Computer Science and Application 计算机科学与应用, 2023, 13(1), 143-153
Published Online January 2023 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2023.131015

Hans汉斯

基于拉丁方的混沌图像加密算法设计

张　瑶，田传俊

深圳大学电子与信息工程学院，广东　深圳

收稿日期：2022年12月28日；录用日期：2023年1月24日；发布日期：2023年1月31日

摘　要

本文研究了一类二维时变离散时空系统的混沌性，并分析了它的多种伪随机性能。在此基础上，结合拉丁方构造的基本密码系统，设计了一种新的多元流密码算法。将该算法应用于数字图像加密之中，并与二元流密码系统的加密效果进行了对比。实验结果表明新算法具有足够大的密钥空间，并具有良好的加密性能和安全性。

关键词

流密码算法，基本密码系统，拉丁方，时变离散时空混沌系统

Design of a Chaotic Image Encryption Algorithm Based on Latin Squares

Yao Zhang, Chuanjun Tian

College of Electronics and Information Engineering, Shenzhen University, Shenzhen Guangdong

Received: Dec. 28th, 2022; accepted: Jan. 24th, 2023; published: Jan. 31st, 2023

Abstract

This paper studies the chaos of a class of two-dimensional time-varying discrete spatiotemporal systems and analyzes its several pseudorandom properties. On this basis, combined with a basic cipher system constructed by a Latin square, a new multi-bit stream cipher algorithm is designed out and is applied in digital image encryption. Compared with the encryption effect of the single-bit stream cipher algorithm, simulations show that the new algorithm has a large enough key space, good encryption performance and security.

文章引用: 张瑶, 田传俊. 基于拉丁方的混沌图像加密算法设计[J]. 计算机科学与应用, 2023, 13(1): 143-153.
DOI: 10.12677/csa.2023.131015

Keywords

Stream Cipher Algorithm, Basic Cryptosystem, Latin Square, Time-Varying Discrete Spatiotemporal Chaotic System

1. 引言

随着信息技术的发展，密码学已经成为防止数据泄露、保护数据安全的重要手段。流密码是密码学中常见的一种密码算法，在信息安全领域中有着广泛应用[1] [2] [3]。根据现代密码学可知，常见的流密码算法都是以模加法运算所建立的完善保密通信模型为理论基础，这导致了近几十年以来模 2 加法或 2 元加法或单比特流密码算法得到广泛研究和应用。但是，常见的二元流密码算法的基本加解密变换或运算过于简单而导致其性能存在一些不足[4] [5]。近几年中，文献[2]将模加法流密码的理论模型推广为更一般的基于拉丁方变换的理论模型，将会极大促进流密码算法的理论及其应用的研究。文献[2]明确指出流密码算法设计分为两个部分：基本系统和密钥流生成器设计(或主密钥空间设计)，且任意阶拉丁方都可用于设计基本系统，并有可能实现理想安全的完善保密通信。不难发现，二元加法流密码的基本加解密变换本质上是由 2 阶拉丁方决定的。由于拉丁方的阶数决定了基本系统的复杂度和加解密难度，因而寻求高于 2 阶或 1 比特的拉丁方基本密码系统将有利于设计出安全性更高和性能更好的密码算法。然而，当前利用高阶或多比特拉丁方来设计基本密码系统和流密码算法的研究还未充分发展，有许多问题都值得进一步研究。

另一方面，密钥流序列也会极大地影响流密码算法的安全性和性能，其中的一个关键问题是如何设计出随机性优良的密钥流生成器。一个良好的密钥流生成器应满足输出的密钥流具有较强的不可预测性以及抵抗统计分析的能力。当前，利用离散混沌系统来构造密钥流序列及其相应的流密码算法受到了广泛关注和研究。在混沌序列密码算法研究中，根据各类文献发现，离散混沌系统的构造类型多样且类随机性能优良，但对多维时变离散混沌时空系统的研究相对较少。因此，本文拟对一类二维时变离散时空系统的混沌性进行分析或研究其在流密码算法中的应用，可参见图 1。

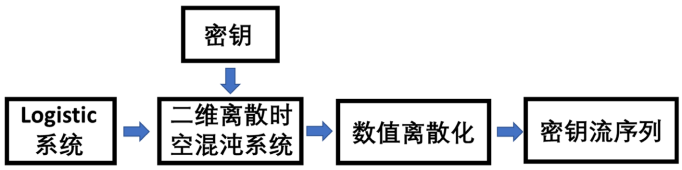


Figure 1. Schematic diagram of key flow generator based on discrete spatiotemporal system
图 1. 基于二维离散时空系统的密钥流生成器结构示意图

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，且

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

其中，$m,n\in N_0$，$f:N_0\times I^3\to I$ 和 $g:N_0\times I^3\to I$ 是两个三元函数，称 (f,g) 为系统(1-1)的系统函数。不难验证：给定两个序列 $\phi=\{\phi_{0,n}\}_{n=0}^{\infty}$ 和 $\varphi=\{\varphi_{0,n}\}_{n=0}^{\infty}$，存在一个二维离散时空序列 $z=\{(x_{m,n},y_{m,n})\}_{m,n=0}^{\infty}$ 满足(1-1)，且 $x_{0,n}=\phi_{0,n}$ 和 $y_{0,n}=\varphi_{0,n}$，$n=0,1,2,\cdots$。称 z 为系统(1-1)初值为 (ϕ,φ) 的一个解。为了方便，下面将列向量 $(a_0,a_1,\cdots)^{\mathrm{T}}$ 与行向量 $(a_0,a_1,\cdots)$ 不加区别。

记

$$I_2^{\infty}=\left\{\left\{(a_n,b_n)^{\mathrm{T}}\right\}_{n=0}^{\infty}=\begin{pmatrix}a_0 & a_1 & \cdots & a_n & \cdots\\ b_0 & b_1 & \cdots & b_n & \cdots\end{pmatrix}\middle| a_i,b_i\in I,i=0,1,2,\cdots\right\} \tag{1-2}$$

