# 基于3D混沌映射和细胞自动机的图像加密方案

李敬医 陈炬桦
(中山大学信息科学与技术学院 广州 510006)

**摘 要** 为设计高效的、加密性能好的图像加密系统,充分结合混沌映射细胞自动机的良好加密性能,提出了一种基于3D混沌映射和2D二阶细胞自动机的图像加密方案。该算法先利用3D混沌映射对图片像素进行置乱,然后利用2D二阶细胞自动机对图像在比特级别进行更进一步的混淆。该算法属于对称密钥加密,具有较大的密钥空间和并行化的加解密过程。实验结果证明,该算法可以在较小的迭代次数内达到良好的加密效果,不会导致密文扩张,且加密结果能够抵御常见的暴力破解攻击、统计分析攻击和差分攻击,具有较高的安全性。

**关键词** 3D混沌映射,2D二阶细胞自动机,图像加密
**中图法分类号** TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.7.040

## 3D Chaos Map and Cellular Automata Based Image Encryption

LI Jing-yi CHEN Ju-hua
(School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China)

**Abstract** To design a high efficiency and good performance image encryption system, a novel scheme was proposed based on 3D chaos map and 2D second order cellular automata. In this algorithm, image pixels are permuted using 3D cat chaos map. Then in diffusion stage, each pixel value in bit level is permuted using 2D second order cellular automata. This scheme belongs to the class of symmetric systems, which also has a large key space, and both encryption and decryption are parallel. The results of several experiments on brute force attack, statistical analysis and differential attack show that the scheme can achieve a high security in few iterations and won't enlarge the cipher image.

**Keywords** 3D chaos map, 2D second order cellular automata, Image encryption

## 1 引言

传统的加密方案可以有效保护信息安全,但是对于图像数据来说则十分低效,因为其不能充分利用图像的特点。

混沌系统是一种复杂的非线性系统,其许多性质都非常符合图像加密的需求,比如其对初始值、系统参数的高度敏感性以及很好的随机性和不可预测性。因此近些年越来越多的学者把混沌系统应用在图像加密上,其中Wang X、Patidar V等人将Logistic变换应用于图像加密的置乱阶段[1-3],而Chen G和Kanso A等人则把3D猫脸变换应用于像素置乱和混淆中[4,5]。彭川等人利用Logistic混沌系统和细胞自动机构造了简单有效的加密方案[6]。

细胞自动机(CA)作为Von[7]在研究自组织特性的离散动力系统时引入的概念,能够通过简单的演化规则表达出复杂的行为模式,非常适合图像加密的实现,尤其是二维细胞自动机在并行加密方面更是有着天然的优势。早在1985年,Wolfram[8]就提出了将CA运用于流密码上。随后国内外的众多学者又将其扩展到图像加密领域,夏学文把二维右触发可逆细胞自动机应用于数据加密上[9]。Abdo AA利用改进的初等细胞自动机实现对图片的加密[10]。Chen RJ和Seredynski M等人分别提出了基于可逆细胞自动机的图像加密方案[11,12]。

本文充分利用了混沌系统和细胞自动机的优点,设计了一种新的图像加密方案。利用3D混沌映射对图像像素进行置乱,利用2D二阶可逆细胞自动机对图像在比特级别进行混淆,通过两个步骤的多次迭代,完成加密过程。

## 2 3D混沌映射和2D二阶细胞自动机模型

### 2.1 3D混沌映射

混沌映射对初值的高敏感性,使其成为了图像加密中的一种有效处理手段。3D混沌映射[5]的基础是Arnold提出的猫脸变换[13],它属于一种可逆的混沌映射。其定义如下:

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \pmod 1 \tag{1}$$

这种线性变换由于其行列值为1,因此是一种保面积映射(Area-preserving Map)。通过上式的矩阵的特征值可以计算Lyapunov指数 $\gamma_1 = \ln(3+\sqrt{5})/2 = 0.9624$ 和 $\gamma_2 = \ln(3-\sqrt{5})/2 = -0.9624$。其中正的Lyapunov指数表示这种映射具备混沌效应,同时意味着这种映射的结果对初始值的变化非常敏感。

