Computer Science and Application 计算机科学与应用, 2020, 10(10), 1706-1713
Published Online October 2020 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2020.1010181

Hans汉斯

基于正交拉丁方的混沌图像加密算法设计

林泽森，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9月30日；录用日期：2020年10月15日；发布日期：2020年10月22日

摘 要

本文构造了一个8阶正交拉丁方组及其所决定的可逆变换的代数式，给出了基于该正交拉丁方组的基本密码系统的设计方法。在此基础上，结合Henon混沌系统设计了一种多元流密码算法，推广了二元加法流密码的设计方法，并对新流密码算法在数字图像上的加密效果进行了直方图、相关性、密钥敏感度及信息熵等分析，结果表明该加密算法具有良好的加密效果。

关键词

流密码算法，图像加密，正交拉丁方，基本密码系统，混沌系统

Design of Chaotic Image Encryption Algorithm Based on Orthogonal Latin Square

Zesen Lin, Chuanjun Tian

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

Received: Sep. 30th, 2020; accepted: Oct. 15th, 2020; published: Oct. 22nd, 2020

Abstract

This paper constructs an 8th-order orthogonal Latin square group and the algebraic formula of the reversible transformation determined by it, and gives the design method of the basic cryptographic system based on the orthogonal Latin square group. On this basis, a multi-ary stream cipher algorithm is designed in combination with the Henon chaotic system, the design method of

文章引用: 林泽森, 田传俊. 基于正交拉丁方的混沌图像加密算法设计[J]. 计算机科学与应用, 2020, 10(10): 1706-1713. DOI: 10.12677/csa.2020.1010181

binary additive stream cipher is promoted, and the encryption effect of the new stream cipher algorithm on digital images is carried out by histogram, correlation, etc. Simulations show that the encryption algorithm has a good encryption effect.

Keywords

Stream Cipher Algorithm, Image Encryption, Orthogonal Latin Square, Basic Cryptosystem, Chaotic System

1. 引言

流密码算法作为一类重要的密码体制是当前密码学的热门研究问题之一，也是信息安全领域的基础内容之一，在数字信息加密领域得到广泛应用[1] [2] [3]。自 1949 年 Shannon 提出完善保密系统模型以来[2]，已有不少学者对其相关的理论模型和实际应用进行了研究[3] [4]。当前，普遍认为完善保密系统模型是流密码算法的理论基础，其中，常见的二元流密码算法是基于模 2 加法运算来进行设计的，它所使用的基本运算过于简单，这会影响整个算法的加密效果和安全性。最近的文献[3]推广了现有的完善保密系统模型，将流密码系统设计分为基本密码系统设计和应用密码系统设计，其中的一个关键是将常见的二元加法密码系统中的模 2 加法基本系统推广为一般的拉丁方基本系统。这样，与以前的基本系统设计相比，该模型最大的特点在于所能设计的基本系统的种类更加丰富、设计技巧更加灵活，并且能够有效地提高算法的复杂度。当前，已有文献[4]专门研究了 4 阶正交拉丁方组基本系统的设计方法，但尚未有文献对利用更高阶的正交拉丁方组设计基本密码系统的方法进行讨论。因此，本文将研究利用 8 阶正交拉丁方组设计基本密码系统的方法，并结合 Henon 混沌系统研究一种新的混沌流密码系统的设计与实现问题。

1997 年，Fridrich 首次将混沌系统应用到数字图像加密中[5]。此后，因混沌系统具有初值敏感性和类随机性等特点，故在信息加密领域中得到广泛应用。由于一维混沌系统具有初始可控参数少，生成的序列随机性较差等缺点，因此，现在常用更高维的混沌系统来设计安全性更高的密码算法[6]。本文将先利用 8 阶正交拉丁方组设计一个基本系统，之后再结合二维 Henon 混沌系统所设计的密钥序列空间来完成整个流密码算法的设计。

2. Henon 系统

考虑到混沌系统所具有的初值敏感性和伪随机性等特点，本文将具体利用 Henon 混沌系统进行密钥序列空间的设计，简要介绍如下。

Henon 映射是一类二维非线性混沌系统，其映射方程[7]如下：

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \tag{1}$$

其中， a, b 为控制参数，取 $a = 1.4, b = 0.3, x_0, y_0 \in (0,1)$ 时，整个系统处于混沌状态[7]。为方便实际应用，还需用对混沌解序列进行某种变换，如取模运算等。