不难验证，在 I_2^{∞} 上定义一个映射 $d_1:I_2^{\infty}\times I_2^{\infty}\to I_2^{\infty}$ 可得到一个度量空间 (I_2^{∞},d_1)：

$$d_1(z_1,z_2)=\sum_{n=0}^{\infty}\frac{|x_{1,n}-x_{2,n}|+|y_{1,n}-y_{2,n}|}{2^n},\quad z_i=\{(x_{i,n},y_{i,n})\}_{n=0}^{\infty},\quad i=1,2. \tag{1-3}$$

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

$$z_m=\{(x_{m,n},y_{m,n})\}_{n=0}^{\infty},\quad m=0,1,2,\cdots \tag{1-4}$$

则系统(1-1)等价于下式(1-5)中的无穷维离散系统：

$$z_{m+1}=\{(x_{m+1,n},y_{m+1,n})=(f(m,y_{m,n},x_{m,n+1}),g(m,x_{m,n},y_{m,n+1}))\}_{n=0}^{\infty}=G_{m+1}(z_m), \tag{1-5}$$

其中，$m=0,1,2,\cdots$，$G_1,G_2,\cdots$ 是由 (f,g) 所决定的 I_2^{∞} 上的一列映射。称(1-5)或 $G=\{G_m\}_{m=0}^{\infty}$ 是由系统(1-1)或 (f,g) 所导出的离散系统或映射列。

2. 拉丁方的构造方法

下面先给出一种拉丁方的构造方法，以便为基本系统设计做好准备。

定理 2.1 设 n 是一个自然数。对任意 $m=m_1m_2\cdots m_{2n}\in Z_2^{2n}$ 和 $k=k_1k_2\cdots k_{2n}\in Z_2^{2n}$，记

$$\begin{aligned}c_{mk}&=c_1c_2c_3c_4\cdots c_{2n-1}c_{2n}\\&=E(m,k)=E(m_1m_2m_3m_4\cdots m_{2n-1}m_{2n},k_1k_2k_3k_4\cdots k_{2n-1}k_{2n})\\&=\left[m_1(\bar{m}_1\oplus m_2)m_3(\bar{m}_3\oplus m_4)\cdots m_{2n-1}(\bar{m}_{2n-1}\oplus m_{2n})\right.\\&\quad\left.+k_1(\bar{k}_1\oplus k_2)k_3(\bar{k}_3\oplus k_4)\cdots k_{2n-1}(\bar{k}_{2n-1}\oplus k_{2n})\right]\bmod 2^{2n}\\&=\left[W(m)+W(k)\right]\bmod 2^{2n}\end{aligned} \tag{2-1}$$

则 $L=(c_{mk})_{2n\times 2n}$ 是一个 $2n$ 阶拉丁方，其中，$\oplus$ 是异或运算，$\bar{a}=1-a$ 表示比特 a 的补运算，并将 $Z_{2^{2n}}$ 与 Z_2^{2n} 对应的数不加区别，且对任意 $u=u_1u_2\cdots u_{2n-1}u_{2n}\in Z_2^{2n}$，映射 $W:Z_2^{2n}\to Z_2^{2n}$ 定义为

$$W(u)=u_1(\bar{u}_1\oplus u_2)u_3(\bar{u}_3\oplus u_4)\cdots u_{2n-1}(\bar{u}_{2n-1}\oplus u_{2n})\in Z_2^{2n}.$$

证明：对任一固定的 $m\in Z_{2^{2n}}$，下面证明当 k 依次取遍 $Z_{2^{2n}}=\{0,1,2,\cdots,2^{2n}-1\}$ 中的每一个整数时，L 第 m 行的所有元素 $c_{m1},c_{m2},\cdots,c_{m,2n-1},c_{m,2n}$ 将是互不相同的整数，即为 $\{0,1,2,\cdots,2^{2n}-1\}$。否则，将存在两个不同的整数 $k=k_1k_2\cdots k_{2n}\in Z_2^{2n}$ 和 $\tilde{k}=\tilde{k}_1\tilde{k}_2\cdots\tilde{k}_{2n}\in Z_2^{2n}$，使得

$$c_{mk}=E(m,k)=E(m,\tilde{k})=c_{m\tilde{k}},$$

即 $m+k_1\left(\overline{k}_1\oplus k_2\right)\cdots k_{2n-1}\left(\overline{k}_{2n-1}\oplus k_{2n}\right)=m+\tilde{k}_1\left(\overline{\tilde{k}}_1\oplus \tilde{k}_2\right)\cdots \tilde{k}_{2n-1}\left(\overline{\tilde{k}}_{2n-1}\oplus \tilde{k}_{2n}\right)\bmod 2^{2n}$。因此，存在一个整数 r，使得 $k_1\left(\overline{k}_1\oplus k_2\right)\cdots k_{2n-1}\left(\overline{k}_{2n-1}\oplus k_{2n}\right)=\tilde{k}_1\left(\overline{\tilde{k}}_1\oplus \tilde{k}_2\right)\cdots \tilde{k}_{2n-1}\left(\overline{\tilde{k}}_{2n-1}\oplus \tilde{k}_{2n}\right)+r2^{2n}$。由于

$$0\le k_1\left(\overline{k}_1\oplus k_2\right)\cdots k_{2n-1}\left(\overline{k}_{2n-1}\oplus k_{2n}\right)<2^{2n}\text{ 和 }0\le \tilde{k}_1\left(\overline{\tilde{k}}_1\oplus \tilde{k}_2\right)\cdots \tilde{k}_{2n-1}\left(\overline{\tilde{k}}_{2n-1}\oplus \tilde{k}_{2n}\right)<2^{2n},$$

因而 $r=0$ 和 $k_1\left(\overline{k}_1\oplus k_2\right)\cdots k_{2n-1}\left(\overline{k}_{2n-1}\oplus k_{2n}\right)=\tilde{k}_1\left(\overline{\tilde{k}}_1\oplus \tilde{k}_2\right)\cdots \tilde{k}_{2n-1}\left(\overline{\tilde{k}}_{2n-1}\oplus \tilde{k}_{2n}\right)$。于是，依次可推出

$$k_1=\tilde{k}_1,\ \left(\overline{k}_1\oplus k_2\right)=\left(\overline{\tilde{k}}_1\oplus \tilde{k}_2\right),\ \cdots,\ k_{2n-1}=\tilde{k}_{2n-1},\ \left(\overline{k}_{2n-1}\oplus k_{2n}\right)=\left(\overline{\tilde{k}}_{2n-1}\oplus \tilde{k}_{2n}\right).$$