到稿日期:2014-07-20 返修日期:2014-10-21
李敬医(1990—),男,硕士生,主要研究方向为细胞自动机、信息安全,E-mail:zawdd@163.com;陈炬桦(1960—),男,副教授,硕士生导师,主要研究方向为信息安全,E-mail:isscjh@mail.sysu.edu.cn。

式(1)可以通过引入两个参数 $a$ 和 $b$ 扩展为式(2)：

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \pmod 1 \tag{2}$$

从而进一步可以从二维扩展到三维：

$$A = \begin{pmatrix} 1+a_x a_z a_y & a_z \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 \\ a_x b_x b_y + b_y & b_x \end{pmatrix}$$

其中，$a_x, a_y, a_z, b_x, b_y, b_z$ 全部都是正整数。

可以计算矩阵 $A$ 的行列式的值依然为 1，所以式(3)依然满足一一映射，即可以通过 $A^{-1}$ 进行逆运算。当 $a_x=1, a_y=1, a_z=1, b_x=2, b_y=2, b_z=2$ 时，矩阵 $A$ 的特征值分别是 $\sigma_1=14.3789, \sigma_2=0.4745, \sigma_3=0.1466$，由于其主特征值远大于 1，因此式(3)依然具有混沌效应。图 1 描绘了根据式(3)产生的随机点序列的分布。

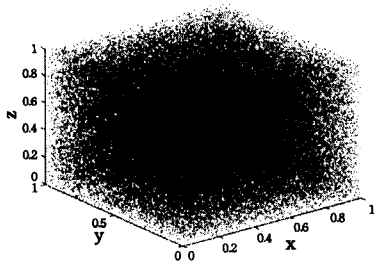



图 1　混沌映射产生的随机序列的分布

## 2.2　2D 二阶细胞自动机

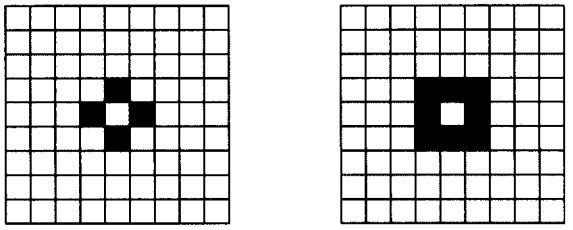
### 2.2.1　初等细胞自动机

细胞：是细胞自动机的基本构成单位，把整个细胞自动机看做一个网状结构，则每个细胞就是一个格子。

细胞状态：每个细胞的状态的集合 $Q$，通常 $Q=\{0,1\}$。

配置空间：也叫做细胞空间，是每个时刻所有细胞的状态所组成的全局状态的集合。在 $t$ 时刻细胞自动机的配置记为 $S^t$，而 $t$ 时刻下细胞 $S_i$ 的状态就是 $S_i^t$。

邻域：细胞邻域是以某一细胞为中心的周围细胞的集合，对于二维细胞自动机，常见的邻域有以下两种，如图 2 所示。本文利用冯诺依曼型邻居作为扩展的基础。



(a)冯诺依曼型邻居　　(b)摩尔型邻居

图 2　二维细胞自动机邻居类型

边界条件：由于细胞自动机中的细胞不是无限的，当处理到边缘细胞时就要考虑到边界条件，通常采用的边界条件有 3 种，分别是反射型、周期型和定值型边界，本文利用的是周期型边界条件。

局部规则：局部规则是一个局部状态转移函数，在初等细胞自动机中，$t$ 时刻下一个中心细胞和其邻域细胞状态为自变量，根据此函数，决定 $t+1$ 时刻此中心细胞的状态。

### 2.2.2　2D 二阶细胞自动机的具体描述

为了使细胞自动机运用于图像加密中，其需要具有可逆

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \\ z_{i+1} \end{pmatrix} = A \begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix} \pmod 1 \tag{3}$$

其中矩阵 $A$ 使映射产生了混沌效应，其定义如下，详见文献[5]。

$$\begin{pmatrix} a_y + a_x a_z + a_x a_y a_z b_x \\ a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{pmatrix}$$

