Computer Science and Application 计算机科学与应用, 2020, 10(11), 1938-1943
Published Online November 2020 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2020.1011204

Hans汉斯

基于拉丁方的流密码算法设计与仿真

李　熙，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10月22日；录用日期：2020年11月6日；发布日期：2020年11月13日

摘　要

本文利用所构造的高阶拉丁方设计了一种新的基本密码系统，并结合常用的Logistic混沌系统提出了一种新的流密码算法。而且，将这种流密码算法应用于图像加密，并对加密效果进行了仿真。仿真结果表明该算法不仅密钥敏感性强、密钥空间大，而且加密后图像具备相邻像素相关性小，信息熵大等优点。

关键词

流密码算法，拉丁方构造，基本密码系统，数字图像，加密

Design and Simulation of Stream Cipher Algorithm Based on Latin Square

Xi Li, Chuanjun Tian

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

Received: Oct. 22nd, 2020; accepted: Nov. 6th, 2020; published: Nov. 13th, 2020

Abstract

This paper uses the constructed high-order Latin square to design a new basic cipher system, and combines the commonly used Logistic chaotic system to propose a new stream cipher algorithm. Moreover, applying this stream cipher algorithm to image encryption, the encryption effect is simulated. The simulation results show that the algorithm not only has strong key sensitivity and large key space, but also the encrypted image has the advantages of small correlation coefficient among neighbor pixels and large information entropy.

文章引用: 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.
DOI: 10.12677/csa.2020.1011204

Keywords

Stream Cipher Algorithm, Latin Square Structure, Basic Cipher System, Digital Image, Encryption

1. 引言

众所周知，加密算法是密码学的基础知识，是保护信息安全的一种基本方法，其中的流密码算法具有加解密速度快和安全性高等优点，因而在信息安全领域有着广泛应用。参照最近建立的完善保密系统一般模型，流密码算法的关键是基本密码系统和密钥流序列的设计。由文献[1] [2] [3] [4] [5]可知，当前常见的模 2 加法流密码算法的基本密码系统是由二元加法设计的，该运算过于简单，不利于设计出性能优良的流密码算法。最近，文献[6]利用了比模 2 加法更复杂的 4 阶拉丁方运算来设计基本密码系统，为流密码算法设计指明了一条新的设计路线。同时，文献[7] [8]也相继研究了 16 阶拉丁方构造基本密码系统的方法。由于拉丁方的数量会随着阶数的增加呈指数式增加，因此，文献[6] [7] [8]所能构造的拉丁方及其基本密码系统是十分有限的，还有许多问题值得进一步研究。当前，基于拉丁方设计基本密码系统的研究还未充分展开，它们在流密码算法设计中的应用还很狭窄。为了进一步推广二元加法流密码算法的设计方法，本文将给出一种任意有限阶拉丁方及其基本密码系统构造的新方法，并结合常见的 Logistic 离散混沌设计一种新的流密码算法。

2. 一些基本概念

参照现有密码学文献，流密码算法的基本步骤为：1) 设明文序列为 $m=m_0m_1m_2\cdots$；2) 利用密钥 k 和密钥流发生器产生一个密钥流序列 $z=k_0k_1k_2\cdots$；3) 利用加密变换 E 逐个加密明文得到密文 $c=c_0c_1c_2\cdots$，其中，$c_j=E\left(k_j,m_j\right)$，对任意 $j=0,1,2,\cdots$；4) 利用解密变换 D 将 c 依次解密恢复出明文序列 $m=D\left(k_0,c_0\right)D\left(k_1,c_1\right)D\left(k_2,c_2\right)\cdots$。

由文献[6]知，在常见的二元流密码算法中，加解密变换 E 和 D 都是模 2 加法。由于基本明文空间和密文空间 $Z_2=\{0,1\}$ 元素很少，因而所能设计的基本密钥变换和基本密码系统都很简单，且数量很少[6]。为了改进这种常见的模 2 加法的基本加密方式，文献[7] [8]分别研究了单个 16 阶拉丁方构造基本密码系统的设计方法，但所构造的基本密码系统类型仍然有限。本文将研究新的高阶拉丁方及其相应的基本密码系统的设计方法。

定义 2.1 设 n 阶方阵 $A=\left(a_{ij}\right)_{n\times n}$，$n\in\{2,3,4,\cdots\}$ 满足 $a_{ij}\in\{0,1,\cdots,n-1\}$。如果 $Z_n=\{0,1,2,\cdots,n-1\}$ 上所有不同的数字在 n 阶方阵 A 的每行和每列中都出现，则称 A 为 n 阶拉丁方。