这样就有 $k_1=\tilde{k}_1$，$k_2=\tilde{k}_2$，$\cdots$，$k_{2n-1}=\tilde{k}_{2n-1}$，$k_{2n}=\tilde{k}_{2n}$，即 $k=\tilde{k}$，矛盾！由此证明了方阵 L 的每一行取遍 $Z_{2^{2n}}=\left\{0,1,2,\cdots,2^{2n}-1\right\}$ 中的每一个整数。类似可证明 L 的每一列也取遍 $Z_{2^{2n}}$ 中的每一个整数。因此，L 是一个 $2n$ 阶拉丁方。证毕！

由定理 2.1 可知，当 $n=4$ 时可得到如下 2^8 阶拉丁方 L：

$$L=\begin{bmatrix} 84 & 83 & 82 & & 167 & 166 & 169 \\ 83 & 82 & 81 & \cdots & 166 & 165 & 168 \\ 82 & 81 & 80 & & 165 & 164 & 167 \\ \vdots & & & \ddots & & \vdots & \\ 167 & 166 & 165 & & 250 & 249 & 252 \\ 166 & 165 & 164 & \cdots & 249 & 248 & 251 \\ 169 & 168 & 167 & & 252 & 251 & 254 \end{bmatrix},\quad H=\begin{bmatrix} 0 & 128 & 64 & & 191 & 127 & 255 \\ 1 & 129 & 65 & \cdots & 190 & 126 & 254 \\ 2 & 130 & 66 & & 189 & 125 & 253 \\ \vdots & & & \ddots & & \vdots & \\ 253 & 125 & 189 & & 66 & 130 & 2 \\ 254 & 126 & 190 & \cdots & 65 & 129 & 1 \\ 255 & 127 & 191 & & 64 & 128 & 0 \end{bmatrix}$$

其中，方阵是文献[6]中所构造的 2^8 阶拉丁方，且 L 比 H 的构造方法要更复杂一些。本文将基于 L 所设计的基本密码系统设为 (M,K,C,E,D)，其中，L 的第 k 行是将基本明文空间 $M=\{0,1,\cdots,255\}$ 依次作加密变换所得到的基本密文单元，即对任一 $m\in M$，按照式(2-1)中当 $n=4$ 时的公式加密可得到密文 $c=E(m,k)$，且基本解密变换如下：对任意 $u=u_1u_2\cdots u_7u_8\in Z_2^8$，

$$m_{mk}=D(m,k)=W\left[\left(c-W(k)\right)\bmod 256\right],\ W(u)=u_1\left(\overline{u}_1\oplus u_2\right)\cdots u_7\left(\overline{u}_7\oplus u_8\right)\in Z_2^8.$$

3. 新混沌离散系统及其伪随机性分析

设 $I=[0,1)$，并定义两个函数 $f:N_0\times I^3\to I$ 和 $g:N_0\times I^3\to I$：

$$f(m,y,x)=\left\langle s_m y^2+a_m x\right\rangle\text{ 和 }g(m,x,y)=\left\langle t_m x^2+b_m y\right\rangle,\tag{3-1}$$

其中，$\{a_m\}_{m=0}^{\infty}$，$\{b_m\}_{m=0}^{\infty}$，$\{s_m\}_{m=0}^{\infty}$ 和 $\{t_m\}_{m=0}^{\infty}$ 都是周期数列，即存在正整数 p，使得 $a_m=a_{m+p}$，$b_m=b_{m+p}$，$s_m=s_{m+p}$ 和 $t_m=t_{m+p}$，对一切 $m\in\{0,1,2,\cdots\}$，且 $\langle u\rangle$ 表示实数 u 的小数。

不难发现，上述映射 (f,g) 可产生如下的二维时变离散时空系统

$$\begin{cases} x_{m+1,n}=f\left(m,y_{m,n},x_{m,n+1}\right)=\left\langle s_m y_{m,n}^2+a_m x_{m,n+1}\right\rangle \\ y_{m+1,n}=g\left(m,x_{m,n},y_{m,n+1}\right)=\left\langle t_m x_{m,n}^2+b_m y_{m,n+1}\right\rangle \end{cases}\tag{3-2}$$

其中，$x_{m,n},y_{m,n}\in I=[0,1)$，对任一 $m,n=0,1,2,\cdots$。参照现有文献可以发现，该二维时变离散时空系统(3-2)的 *Devaney* 混沌性还没有被研究过。参照系统(1-1)和系统(1-5)之间的关系可知，系统(3-2)会等价于如下离散系统：对 $z=\left\{\left(x_{m,n},y_{m,n}\right)\right\}_{m,n=0}^{\infty}\in I_2^{\infty}$，

$$z_{m+1}=\left\{\left(x_{m+1,n},y_{m+1,n}\right)=\left(\left\langle s_m y_{m,n}^2+a_m x_{m,n+1}\right\rangle,\left\langle t_m x_{m,n}^2+b_m y_{m,n+1}\right\rangle\right)\right\}_{n=0}^{\infty}=G_{m+1}\left(z_m\right),\tag{3-3}$$

其中，$G_{m+1}:I_2^{\infty}\to I_2^{\infty}$ 是由 f 和 g 决定的映射，即对任一 $\beta=\left\{\left(u_m,v_m\right)\right\}_{m=0}^{\infty}\in I_2^{\infty}$，都有

$$G_{m+1}\left(\beta\right)=\left\{\left\langle s_m v_n^2+a_m u_{n+1}\right\rangle,\left\langle t_m u_n^2+b_m v_{n+1}\right\rangle\right\}_{n=0}^{\infty},\ m=1,2,\cdots.\tag{3-4}$$

