Shannon, C.E. (1949) Communication Theory of Secrecy System. *Bell System Technical Journal*, **28**, 656-715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[4] 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.

[5] 田传俊, 林敬, 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.

[6] 田传俊, 黎杏玲, 林敬. 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.

[7] Tian, C. (2017) Chaos in the Sense of Devaney for Two-Dimensional Time-Varying Generalized Symbolic Dynamical Systems. *International Journal of Bifurcation and Chaos*, **27**, Article ID: 1750060. https://doi.org/10.1142/s0218127417500602