由于基本密码系统取决于选取的拉丁方，因此需要研究拉丁方的构造方法。考虑到同一个整数都能利用十进制和二进制两种不同形式加以表示，为了便于表述，下面将十进制整数集 $Z_{2^t}=\{0,1,\cdots,2^t-1\}$ 和二进制数集 $Z_2^t=\{0\cdots00,0\cdots01,1\cdots11\}$ 不加区别，且把它们对应相等的数也不加区别。

定理2.1 设 $n=2^t$。在 $Z_n=Z_2^t$ 上定义变换或函数：对任一 $m=m_1m_2m_3\cdots m_t\in Z_n$，$m_j\in Z_2$，对任一 $j=1,2,\cdots,t$，定义 $f_0\left(m\right)=m_tm_{t-1}\cdots m_2m_1$，$f_1\left(m\right)=m_tm_{t-1}\cdots m_2\bar{m}_1$，$f_2\left(m\right)=m_tm_{t-1}\cdots\bar{m}_2m_1$，$\cdots$，$f_{n-1}\left(m\right)=\bar{m}_t\bar{m}_{t-1}\cdots\bar{m}_2\bar{m}_1$。记

$$A=\left(a_{ij}\right)_{n\times n}=\begin{pmatrix} f_0(0) & f_0(1) & \cdots & f_0(n-1) \\ f_1(0) & f_1(1) & \cdots & f_1(n-1) \\ \vdots & \vdots & \ddots & \vdots \\ f_{n-1}(0) & f_{n-1}(1) & \cdots & f_{n-1}(n-1) \end{pmatrix}$$

则 $A=\left(a_{ij}\right)_{n\times n}$ 是一个n阶拉丁方。

证明：当 $m=m_1m_2m_3\cdots m_t\in Z_n$ 依次取遍 $0,1,\cdots,n-1$ 时，对于固定的 $j=0,1,\cdots,n-1$，依次计算 $f_j(m)$ 会得到一个n维向量，它正好是向量 $(0,1,\cdots,n-1)$ 的一个置换。因此，矩阵 $A=\left(a_{ij}\right)_{n\times n}$ 中每一行的全部元素是由 $0,1,\cdots,n-1$ 组成的。而且，由变换 $f_0,f_1,\cdots,f_{n-1}$ 的定义，不难发现，当选定一个元素 $m=m_1m_2m_3\cdots m_t\in Z_n$ 时，$f_0(m),f_1(m),\cdots,f_{n-1}(m)$ 都不相同，因此，$A=\left(a_{ij}\right)_{n\times n}$ 中每一列的全部元素也是由 $0,1,\cdots,n-1$ 组成的。于是，由定义2.1可知，$A=\left(a_{ij}\right)_{n\times n}$ 是一个n阶拉丁方，证毕！

特别地，当t取8时，由定理2.1可得如下2^8阶拉丁方

$$L_{256\times 256}=\begin{bmatrix} 0 & 128 & 64 & 192 & \cdots & 255 \\ 1 & 129 & 65 & 193 & \cdots & 254 \\ 2 & 130 & 66 & 194 & \cdots & 253 \\ 3 & 131 & 67 & 195 & \cdots & 252 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 255 & 127 & 191 & 63 & \cdots & 0 \end{bmatrix}=\begin{bmatrix} T_0 \\ T_1 \\ T_2 \\ T_3 \\ \vdots \\ T_{255} \end{bmatrix}$$

其中，$T_0:Z_{256}\leftrightarrow Z_{256}$ 表示可逆变换：$T_0(0)=0,T_0(1)=128,\cdots,T_0(255)=255$ 等，其中，将 Z_{256} 与 Z_2^8 中相互对应的数不加以区别。因此，基于 L 设计的理论基本密码系统 (M,C,T) 满足 $M=C=Z_2^8=Z_{256}$ 和 $T=\{T_0,T_1,\cdots,T_{255}\}$。类似于文献[6]中的记号，下面将所设计的流密码系统的具体明文单元设为 $m_j\in M$，对任意 $j=0,1,2,\cdots$，等等。

3. 一种新的流密码算法设计

3.1. 算法描述

参照文献[6]，保密系统定义为从明文集 M 到密文集 C 的一组可逆变换 T，可将每次加密的最小明文单元称为基本明文。基本密钥、基本密文和基本加解变换可类似定义。当 M,T,C 都是基本单元时，称 (M,T,C) 为理论基本(密码)系统。T^{-1} 为理论密钥(变换)集 T 的逆变换集。应用密码系统可类似定义。为了方便实际使用，有必要将 T 和 T^{-1} 转化为集合 K 和加密变换 E 与解密变换 D 来实现。上面已设计出一个理论基本系统 (M,T,C)，因而还需要设计与它对应的实际基本(密码)系统 (M,C,K,E,D)。