参照文献[7] [8] [9] [10]，易得如下引理及推论。

引理 3.1 式(3-3)中映射列 $G=\left\{G_m\right\}_{m=1}^{\infty}$ 是周期为 p 的周期序列，即 $G_m=G_{m+p}$，$m=1,2,\cdots$。而且，对一切 $m,s,t\in N_1$，都有

$$G_{s+mp-1}\circ G_{s+mp-2}\circ\cdots\circ G_s=G_{t+mp-1}\circ G_{t+mp-2}\circ\cdots\circ G_t.$$

记式(3-3)定义的映射列 $G=\left\{G_m\right\}_{m=1}^{\infty}$ 所确定的复合映射为

$$H_m=G_m\circ G_{m-1}\circ\cdots\circ G_1,\ m=1,2,\cdots.\tag{3-5}$$

引理 3.2 对任一给定的常数 $c_m\geq 1$，$h,r\in I$ 和 $m=1,2,\cdots$，存在 $u\in I$，使得 $\left\langle h+c_m u\right\rangle=r$。

定义 3.1 若式(1-1)的系统函数 $\left(f,g\right)$ 所确定的映射列 $G=\left\{G_m\right\}_{m=1}^{\infty}$ 或系统(1-5)在度量空间 $\left(I_2^{\infty},d_1\right)$ 上具有传递性、周期点的稠密性和初值敏感依赖性，则称 $G=\left\{G_m\right\}_{m=1}^{\infty}$ 或系统(1-5)是 *Devaney* 混沌的，也称与系统(1-5)相应的等价系统(1-1)在 $\left(I_2^{\infty},d_1\right)$ 上是 *Devaney* 混沌的。

定理 3.1 在上述条件下，离散系统(3-2)是 $\left(I_2^{\infty},d_1\right)$ 上的 *Devaney* 混沌系统。

证明：由定义 3.1 可知，只需证明系统(3-3)在 $\left(I_2^{\infty},d_1\right)$ 上是 *Devaney* 混沌的，即该系统具有周期点的稠密性、传递性和初值的敏感依赖性。首先将证明该系统具有周期点的稠密性。

对于给定的任一点 $\alpha=\left\{\left(u_n,v_n\right)\right\}_{n=0}^{\infty}\in I_2^{\infty}$ 和 α 的任一邻域 $U\subseteq I_2^{\infty}$，都存在 $\delta>0$，使得

$$B_{\delta}\left(\alpha\right)=\left\{x=\left\{\left(x_n,y_n\right)\right\}_{n=0}^{\infty}\in I_2^{\infty}\mid d_1\left(x,\alpha\right)<\delta\right\}_{n=0}^{\infty}\subseteq U.$$

根据式(1-3)中 d_1 的定义知，存在整数 $M\in\left\{1,2,\cdots\right\}$，使得

$$\left\{x=\left\{\left(x_n,y_n\right)\right\}_{n=0}^{\infty}\in I_2^{\infty}\mid x_i=u_i,y_i=v_i;i=0,1,\cdots,M-1;\forall x_j,y_j\in I,j\geq M\right\}_{n=0}^{\infty}\subseteq B_{\delta}\left(\alpha\right)\tag{3-6}$$

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

$$H_1\left(x\right)=G_1\left(x\right)=\left\{\left(x_n^{(1)},y_n^{(1)}\right)=\left(\left\langle s_0 y_n^2+a_0 x_{n+1}\right\rangle,\left\langle t_0 x_n^2+b_0 y_{n+1}\right\rangle\right)\right\}_{n=0}^{\infty}=x^{(1)},$$

$$H_2\left(x\right)=G_2\left(x^{(1)}\right)=\left\{\left(x_n^{(2)},y_n^{(2)}\right)=\left(\left\langle s_1\left(y_n^{(1)}\right)^2+a_1 x_{n+1}^{(1)}\right\rangle,\left\langle t_1\left(x_n^{(1)}\right)^2+b_1 y_{n+1}^{(1)}\right\rangle\right)\right\}_{n=0}^{\infty}=x^{(2)},$$

其中，$x_n^{(2)}=\left\langle s_1\left(t_0 x_n^2+b_0 y_{n+1}\right)^2+a_1 s_0 y_{n+1}^2+a_1 a_0 x_{n+2}\right\rangle=\left\langle f_1\left(x_n,x_{n+1},y_n,y_{n+1}\right)+a_1 a_0 x_{n+2}\right\rangle$，且

$$f_1\left(x_n,x_{n+1},y_n,y_{n+1}\right)=\left\langle s_1\left(t_0 x_n^2+b_0 y_{n+1}\right)^2+a_1 s_0 y_{n+1}^2\right\rangle,$$

以及 $y_n^{(2)}=\left\langle g_1\left(y_n,y_{n+1},x_n,x_{n+1}\right)+b_1 b_0 y_{n+2}\right\rangle$ 和 $g_1\left(y_n,y_{n+1},x_n,x_{n+1}\right)=\left\langle t_1\left(s_0 y_n^2+a_0 x_{n+1}\right)^2+b_1 t_0 x_{n+1}^2\right\rangle$。

由递推法可知，对任意 $m=1,2,\cdots$ 和 $x=\left\{\left(x_n,y_n\right)\right\}_{n=0}^{\infty}\in I_2^{\infty}$，有

$$H_m(x)=G_m\left(x^{(m-1)}\right)=G_m\circ\cdots\circ G_1(x)=\left\{\left(x_n^{(m)},y_n^{(m)}\right)\right\}_{n=0}^{\infty}=x^{(m)},$$

其中，$f_m\left(x_n,\cdots,x_{n+m},y_n,\cdots,y_{n+m}\right)=f_m\left(\lambda_n\right)$ 和 $g_m\left(y_n,\cdots,y_{n+m},x_n,\cdots,x_{n+m}\right)=g_m\left(\rho_n\right)$ 是两个多元函数，$\lambda_n=\left(x_n,\cdots,x_{n+m},y_n,\cdots,y_{n+m}\right)$ 和 $\rho_n=\left(y_n,\cdots,y_{n+m},x_n,\cdots,x_{n+m}\right)$，且

$$x^{(m+1)}=\left\{\left(\left\langle f_m\left(\lambda_n\right)+a_m\cdots a_0x_{n+m+1}\right\rangle,\left\langle g_m\left(\rho_n\right)+b_m\cdots b_0y_{n+m+1}\right\rangle\right)\right\}_{n=0}^{\infty}. \tag{3-7}$$