性。这里对可逆性的定义是：对于一个初始状态，经过一个细胞自动机的若干次演化后，若能找到另一个细胞自动机使其在相同的演化次数后回到初始状态，则这一对细胞自动机就具有可逆性。然而在初等细胞自动机中，并不是每一对局部规则都具有这种性质，这样的规则是有限的，并且寻找起来很困难[14]。所以本文利用了一种 2D 二阶细胞自动机，对于一个任意的二维细胞自动机局部规则都可以构造出一个可逆的规则。

在初等细胞自动机中，细胞 $S_i$ 在 $t+1$ 时刻的状态 $S_i^{t+1}$ 是由 $t$ 时刻此细胞和其邻居的状态根据局部规则决定的，即 $s_i^{t+1}=f(s_i^t)$，其中 $f$ 为局部状态转移函数。如果局部规则需要利用此细胞在 $t-1$ 时刻的状态，即 $s_i^{t+1}=f(s_i^t, s_i^{t-1})$，则原初等细胞自动机就扩展为了二阶细胞自动机。对于二维冯诺伊曼型邻居的细胞自动机，经过此扩展后，中心细胞有 5 个邻居，其局部规则有 $2^{2^{5+1}}=2^{64}$ 种。对这种 2D 二阶细胞自动机进行改进，在 $t$ 时刻细胞 $S_{(i,j)}$ 和其邻居状态不变的情况下，若 $t-1$ 时刻 $S_{(i,j)}$ 的状态不同，则 $t+1$ 时刻 $S_{(i,j)}$ 的状态也应该不同。可以证明这种 2D 二阶细胞自动机是可逆的[15]，并且其逆细胞自动机就是它自己。

表 1 列出了规则号 $r=F33F0F300CC0F0CF$(16 进制)的 2D 二阶细胞自动机所表示的局部状态转移规则。

表 1　局部规则状态转移表

| $S^t_{(i,j-1)}S^t_{(i-1,j)}S^t_{(i,j)}S^t_{(i+1,j)}S^t_{(i,j+1)}$ | $S^{t+1}_{i,j}$ ($S^{t-1}_{i,j}=0$) | $S^{t+1}_{i,j}$ ($S^{t-1}_{i,j}=1$) | $S^t_{(i,j-1)}S^t_{(i-1,j)}S^t_{(i,j)}S^t_{(i+1,j)}S^t_{(i,j+1)}$ | $S^{t+1}_{i,j}$ ($S^{t-1}_{i,j}=0$) | $S^{t+1}_{i,j}$ ($S^{t-1}_{i,j}=1$) |
|---|---|---|---|---|---|
| 00000 | 1 | 0 | 10000 | 0 | 1 |
| 00001 | 1 | 0 | 10001 | 0 | 1 |
| 00010 | 1 | 0 | 10010 | 0 | 1 |
| 00011 | 1 | 0 | 10011 | 0 | 1 |
| 00100 | 0 | 1 | 10100 | 0 | 1 |
| 00101 | 0 | 1 | 10101 | 0 | 1 |
| 00110 | 1 | 0 | 10110 | 1 | 0 |
| 00111 | 1 | 0 | 10111 | 1 | 0 |
| 01000 | 0 | 1 | 11000 | 0 | 1 |
| 01001 | 0 | 1 | 11001 | 0 | 1 |
| 01010 | 0 | 1 | 11010 | 1 | 0 |
| 01011 | 0 | 1 | 11011 | 1 | 0 |
| 01100 | 1 | 0 | 11100 | 0 | 1 |
| 01101 | 1 | 0 | 11101 | 0 | 1 |
| 01110 | 1 | 0 | 11110 | 0 | 1 |
| 01111 | 1 | 0 | 11111 | 0 | 1 |

## 3　加密方案描述

步骤 1　密钥产生阶段。选择一个长度为 288 位的比特流作为密钥 $key$，用来产生 3D 混沌映射的系数、迭代次数和细胞自动机演化规则的规则号。密钥生成算法为：对于前 7×32比特，每 32 比特表示一个整数，分别作为 3D 混沌映射的 6 个系数($a_x a_y a_z b_x b_y b_z$)和迭代次数 $t$，最后 64 位构成细胞自动机的规则号 $r$。