3. 基于正交拉丁方的流密码算法设计

3.1. 基本密码系统设计

在基本密码系统设计时需要利用拉丁方，介绍如下。

定义 3.1 若存在 $n(n\geq 2)$ 阶方阵 A，使得 $Z_n=\{0,1,\cdots,n-1\}$ 上每个元素在 A 的每一行和每一列里仅出现一次，则称方阵 A 为 n 阶拉丁方。设 $A=(a_{ij})_{n\times n}$ 和 $B=(b_{ij})_{n\times n}$ 都是 n 阶拉丁方，若 (A,B) 的 n^2 个元素组成的集合等于 $\{(i,j)\mid i,j=0,1,\cdots,n-1\}$，则称 A 和 B 正交。特别地，当 $k(k\geq 2)$ 个拉丁方 $A_1,A_2,\cdots,A_k$ 两两正交时，则称 $A_1,A_2,\cdots,A_k$ 为正交拉丁方组。

文献[4]对 4 阶正交拉丁方组所设计的基本密码系统进行了研究。本文将利用如下更高的 8 阶正交拉丁方组来设计基本密码系统：

$$L_1=\begin{bmatrix}7&0&1&2&3&4&5&6\\6&1&0&3&2&5&4&7\\5&2&3&0&1&6&7&4\\4&3&2&1&0&7&6&5\\3&4&5&6&7&0&1&2\\2&5&4&7&6&1&0&3\\1&6&7&4&5&2&3&0\\0&7&6&5&4&3&2&1\end{bmatrix}=\begin{bmatrix}T_0\\T_1\\T_2\\T_3\\T_4\\T_5\\T_6\\T_7\end{bmatrix},\quad L_2=\begin{bmatrix}7&0&1&2&3&4&5&6\\3&4&5&6&7&0&1&2\\6&1&0&3&2&5&4&7\\2&5&4&7&6&1&0&3\\1&6&7&4&5&2&3&0\\5&2&3&0&1&6&7&4\\0&7&6&5&4&3&2&1\\4&3&2&1&0&7&6&5\end{bmatrix}=\begin{bmatrix}T_8\\T_9\\T_{10}\\T_{11}\\T_{12}\\T_{13}\\T_{14}\\T_{15}\end{bmatrix}\tag{2}$$

其中，L_1,L_2 中的每一行可看成 $M=\{0,1,2,3,4,5,6,7\}$ 的一个可逆变换，比如 $T_1:Z_8\leftrightarrow Z_8$ 表示如下可逆变换：

$$T_1(0)=6,T_1(1)=1,T_1(2)=0,T_1(3)=3,T_1(4)=2,T_1(5)=5,T_1(6)=4,T_1(7)=7.$$

这样，利用上述两个 8 阶正交拉丁方可设计出理论基本密码系统 (M,C,T)，其中

$$M=C=Z_8=Z_2^3,\ T=\{T_0,T_1,T_2,\cdots,T_{15}\}.$$

下面再考虑与 (M,C,T) 相应的实际基本密码系统 (M,C,K,E,D) 的设计问题。将 Z_8 和 Z_2^3 相互对应的十进制整数和 3 比特向量不加区别。对任意的 $m=m_1m_2m_3\in Z_8$ 和 $c=c_1c_2c_3\in Z_8$：

$$T_0(m)=(m+7)\bmod 8$$

$$T_1(m)=\left[(3\times m_2m_3+1)\bmod 4+4\times m_1+1+4\times \bar{m}_3\right]\bmod 8$$

$$T_2(m)=\left[(m_2m_3+2)\bmod 4+4\times m_1+3+4\times m_3\right]\bmod 8$$

$$T_3(m)=\left[(3\times m_2m_3+3)\bmod 4+4\times m_1+1\right]\bmod 8$$

$$T_4(m)=(m_2m_3+4\times \bar{m}_1+7)\bmod 8$$

$$T_5(m)=\left[(3\times m_2m_3+1)\bmod 4+4\times \bar{m}_1+1+4\times \bar{m}_3\right]\bmod 8$$

$$T_6(m)=\left[(m_2m_3+2)\bmod 4+4\times \bar{m}_1+3+4\times m_3\right]\bmod 8$$

$$T_7(m)=\left[(3\times m_2m_3+3)\bmod 4+4\times \bar{m}_1+1\right]\bmod 8$$

对应的逆变换的代数式如下：

$$T_0^{-1}(c)=(c+1)\bmod 8$$

$$T_1'(c)=(3\times c_2c_3+1)\bmod 4+4\times c_1,\ T_1^{-1}(c)=T_1'\left[(c+3+4\times c_3)\bmod 8\right]$$