由已知条件可知，对任一 $m=1,2,\cdots$，都有 $a_m\cdots a_0\geq 1$ 和 $b_m\cdots b_0\geq 1$。由引理 3.2，对任一固定的 $\eta\in I$，$\lambda,\rho\in I^{2(m+1)}$ 和 $m=1,2,\cdots$，都存在实数 $c=c_m,e=e_m\in I$，使得

$$\left\langle f_m\left(\lambda\right)+a_m\cdots a_0c\right\rangle=\eta \text{ 和 } \left\langle g_m\left(\rho\right)+b_m\cdots b_0e\right\rangle=\eta. \tag{3-8}$$

对于 $\alpha=\left\{\left(u_n,v_n\right)\right\}_{n=0}^{\infty}\in U$，由式(3-6)、(3-7)、(3-8)，存在一点 $\beta=\left\{\left(\sigma_n,\tau_n\right)\right\}_{n=0}^{\infty}\in U$，使得 $\sigma_n=u_n,\tau_n=v_n$，$n=0,1,\cdots,M-1$，且 $\sigma_M,\tau_M,\sigma_{M+1},\tau_{M+1},\cdots$ 依次满足：

$$\left\langle f_{M-1}\left(\lambda_n\right)+a_M\cdots a_0\sigma_{n+M+1}\right\rangle=\sigma_n,\ \left\langle g_{M-1}\left(\rho_n\right)+b_M\cdots b_0\tau_{n+M+1}\right\rangle=\tau_n,\ n=0,1,2,\cdots.$$

因此，$H_M\left(\beta\right)=G_M\circ\cdots\circ G_1\left(\beta\right)=\beta\in V$ 和 $\beta\in U$，即 β 是 $G=\left\{G_m\right\}_{m=1}^{\infty}$ 的一个周期点。于是，系统(3-3)在 $\left(I_2^{\infty},d_1\right)$ 上具有周期点的稠密性。同样地，可利用与上述类似的方法证明系统(3-3)还具有传递性和初值敏感依赖性。故系统(3-3)在 $\left(I_2^{\infty},d_1\right)$ 上是 *Devaney* 混沌的。证毕！

例1：设二维时变离散时空系统为

$$\begin{cases}x_{m+1,n}=f\left(m,y_{m,n},x_{m,n+1}\right)=\left\langle 4y_{m,n}^2+a_mx_{m,n+1}\right\rangle\\ y_{m+1,n}=g\left(m,x_{m,n},y_{m,n+1}\right)=\left\langle 4x_{m,n}^2+b_my_{m,n+1}\right\rangle\end{cases} \tag{3-9}$$

其中，$a_m=3+\left(-1\right)^m$ 和 $b_m=3+\left(-1\right)^{m+1}$，对任意 $m=0,1,2,\cdots$。

基于现有文献无法断定上述系统是否具有*Devaney*混沌性。但由于该系统是(3-2)的特殊情形，结合定理3.1可知，该系统是 $\left(I_2^{\infty},d_1\right)$ 上的*Devaney*混沌系统。

下面通过 SP800-22Rvlla 标准系统检验例 1 系统混沌解序列的伪随机性能，其中，SP800-22Rvlla 标准由美国国家标准技术研究所提出的专门针对随机数或伪随机数发生器产生的二进制随机序列的统计测试法。对长度为 1×10^6 的混沌序列进行伪随机性检验，设置比特序列长度为 10^6，显著性水平为 0.01，当测试 p 值大于显著性水平时，检验通过，测试结果见表 1，且混乱性可见图 2。

Table 1. Test results of SP800-22Rvlla
表 1. SP800-22Rvlla 测试结果

测试方法	P值	测试结果
Approximate Entropy	0.0930	通过
Block Frequency	0.2779	通过
Cumulative Sums	0.0180	通过
FFT	0.7550	通过
Frequency	0.0194	通过
Linear Complexity	0.4882	通过
Longest Run	0.0751	通过
Non Overlapping Template	0.4914	通过

Continued

Overlapping Template	0.2427	通过
Random Excursions	0.6105	通过
Random Excursions Variant	0.5293	通过
Rank	0.2576	通过
Runs	0.4560	通过
Serial	0.2563	通过
Universal	0.7750	通过