步骤 2　把明文图片的像素由二维变成三维(对于彩色RGB图像可以对每个通道分别处理),假设图片 $M$ 的长度和高度分别为 $W$ 和 $H$,以先行后列的次序依次提取图片的像素构成若干像素立方体,使其满足式(4)。

$$W\times H=2N_1^3+2N_2^3+\cdots+2N_k^3+R \tag{4}$$

把每个像素看做一个边长为 1 的小立方体,则 $N_i^3$ 是一个边长为 $N_i$ 的立方体的像素个数,$2N_i^3$ 表示两个这样的立方体,其中 $i\in[1,k]$。最后 $R\in(0,1,\cdots,15)$是无法分解的尾项,在之后的加密过程中不参与运算。

步骤 3　以一对相等体积的像素立方体为例,设其为 $Q$ 和 $Q'$,先对 $Q$ 用式(3)进行一次 3D 混沌映射得到 $Q_1$,即对像素立方体中的像素位置进行置乱。然后 $Q_1$ 和 $Q'$ 进行异或操作(XOR)得到 $Q_1'$,接着对 $Q_1'$进行 3D 混沌映射得到 $Q_2'$,最后 $Q_1$ 和 $Q_2'$进行异或操作(XOR)得到 $Q_2$。

步骤 4　把 $Q_2$ 和 $Q_2'$中的每个像素按位展开,构成二维平面,分别作为 2D 二阶细胞自动机演化的两个初始状态 $C_0$ 和 $C_1$,按照规则号 $r$ 以表 1 的形式对其进行演化,以函数来表示这种全局变化,从而得到 $C_{t+1}=G(C_t,C_{t-1})$,对两初始状态进行两次演化,结果为 $C_2$ 和 $C_3$。

步骤 5　把步骤 4 的结果再次变换为像素立方体,以此作为一次加密迭代,判断迭代次数是否达到 $t$ 次。若满足迭代次数,则根据式(4)逆向构造出密文图像;否则跳到步骤 3,进行下一轮迭代,直到满足次数为止。

尽管随着加密轮数的增加,加密的效果会有提高,但是由于时间和效率的原因,通常迭代 10 次左右就可以得到较好的结果,加密过程如图 3 所示。

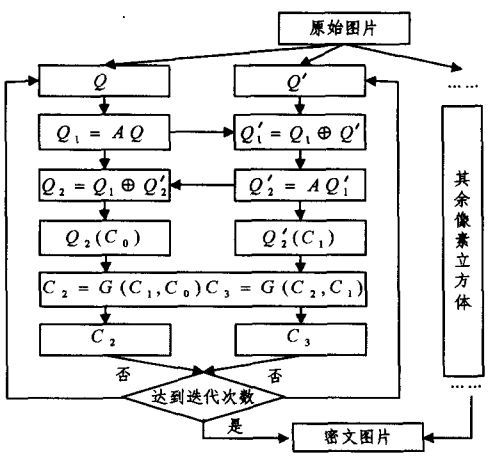



图 3　分块加密过程图示

解密时,由于 3D 混沌映射和 2D 二阶细胞自动机均是可逆的,因此对于密文图像,只需要根据密钥反向执行步骤 3 和步骤 4 的运算过程,直到规定的迭代次数即可解密,得到原始图像。