$$T_2'(c)=(c_2c_3+2)\bmod 4+4\times c_1,\ T_2^{-1}(c)=T_2'\left[(c+1+4\times c_3)\bmod 8\right]$$

$$T_3'(c)=(3\times c_2c_3+3)\bmod 4+4\times c_1,\ T_3^{-1}(c)=T_3'\left[(c+7)\bmod 8\right]$$

$$T_4'(c)=(c_2c_3+4\times \overline{c}_1),\ T_4^{-1}(c)=T_4'\left[(c+1)\bmod 8\right]$$

$$T_5'(c)=(3\times c_2c_3+1)\bmod 4+4\times \overline{c}_1,\ T_5^{-1}(c)=T_5'\left[(c+3+4\times c_3)\bmod 8\right]$$

$$T_6'(c)=(c_2c_3+2)\bmod 4+4\times \overline{c}_1,\ T_6^{-1}(c)=T_6'\left[(c+1+4\times c_3)\bmod 8\right]$$

$$T_7'(c)=(3\times c_2c_3+3)\bmod 4+4\times \overline{c}_1,\ T_7^{-1}(c)=T_7'\left[(c+7)\bmod 8\right]$$

其中，$m_1\in Z_2, m_2m_3\in Z_4, \overline{m}_1=1-m_1$，×表示实数乘法，类似地可将$T_8,T_9,\cdots,T_{15}$的变换式及其逆变换式全部写出。因此，式(2)中 2 个拉丁方的每一行所决定的变换及其逆变换都可以用代数式来表示。这样，可将实际基本密钥空间设计为$k=k_1k_2k_3k_4\in Z_{16}$，并将加解密变换设计如下：

a) 基本加密变换 E：对任意 3 比特明文$m=m_1m_2m_3\in Z_8$和 4 比特密钥$k=k_1k_2k_3k_4\in Z_{16}$，其中$m_1,m_2,m_3,k_1,k_2,k_3,k_4\in Z_2$，可利用如下统一代数式将加密变换$c=E(m,k)$设计为：

$$\begin{aligned}c=&\tilde{k}_0\times T_0(m)+\tilde{k}_1\times T_1(m)+\tilde{k}_2\times T_2(m)+\tilde{k}_3\times T_3(m)+\tilde{k}_4\times T_4(m)+\tilde{k}_5\times T_5(m)\\&+\tilde{k}_6\times T_6(m)+\tilde{k}_7\times T_7(m)+\tilde{k}_8\times T_8(m)+\tilde{k}_9\times T_9(m)+\tilde{k}_{10}\times T_{10}(m)\\&+\tilde{k}_{11}\times T_{11}(m)+\tilde{k}_{12}\times T_{12}(m)+\tilde{k}_{13}\times T_{13}(m)+\tilde{k}_{14}\times T_{14}(m)+\tilde{k}_{15}\times T_{15}(m)\end{aligned}$$

其中，$\tilde{k}_0=\overline{k}_1\wedge\overline{k}_2\wedge\overline{k}_3\wedge\overline{k}_4$，$\tilde{k}_1=\overline{k}_1\wedge\overline{k}_2\wedge\overline{k}_3\wedge k_4$，$\tilde{k}_2=\overline{k}_1\wedge\overline{k}_2\wedge k_3\wedge\overline{k}_4$，$\tilde{k}_3=\overline{k}_1\wedge\overline{k}_2\wedge k_3\wedge k_4$，$\tilde{k}_4=\overline{k}_1\wedge k_2\wedge\overline{k}_3\wedge\overline{k}_4$，$\tilde{k}_5=\overline{k}_1\wedge k_2\wedge\overline{k}_3\wedge k_4$，$\tilde{k}_6=\overline{k}_1\wedge k_2\wedge k_3\wedge\overline{k}_4$，$\tilde{k}_7=\overline{k}_1\wedge k_2\wedge k_3\wedge k_4$，$\tilde{k}_8=k_1\wedge\overline{k}_2\wedge\overline{k}_3\wedge\overline{k}_4$，$\tilde{k}_9=k_1\wedge\overline{k}_2\wedge\overline{k}_3\wedge k_4$，$\tilde{k}_{10}=k_1\wedge\overline{k}_2\wedge k_3\wedge\overline{k}_4$，$\tilde{k}_{11}=k_1\wedge\overline{k}_2\wedge k_3\wedge k_4$，$\tilde{k}_{12}=k_1\wedge k_2\wedge\overline{k}_3\wedge\overline{k}_4$，$\tilde{k}_{13}=k_1\wedge k_2\wedge\overline{k}_3\wedge k_4$，$\tilde{k}_{14}=k_1\wedge k_2\wedge k_3\wedge\overline{k}_4$，$\tilde{k}_{15}=k_1\wedge k_2\wedge k_3\wedge k_4$。