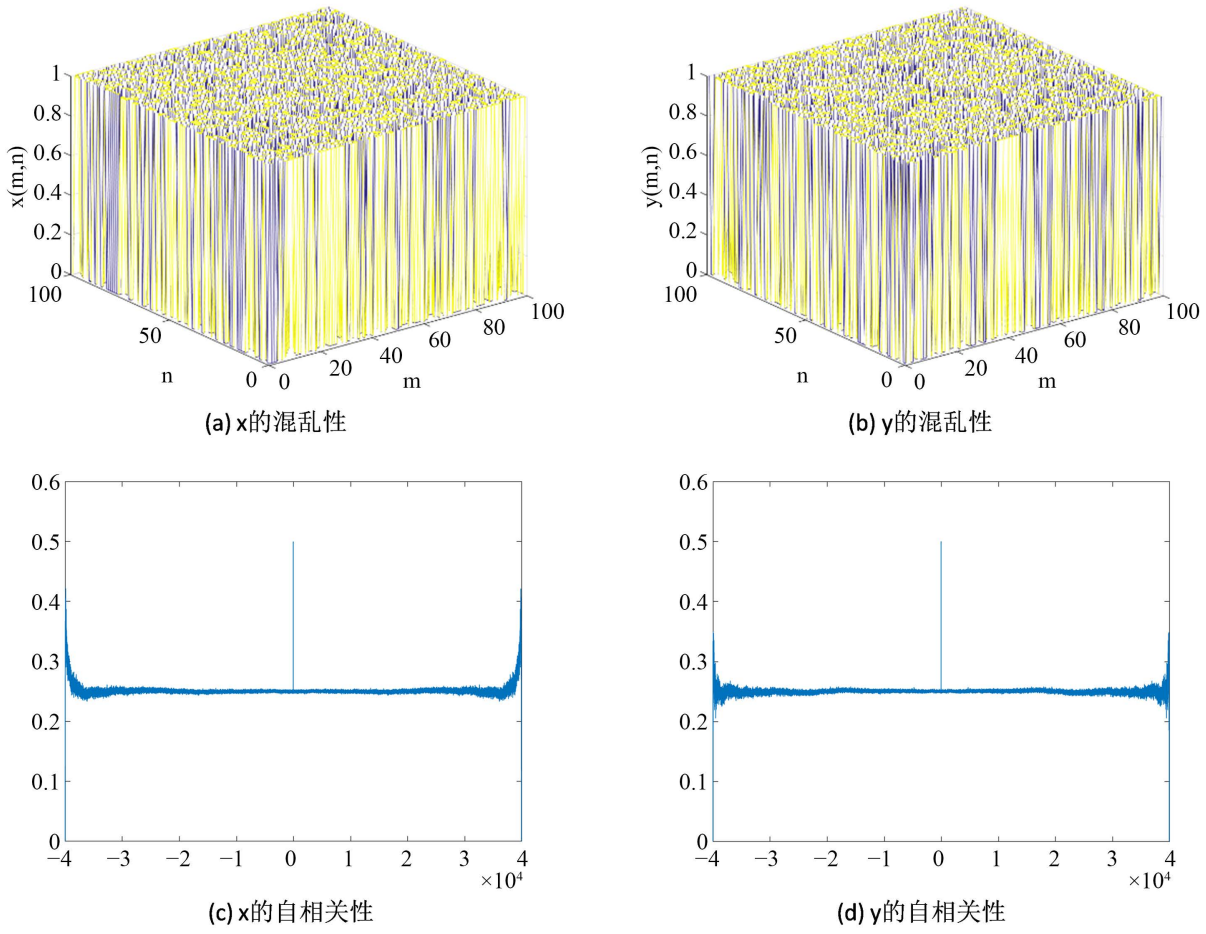


Figure 2. Confusion and autocorrelation of solutions
图 2. 解的混乱性和自相关性

4. 基于拉丁方的多比特流密码算法

4.1. 算法描述

先将基本系统设计为上述 8 比特的拉丁方基本系统$\left(M=C=K=Z_2^8,E,D\right)$，再结合定理 3.1，将完整的加解密变换具体设计如下：

1) 取一幅数字图像作为明文m (如Lena图像)，并将m转换为二元序列 $m=m_1m_2\cdots$， $m_j\in Z_2$，将该二元序列按每8比特进行分组，将分组后得到的明文单元序列设为 $\tilde{m}=\tilde{m}_1\tilde{m}_2\cdots$，其中 $\tilde{m}_1=m_{11}m_{12}\cdots m_{18}\in Z_2^8$，

等等。必要时可对m的最后一个分组填充而组成一个8比特分组。

2) 加密变换E：$\tilde{c}_j = E\left(\tilde{k}_j, \tilde{m}_j\right)$，$j = 1,2,\cdots$，其中，将系统(3-9)的一个解序列作为256元密钥流序列$\tilde{k} = \tilde{k}_1\tilde{k}_2\cdots$，可得到256元密文单元序列$\tilde{c} = \tilde{c}_1\tilde{c}_2\cdots$。

3) 解密变换D：$\tilde{m}_j = D\left(\tilde{k}_j, \tilde{c}_j\right)$，$j = 1,2,\cdots$，可得到明文256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8比特明文分组就得到解密后的原始二元明文序列$m = m_1m_2\cdots$。最后可恢复出原数字图像m。

4.2. 实验结果及分析

将上述流密码算法用于数字图像加解密，从直方图、相邻像素相关性、密钥敏感性以及信息熵四个方面将它与单比特流密码系统进行比较，仿真效果一一介绍如下。

4.2.1. 直方图分析

直方图可以直观地反映一幅图像的像素值分布特征。如果密文图像的像素值分布越均匀，那么其抵抗统计攻击的能力越强，算法的安全性越高。在 Matlab 中，两种流密码算法仿真的加解密效果图及直方图如下图 3 所示：