1) 实际基本密码系统的设计 (M,C,K,E,D)

先将 $T=\{T_0,T_1,T_2,\cdots,T_{255}\}$ 中每个变换的计算公式表示为：对任意 $m=m_0m_1m_2\cdots m_7\in Z_2^8$，

$$T_0(m)=m_7m_6\cdots m_1m_0,\quad T_1(m)=m_7m_6\cdots m_1\bar{m}_0,$$

$$T_2(m)=m_7m_6\cdots\bar{m}_1m_0,\quad \cdots,\quad T_{255}(m)=\bar{m}_7\bar{m}_6\cdots\bar{m}_1\bar{m}_0,$$

其中，$m_i\in Z_2$，$\bar{m}_i=1-m_i$，$i=0,1,\cdots,7$。这样，实际基本密钥空间 $K=Z_{256}$ 满足 $k\leftrightarrow T_k$，对任意 $k\in K=Z_2^8$。因此，基本加密函数 E 的计算公式为 $c=E(k,m)=T_k(m)$。

为了方便实际应用，可将基本加密函数 E 和解密函数 D 的具体计算公式设计如下：

a) 基本加密函数 E：对任一 8 比特基本明文 $m=m_0m_1\cdots m_7\in Z_2^8$ 和 8 比特密钥 $k=k_0k_1k_2\cdots k_7\in Z_2^8$，其中 $m_0,m_1,\cdots,m_7,k_0,k_1,\cdots,k_7\in Z_2$，将加密变换 $c=E(k,m)$ 统一设计为

$$c=(m_7\oplus k_0)(m_6\oplus k_1)(m_5\oplus k_2)(m_4\oplus k_3)(m_3\oplus k_4)(m_2\oplus k_5)(m_1\oplus k_6)(m_0\oplus k_7),$$

其中，$\oplus$ 表示异或运算，多个相连的圆括号表示将多个比特组成一个多比特序列。

b) 基本解密函数 D：对任一 8 比特密文 $c=c_0c_1c_2\cdots c_7\in Z_2^8$ 和 8 比特密钥 $k=k_0k_1k_2\cdots k_7\in Z_2^8$，其中 $c_0,c_1,\cdots,c_7,k_0,k_1,\cdots,k_7\in Z_2$，可将解密变换 $m=D(k,c)$ 设计为

$$m=(c_7\oplus k_7)(c_6\oplus k_6)(c_5\oplus k_5)(c_4\oplus k_4)(c_3\oplus k_3)(c_2\oplus k_2)(c_1\oplus k_1)(c_0\oplus k_0)。$$

至此就完成了实际基本密码系统 (M,C,K,E,D) 的设计。

易见，本基本密码系统是利用定理 2.1 中的高阶拉丁方设计的，不过，类似于上述方法，若将定理 2.1 中拉丁方的阶数 t 加以改变，则可得到不同的拉丁方，进而可设计出不同的基本密码系统。本文不再考虑了。

2) 应用密码系统中密钥流序列的设计

上面已设计出实际基本密码系统 (M,C,K,E,D)，还需要设计应用密钥序列空间才能构成一个完整的流密码算法。下面再来讨论应用系统中密钥序列空间的设计问题，将利用现有的 Logistic 混沌系统作为一个密钥流发生器来对密钥流序列空间进行设计。该混沌系统表达式如下：

$$x_{n+1}=\mu x_n(1-x_n)$$

其中 $x_n\in[0,1]$，对任意的 $n=0,1,2,\cdots$，且 $\mu\in[0,4]$。当 $\mu\in[3.571448,4]$ 时，系统会处于混沌状态。

综合上述基本密码系统和 Logistic 混沌系统，下面将给出一种新的流密码算法设计步骤：

1) 选择一幅数字灰度图像作为明文，在 Matlab 软件中，该明文可表示成一个矩阵 $I=(m_{ij})_{m\times n}$，其中，$m_{ij}\in Z_{256}$，对任意 $i,j=0,1,\cdots,255$；

2) 将矩阵 I 按照从左到右，从上到下的顺序转化为明文序列 $m=\tilde{m}_1\tilde{m}_2\tilde{m}_3\cdots$，其中 $\tilde{m}_i\in Z_{256}$；