b) 基本解密变换 D：对任意 3 比特密文$c=c_1c_2c_3\in Z_8$和 4 比特密钥$k=k_1k_2k_3k_4\in Z_{16}$，其中$c_1,c_2,c_3,k_1,k_2,k_3,k_4\in Z_2$，可利用如下统一代数式将解密变换$m=D(c,k)$设计为：$m=\sum_{i=0}^{15}\tilde{k}_i\times T_i^{-1}(c)$。

3.2. 算法设计

参照文献[3]，可将流密码系统设计分为基本密码系统和应用密码系统设计。其中，应用密码系统设计的关键在于密钥序列空间的设计。下面就综合利用上述基本密码系统和 Henon 混沌系统来设计整个流密码算法，其设计步骤如下：

a) 选取大小为$M\times N$的灰度图像P，并将其表示成数字矩阵$I=(m_{ij})_{M\times N}$，其中$m_{ij}\in Z_{256}, i\in\{0,1,\cdots,M-1\}, j\in\{0,1,\cdots,N-1\}$；

b) 将矩阵I中每个像素值读取的 8 比特序列$m=\tilde{m}_1\tilde{m}_2\tilde{m}_3\cdots$转换为 2 元序列，其中，$\tilde{m}_1=m_1m_2m_3\cdots m_8$等。同时，对每个 8 比特进行逐 3 比特的分组，转换为 8 元序列，其中，$\overline{m}_1=m_1m_2m_3\in Z_8, \overline{m}_2=m_4m_5m_6\in Z_8$，剩余 2 比特$m_7m_8$不参与分组和加密，等等；

c) 选定初始参数$x_0=0.000001, y_0=0.000001, a=1.4, b=0.3$代入 Henon 混沌系统，迭代产生混沌序列并对 1 进行取模运算，然后通过取整变换为 2 元序列，再将 2 元序列变换为 16 元密钥流序列$z=\tilde{k}_1\tilde{k}_2\cdots$，其中，$\tilde{k}_1=k_1k_2k_3k_4$，等等；