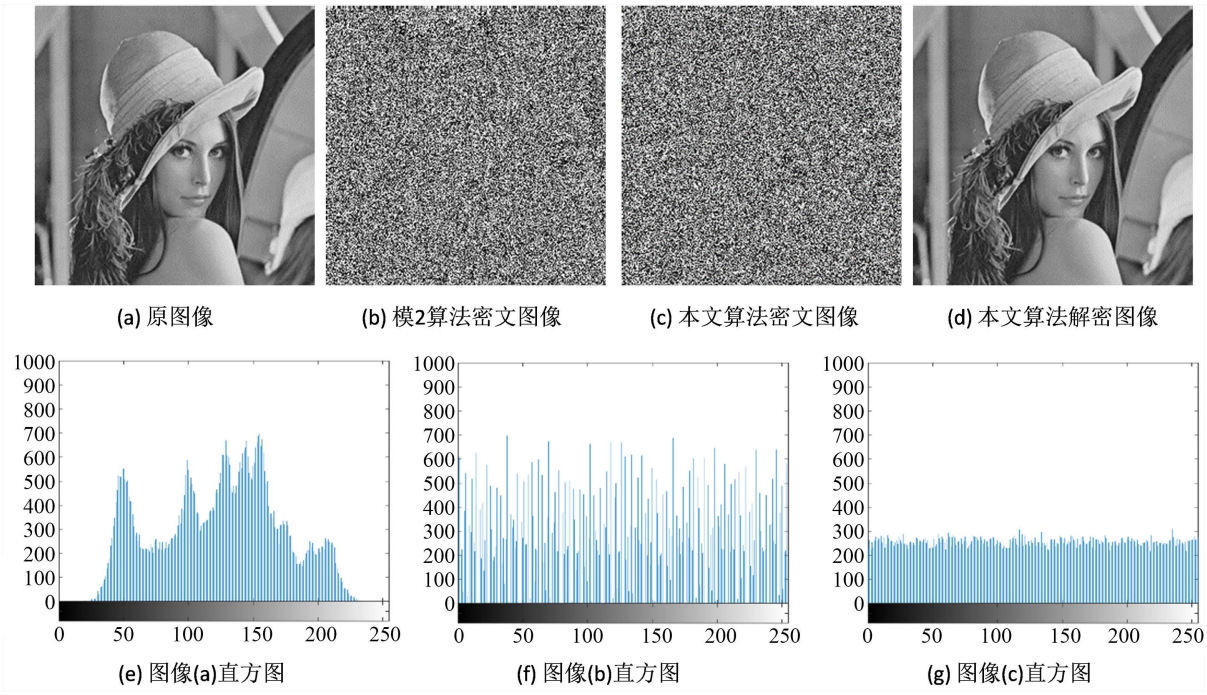


Figure 3. Simulation renderings of two algorithms
图 3. 算法仿真效果图

模 2 加法或单比特流密码算法密文图像的像素分布区间为[0, 255]，分布近似呈现周期性或不具有均匀分布，且周期内分布杂乱；密文图像(d)的像素在区间[0, 255]接近均匀分布。因此，与单比特算法密文图像相比，本加密算法加密后的统计特性更好，因而抵抗统计攻击的能力会更强。

4.2.2. 相邻像素相关性分析

像素相关性表示一幅图像中相邻像素之间的关联程度。当数字图像的原图或加密图像相邻像素点之间有较高相关性时，可利用相邻像素预测该点的像素值，进而有可能获取图像信息。可靠的加密算法应

保证加密之后的密文图像具有足够弱的像素相关性。衡量图像相邻像素间的相关性主要有定性和定量两种方法：定性的方法是指从水平、垂直以及对角三个方向上直观地显示像素相关性分布图；定量的方法可通过计算相邻像素的相关系数，可利用该量化指标进行衡量。

从 Lena 原图像和两种加密算法得到的密文图像中随机选取 4000 相邻像素对，并从水平、垂直以及对角三个方向绘制像素分布图，结果见图 4。

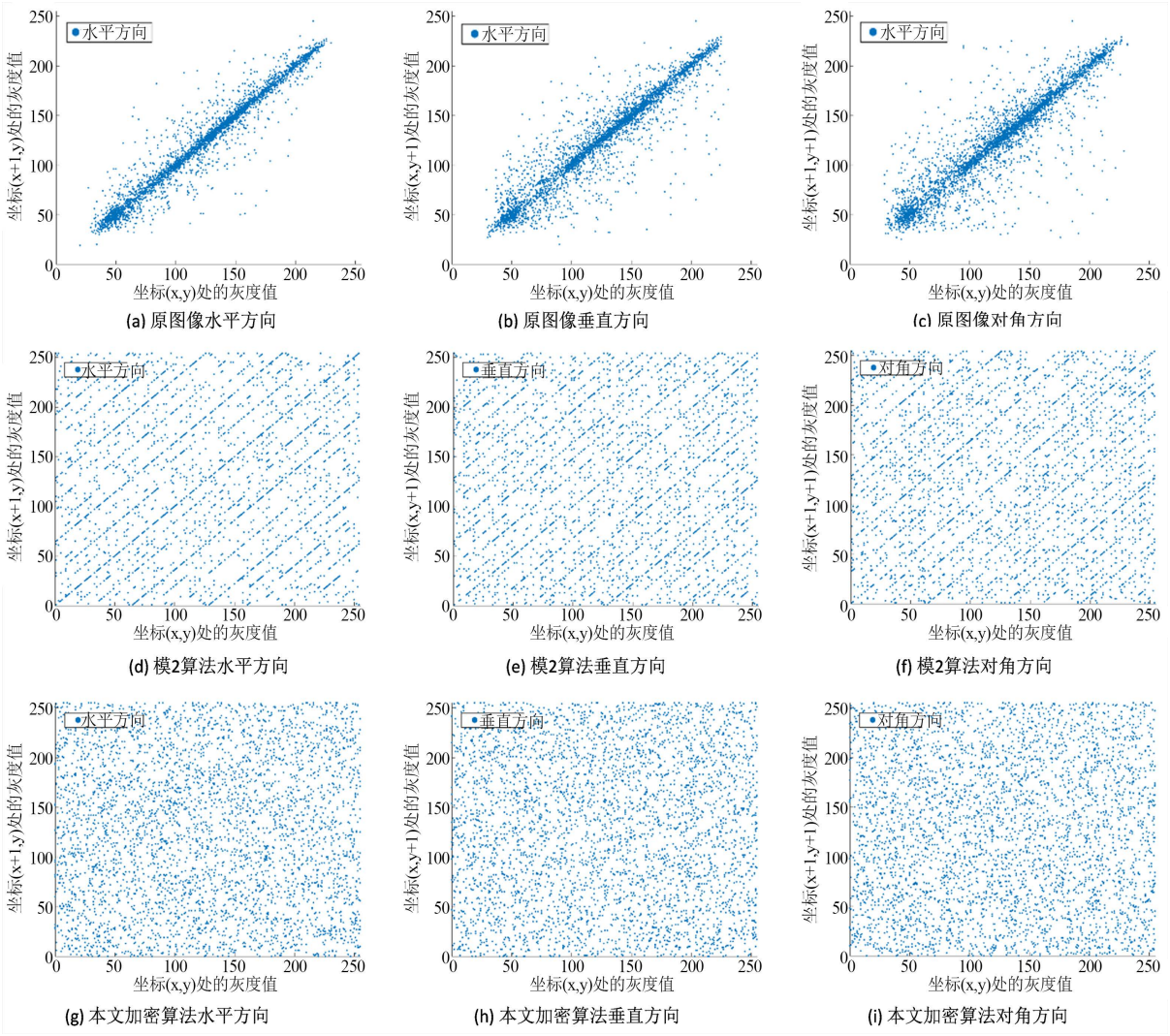


Figure 4. Pixel correlation distribution
图 4. 像素相关性分布图

从像素间相关性分布图来看，原图像的像素点在水平、垂直和对角方向上都分布在对角线附近，表明这些方向上相邻像素间的相关性较强；模 2 算法的密文图像像素点分布在 250 × 250 整个平面区域内，但像素点在 45˚方向上表现出较强的线性关系；本文算法的密文图像像素点在整个区域内均匀分布，相邻像素点的相关性大大减弱，可较好地掩盖原始图像的相关特征。