3) 设 $\mu_1,x_0,\mu_2,y_0,\mu_3$，$\mu_1,\mu_2,\mu_3\in[3.571448,4]$，$x_0,y_0\in[0,1]$ 为算法的 5 个密钥，其中 μ_1，μ_2，μ_3 为 Logistic 混沌 3 个不同的控制参数，x_0 和 y_0 为 2 个初值。将 x_0 和 y_0 分别代入 μ_1 和 μ_2 所决定的 Logistic 混沌系统，重复迭代 500 次可使得解序列较为混乱，并记 $w_0=(x_{501}+y_{501})/2$；

4) 将 w_0 作为初值带入 μ_3 所决定的 Logistic 混沌系统，进行多次迭代，并舍去前 500 个数值，令 $k_0=round(w_{501}),k_1=round(w_{502}),\cdots$，可得密钥流序列 $z=k_0k_1\cdots$，$k_j\in Z_2$，将密钥流序列按每 8 比特进行分组，将分组后的序列记为 $\tilde{z}=\tilde{k}_0\tilde{k}_1\cdots$，其中 $\tilde{k}_0=k_0k_1k_2k_3k_4k_5k_6k_7\in Z_{256}$ 等；

5) 加密变换：按照加密变换 $E:\tilde{c}_j=E(\tilde{k}_j,\tilde{m}_j),j=1,2,\cdots$，依次对明文单元 $\tilde{m}_j$ 加密，可得密文单元序列 $c=\tilde{c}_1\tilde{c}_2\cdots$，若有必要，可将 c 变换为 2 元密文序列；

6) 解密变换：按照解密变换 $D:\tilde{m}_j=D(\tilde{k}_j,\tilde{c}_j),j=1,2,\cdots$，依次对密文单元 $\tilde{c}_j$ 解密，可得明文单元序列 $m=\tilde{m}_1\tilde{m}_2\cdots$。然后可将 m 还原为原数字图像矩阵 $I=(m_{ij})_{m\times n}$。

3.2. 实验结果与分析

将上述密码算法运用于数字图像加解密，取密钥 $x_0=0.578$，$y_0=0.189$，$\mu_1=3.723$，$\mu_2=3.912$，$\mu_3=4.000$，与文献[9]中常用密码算法进行对比，Matlab 仿真的加解密效果图及灰度直方图如下：

图 1(e)~(g)分别为原始图像、本算法加密图像、对比算法加密图像的像素分布直方图，从图中可看出，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。更进一步，根据式(3-1)再对两种算法加密图像的相邻像素间的相关性进行计算，结果如表 1。