d) 加密变换：依次对步骤(b)处理后所得到的 8 元序列进行加密。先对明文序列 m 中每个 8 比特$\tilde{m}_j$中

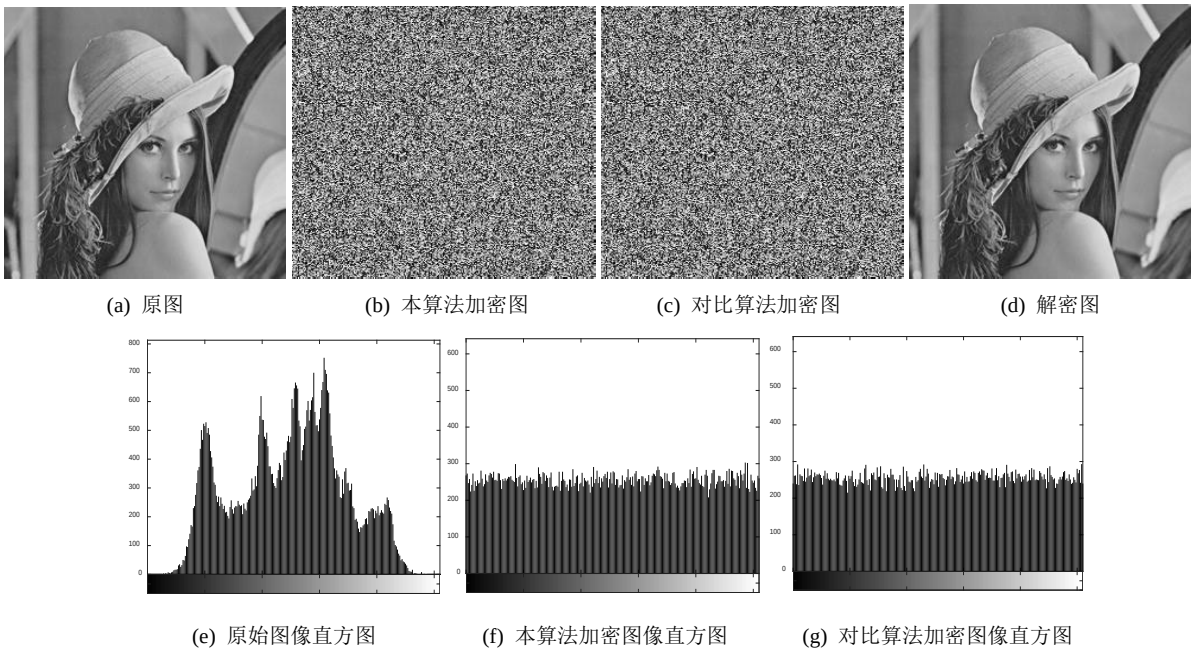
的分组如 $\bar{m}_1\bar{m}_2$ 进行加密 $\bar{c}_i = E\left(\bar{m}_i, \tilde{k}_j\right), i=1,2;\ j=1,2,\cdots$，可得到加密后的分组序列 $\bar{c}_1\bar{c}_2$，转换成 6 比特后拼接上未作加密的 2 比特 m_7m_8，从而得到 8 比特的密文分组 $\tilde{c}_j$，对矩阵 I 中的所有像素值加密完成后即可得到密文图像 c；

e) 解密变换：依次对经过步骤(d)加密处理的每个密文序列 c 进行解密。同样只对 8 比特密文分组 $\tilde{c}_j$ 决定的 3 比特序列 $\bar{c}_1\bar{c}_2$ 进行解密 $\bar{m}_i = D\left(\bar{c}_i, \tilde{k}_j\right), i=1,2;\ j=1,2,\cdots$，可得到解密后的序列 $\bar{m}_1\bar{m}_2$，转换成 6 比特后拼接上未作加密的 2 比特 m_7m_8，从而得到 8 比特的明文序列 m，全部解密完成即可得到明文图像 P。

特别说明如下：将矩阵 I 中每个像素值转换成 8 比特的 2 元序列后，为避免逐 3 比特分组不完整的情况，只需对前 6 位比特进行加密。由于灰度图像的效果主要由每个像素值的高位决定，因此只对每个 8 比特像素的前 6 位进行加密并不影响图像的加解密效果。

3.3. 仿真结果及分析

本文选取了大小为 256 × 256 的灰度图像 Lena，根据上述算法步骤进行加解密，绘制了加密前后的图像直方图，与文献[8]所提出的复合两种混沌系统(Kawakami 混沌系统和 Bao 混沌系统)且基于模 2 加法设计基本密码系统的流密码算法进行比较，仿真结果见图 1。为方便叙述，本文将把文献[8]所提出的算法作为对比算法与本算法进行加密效果比较。



(a) 原图　(b) 本算法加密图　(c) 对比算法加密图　(d) 解密图

(e) 原始图像直方图　(f) 本算法加密图像直方图　(g) 对比算法加密图像直方图

Figure 1. Simulation effect of algorithm
图 1. 算法仿真效果图

图像的直方图反映的是图像像素值的分布情况，像素值的分布越均匀，抵抗统计攻击的能力就越强。可以发现，两种算法都能对原始图像进行有效地加解密，加密效果相当，应用两种算法加密得到的密文图像的灰度值都接近均匀分布，能够有效抵抗统计分析，使得攻击者无法得到任何有效信息。

3.3.1. 相关性分析

图像像素的相关性指的是图像中相邻像素之间的关联程度，像素的相关性高，攻击者便可通过相邻像素预测像素值，从而获取图像数据。可靠的加密算法应保证相邻像素之间的相关性足够弱。本文在明