为定量测试密文图像的相邻像素相关性，在图像各个方向上选取 4000 个相邻像素点，根据下面的式(4-1)和(4-2)计算 100 组相邻像素的相关系数，其均值结果如表 2 所示。

$$r_{xy}=\frac{cov(x,y)}{\sqrt{D(x)}\times\sqrt{D(y)}} \tag{4-1}$$

$$\begin{cases} cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)\left(y_i-E(y)\right) \\ E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \\ D(x)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)^2 \end{cases} \tag{4-2}$$

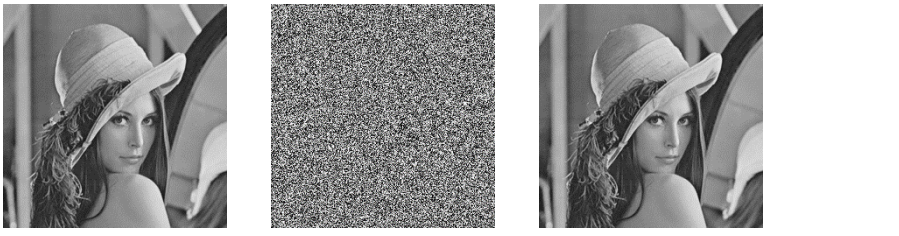
Table 2. Correlation simulation data
表 2. 相关性仿真数据

方向	明文图像	模 2 加法算法	本文算法
水平方向	0.9698	0.0367	0.0001
竖直方向	0.9365	0.0261	0.0004
对角方向	0.9137	0.0016	−0.0015

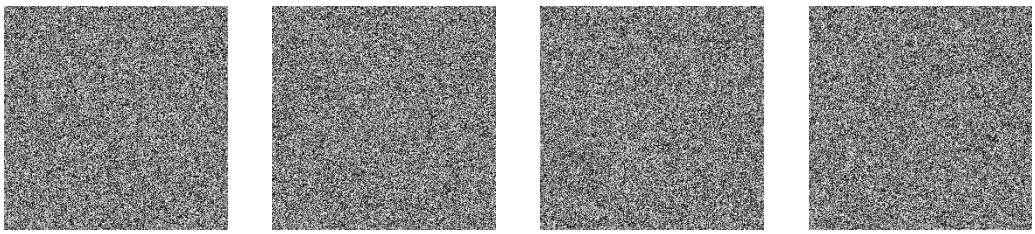
对比单比特流密码算法得到的密文图像，本文加密算法得到的密文图像在各个方向上的相邻像素相关系数都更接近 0，几乎不存在相关性。

4.2.3. 密钥敏感性

一个好的加密算法应对密钥的变化极其敏感。当密钥仅发生微小变化时，也无法还原出明文图像。为了评估本文所提出的加密算法的密钥敏感度，利用单一变量法，每次仅改变密钥 x_0、y_0、u_1 和 u_2 其中一个密钥值，改动幅度为 1×10^{-14}，得到 key1、key2、key3 和 key4 四个新密钥。当攻击方获取原密钥加密的原加密图像后，分别利用四个微小改变的新密钥对原加密图像进行解密也无法恢复出明文图像，且解密图像中无有效信息。因此，本文加密系统具有良好的密钥敏感性，可保证密钥空间具有足够多的密钥量(图 5)。



(a) 原始图像　(b) 密文图像　(c) 原密钥的解密图像



(d) key1 的解密图像　(e) key2 的解密图像　(f) key3 的解密图像　(g) key4 的解密图像

Figure 5. Key sensitivity test
图 5. 密钥敏感性测试

4.2.4. 信息熵分析

信息熵为图像所含信息量，可以反映图像的随机性或不确定性。一幅图像的不确定性越强，信息量越大，且信息熵越大。根据图像信息熵的计算公式(4-3)和最大熵原理[11], 当图像灰度值范围为[0, 255]时，理论最大信息熵达到 8。明文图像和密文图像的信息熵结果如表 3 所示。

$$H(x)=-\sum_{i=1}^{256}P(x_i)\log_2 P(x_i) \tag{4-3}$$

其中，$x_i=i$，$P(x_i)$为像素 x_i 出现的概率。

Table 3. Comparison of information entropy
表 3. 信息熵对比结果

	明文图像	模 2 加法加密图像	本文算法加密图像
信息熵	7.4442	7.4442	7.9971

明文图像和单比特流加密算法得到的密文图像信息熵均为 7.4442，而本文加密算法得到的密文图像信息熵为 7.9971，接近理想值 8。因此，本文加密算法可以更好地抵御信息熵的攻击，具有更好的加密性能。

5. 小结

本文构建了一类新的时变离散时空混沌系统，基于该系统和高阶拉丁方构造了与常见模2加法或1比特流密码算法明显不同的一种多比特流密码算法。通过对数字图像加解密的多种效果分析与对比，验证了本文提出的算法具有可行性和良好的性能与安全性，具有一定的实际应用参考价值。不过，也要指出：复杂度适中的拉丁方及其变换组的流密码系统性构造方法还值得今后进一步研究。

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. *The Bell System Technical Journal*, **28**, 656-715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[4] 杨轶, 荣锋, 武志刚. 改进混沌方程及其在保密 VoIP 系统中的应用与实现[J]. 电讯技术, 2022, 62(7): 971-977.

[5] 严利民, 葛雨阳, 石磊. 混沌映射和流密码结合的图像加密算法仿真[J]. 计算机仿真, 2020, 37(3): 264-269.

[6] 李熙, 田传俊. 基于拉丁方的流密码算法设计与仿真[J]. 计算机科学与应用, 2020, 10(11): 1938-1943.

[7] 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.

[8] 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.

[9] 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.

[10] 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**, 1750060. https://doi.org/10.1142/S0218127417500602

[11] 刘为超, 刘义沛. 基于 Logistic 混沌置乱的图像加密算法[J]. 科学技术创新, 2020(36): 125-126.