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{3-1}$$

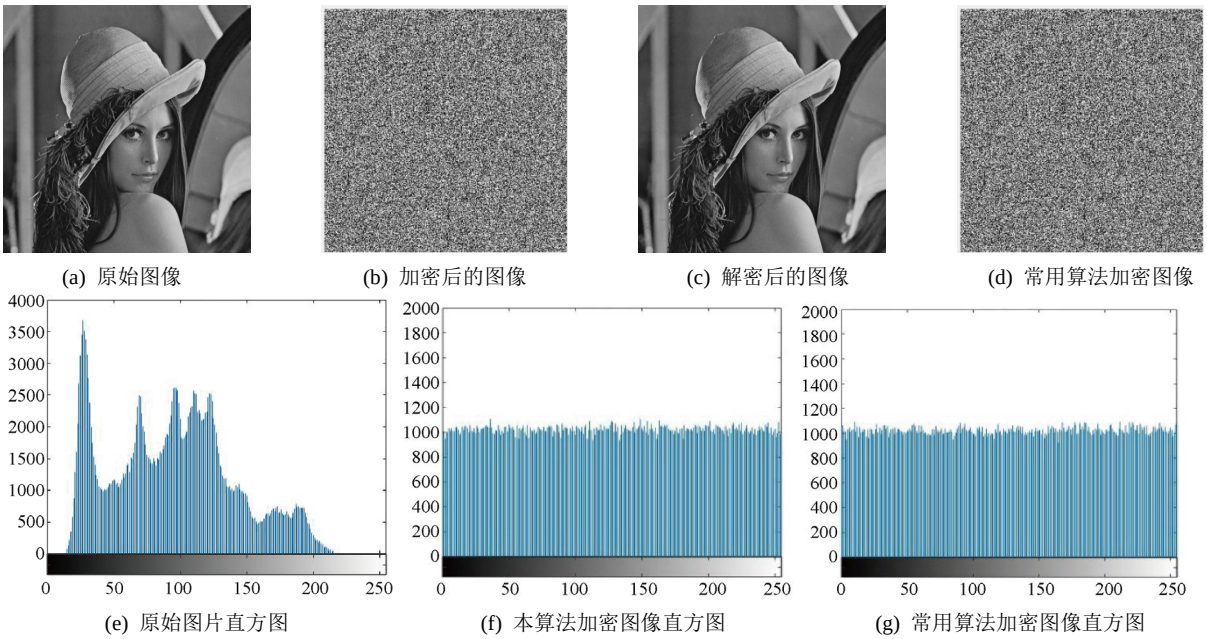

Figure 1. Algorithm simulation renderings
图 1. 算法仿真效果图

Table 1. Correlation simulation data
表 1. 相关性仿真数据

方向	原图	本算法	常用流密码算法
水平	0.97205	−0.00125	0.0076
竖直	0.98617	0.00118	0.0012
对角	0.96523	0.00186	0.0039

其中：

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)\left(y_i-E(y)\right),$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)^2,$$

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i$$

从表 1 中可看出，两种算法加密后的图像，在各个方向上相邻像素间的关系几乎为零，这说明像素间基本没有相关性。其次从表 1 中可知，本算法加密后的图像除了在竖直方向上仅有微小的差异外，在水平和对角方向上都比常见的流密码算法具有更低的像素相关性，这说明新算法具有更好的置乱效果。

下面对密钥空间进行分析。本算法包括五个密钥 $x_0, y_0, \mu_1, \mu_2, \mu_3$，假设计算精度为 10^{-16}，则密钥空间约为$10^{80} \approx 2^{256}$。一般认为密钥空间大于 2^{128} 便能抵抗穷举攻击，因而本密码算法具有较强的抗穷举攻击的能力。另外，再对密钥敏感性进行测试，密钥敏感性指的是当密钥发生细小变化时，系统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，假定 μ_1, μ_2, μ_3 为固定值，采用了差别极其微小的两组密钥 $\text{key1}=\{x_0:0.278, y_0:0.189\}$ 和 $\text{key2}=\{x_0:0.2780000001, y_0:0.189\}$ 分别对图像进

行加解密，测试结果如图 2 所示。分析图 2 知，即使对解密密钥进行微小的改动，也无法恢复出明文，这说明本文所设计的算法对密钥极度敏感。

(a) 原始图像　(b) key1 的加密图像　(c) key1 的解密图像　(d) key2 的解密图像

Figure 2. Key sensitivity test
图 2. 密钥敏感性测试

下面再进行信息熵分析。根据图像信息熵的定义式(3-2)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]，故图像中各像素值等概率出现时最大信息熵达到 8。其中熵的计算公式为

$$H(X)=-\sum_{i=1}^{256}P(x_i)\log_2 P(x_i) \tag{3-2}$$

根据本文所选取的数字图像计算，可得原始图像信息熵为 7.3722，文献[9]中的算法加密后的信息熵为 7.9856，本算法加密后的图像信息熵为 7.9994。从结果可看出，本算法加密后的图像信息熵比常用密码算法加密后的图像信息熵更接近理想值，故新密码算法具有更好的性能。

4. 小结

本文提出了一种高阶拉丁方的构造方法，并研究了这种拉丁方构造基本密码的设计问题，以及结合常见的密钥流产生器提出了一种新的流密码算法。通过与常见流加密算法对比分析可知，该算法密钥空间大，且加密后的图片信息熵更接近理想信息熵，因此该算法具有更强的抗攻击能力，具有一定的实用参考价值。

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] Ge, X., Luo, X.Y., Lu, B., *et al*. (2017) Cryptanalyzing an Image Encryption Algorithm with Compound Chaotic Stream Cipher Based on Perturbation. *Nonlinear Dynamics*, **90**, 1141-1150. https://doi.org/10.1007/s11071-017-3715-7

[3] 田传俊, 李佳佳, 曾泉, 等. 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): 33-36.

[4] 田传俊, 林敬, 曾泉, 等. 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. https://doi.org/10.12677/CSA.2018.811189

[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] 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.

[7] 汤艳华, 田传俊. 基于拉丁方的数字图像加密算法设计[J]. 应用数学展, 2020, 9(2): 257-262. https://doi.org/10.12677/AAM.2020.92030

[8] 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. https://doi.org/10.12677/CSA.2020.101013

[9] 张永红, 张博. 基于 Logistic 混沌系统的图像加密算法研究[J]. 计算机应用研究, 2015, 32(6): 1770-1773.