文图像及其密文图像中随机选取了 3000 对相邻像素对，从水平、垂直和对角方向上绘制像素分布图，分析它们各自在三个方向上的相关性，结果如图 2 所示。其中，图 2(a)~(c)是明文图像在水平、垂直和对角方向上像素的分布，图 2(d)~(f)是利用对比算法加密得到的密文图像在水平、垂直和对角方向上像素的分布，图 2(g)~(i)是利用本文算法加密得到的密文图像在水平、垂直和对角方向上像素的分布。可以看到，明文图像在三个方向的线性相关性都比较高，采用两种算法加密之后，密文图像在三个方向上的像素分布均匀性都能显著提高，相邻像素点的相关性大幅减弱，很好地掩盖了明文图像的相关特征。

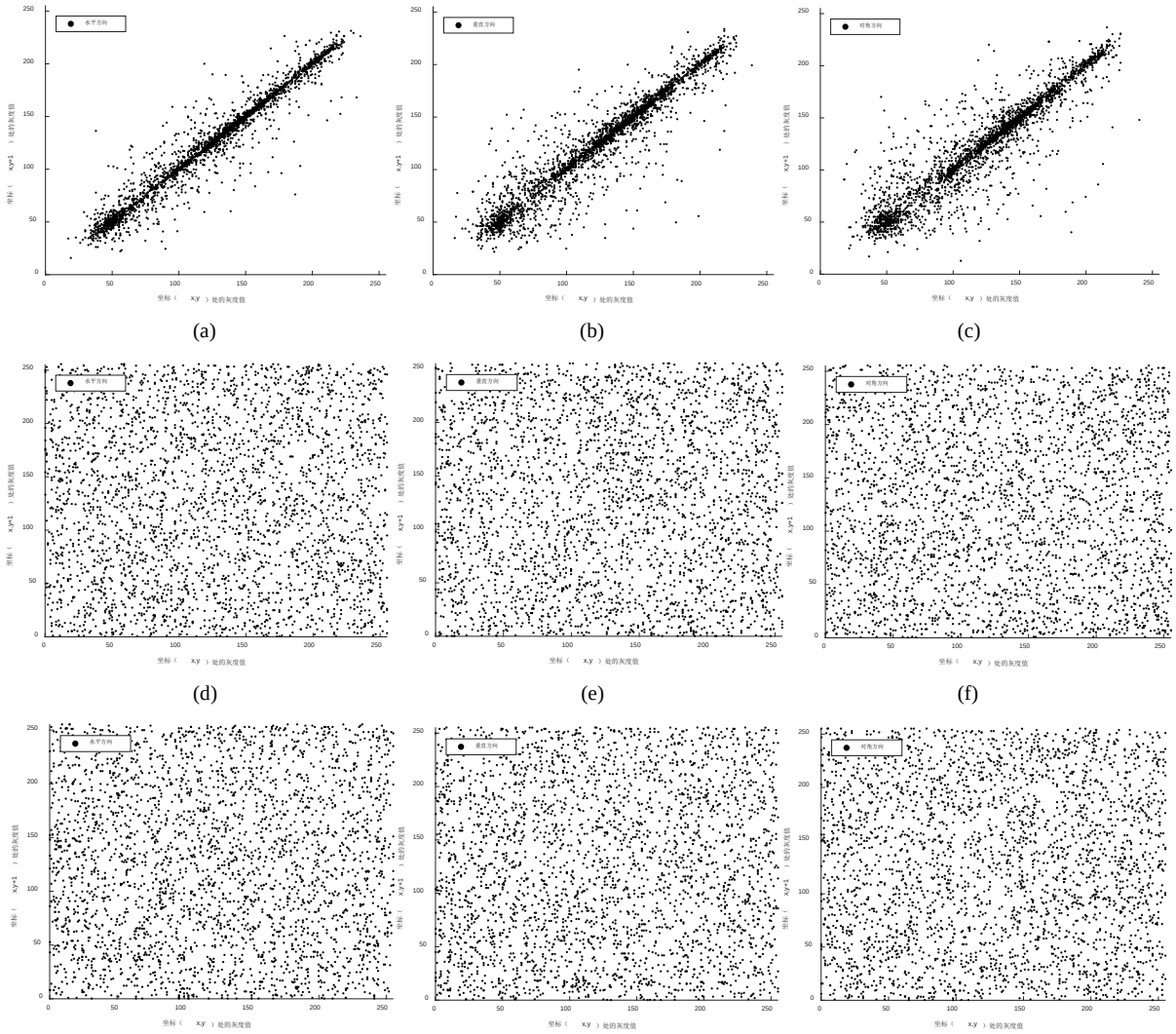


Figure 2. Neighboring Pixel distribution
图 2. 相邻像素分布图

相邻像素之间的相关性还可通过相关系数来表示，系数值越小，说明该图像相邻像素之间的相关性越弱，随机性越强，反之系数值越大，说明相关性越强，随机性越弱。随机选取 N 对相邻的像素对，并记其灰度值为 $(x_i, y_i), i=1,2,\cdots,N$，相关系数的计算公式如下：

$$\rho_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{3}$$

其中：

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

根据式(3)和(4)分别计算明文图像和密文图像在水平、垂直和对角方向的相关系数，结果见表 1。从表中可以看出，明文图像在三个方向的相关系数均接近 1，表明图像像素之间的相关性较强，经过加密之后，所有方向的相关系数均接近于 0，有效降低了图像像素的相关性。两种算法尽管在某一方向上的相关系数有微小差异，但总体相差无几，均可以打乱图像像素之间的关联。

Table 1. Image correlation coefficient
表 1. 图像相关系数

方向	原图	对比算法	本文算法
水平	0.9751	0.0021	0.0030
垂直	0.9339	0.0009	0.0082
对角	0.9210	0.0033	0.0011

3.3.2. 密钥敏感度分析

更进一步，对密钥敏感度进行分析，密钥敏感度指的是当密钥发生细小变化时，系统的加解密效果会发生显著变化。为了评估本文所提出的加密算法的密钥敏感度，采用了差别极其微小的两组密钥 $\text{key}\,1=\{x_0:0.000001, y_0=0.000001\}$ 和 $\text{key}\,2=\{x_0:0.000001001, y_0=0.000001001\}$ 分别对图像进行加解密，结果如图 3 所示。对于使用 key1 加密的密文图像，采用 key2 进行解密，根本无法得到原始图像，这说明本文所设计的算法对密钥极度敏感，具有较高的安全性。

(a) 原图　(b) key1 加密图　(c) key1 解密图　(d) key2 解密图

Figure 3. Encrypt and decrypt images with different keys
图 3. 不同密钥加解密图像

3.3.3. 信息熵分析

图像的信息熵反映了图像像素值的不确定性，熵值越高，不确定性就越高。一个可靠的图像加密算法应保证密文图像具有足够高的不确定性。信息熵的计算公式如下：

$$H(m)=-\sum_{i=0}^{M-1}p(m_i)\log_2 p(m_i),\ \sum_{i=0}^{M-1}p(m_i)=1 \tag{5}$$

其中， $M=256$ 表示 256 个灰度级， $p(m_i)$ 表示灰度值 m_i 出现的概率，根据最大熵原理，理想的密文图像的最大信息熵为 8。本文计算了图像加密前后的信息熵，并与使用对比算法[8]得到的密文图像的信息熵进行比较，结果如表 2 所示。可以看到，应用本算法对图像进行加密所得到的信息熵更接近理想值 8，说明经过本算法加密的密文图像具有更好的不可预测性，优于对比算法。

Table 2. Image information entropy
表 2. 图像信息熵

	原图	对比算法	本文算法
熵值	7.4587	7.9676	7.9973

4. 小结

本文研究了基于 8 阶正交拉丁方组的基本密码系统的设计方法，同时结合 Henon 混沌系统设计了一种新的多元流密码算法，并将其应用到图像加密上。通过对仿真结果的分析可知，该算法具有较高的安全性和可行性，为后续研究更高阶正交拉丁方组及其基本密码系统设计打下了基础。

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] 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

[3] 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.

[4] 田传俊. 基于 4 阶正交拉丁方组实际基本密码系统设计[J]. 深圳大学学报(理工版), 2020, 37(3): 251-256.

[5] Fridrich, J. (1997) Image Encryption Based on Chaotic Maps. *IEEE International Conference on Systems*, Orlando, FL, 12-15 October 1997, 1105-1110.

[6] 朱和贵, 蒲宝明, 朱志良, 赵怡然, 宋禹佳. 二维 Sine-Tent 超混沌映射及其在图像加密中的应用[J]. 小型微型计算机系统, 2019, 40(7): 1510-1518.

[7] Hénon, M. (1976) A Two-Dimensional Mapping with a Strange Attractor. *Communications in Mathematical Physics*, **50**, 69-77. https://doi.org/10.1007/BF01608556

[8] 缑新科, 吴贻峰. 基于复合混沌的数字图像加密算法[J]. 计算机与数字工程, 2018, 46(12): 2574-2579.