## 4　安全分析

### 4.1　密钥空间及敏感性分析

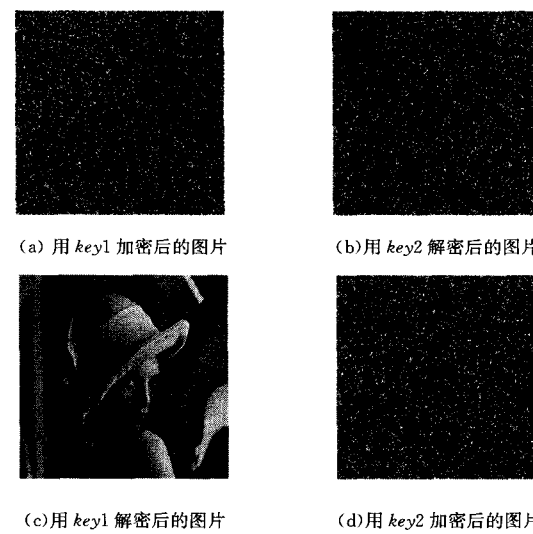
对于任何加密方案,密钥空间的大小直接决定了其安全性,当密钥空间较小时,就不可避免地会遭受暴力破解攻击。本文提出的方法中,密钥主要由 3 部分组成:(1)3D 混沌映射的系数($a_x a_y a_z b_x b_y b_z$);(2)细胞自动机演化的规则号 $r$;(3)加密时迭代的次数 $t$。

其中规则号 $r\in[0,2^{64}-1]$,其余每个整数的取值为[0,$2^{32}-1$]。所以整个密钥 $key$ 有 $32\times7+64=288$ 位,大于通常的加密方案,足以抵御暴力破解的攻击。表 2 比较了几种图像加密方案的密钥空间。

表 2　密钥空间对比

| 方案 | 本文方案 | 文献[1] | 文献[2] | 文献[3] |
|---|---|---|---|---|
| 密钥大小 | $2^{288}$ | $2^{280}$ | $2^{128}$ | $2^{157}$ |

由于混沌映射的特点,密钥的敏感性很高。图 4(a)是用密钥 $key1$($a_x=1,b_x=2,a_y=1,b_y=2,a_z=1,b_z=2,t=11$,$r$=F33F0F300CC0F0CE)进行加密后的结果,改变密钥的一位使 $r$=F33F0F300CC0F0CF,得到 $key2$。图 4(b)为采用密钥 $key2$ 解密 $key1$ 加密图像的结果,而图 4(c)则是采用正确密钥解密的结果。图 4(d)是用密钥 $key2$ 对图 4(c)进行加密的结果,经过与图 4(a)比较可知,在改变了一位密钥后,不同加密结果之间99.65%的像素都不同,说明本文算法的密钥敏感度很高。



(a) 用 $key1$ 加密后的图片　(b)用 $key2$ 解密后的图片

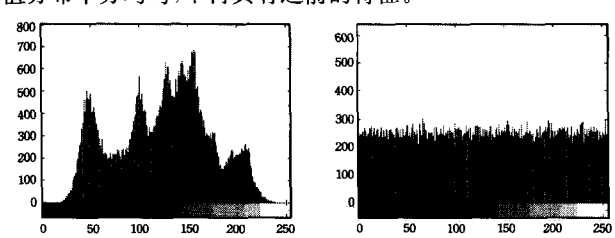
(c)用 $key1$ 解密后的图片　(d)用 $key2$ 加密后的图片

图 4　密钥敏感性实验

### 4.2　统计攻击分析

根据香农的理论,许多加密方案都可以利用统计分析作为其破解方法,所以一个加密方案要保证安全,就要能够抵御基于统计分析的攻击。对于图像加密而言,图像的灰度直方图以及图像像素间的相关性关系是两个最主要的统计特征,所以为了抵御统计分析攻击,一个良好的加密方案须能隐藏这种统计特征,而本文提出的方案正满足了这一点。

(1)加密图像的灰度直方图分析。选择 256×256 大小的灰度图 Lena 作为原始图片,并采用本方案对其加密,分别统计加密前后两者的灰度直方图,由图 5 可见,密文图片的灰度值分布十分均匀,不再具有之前的特征。



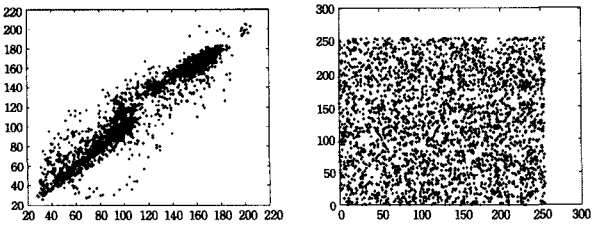

(a)原始图像灰度直方图　(b)密文图像灰度直方图

图 5　图像加密前后灰度直方图对比

(2)相邻像素相关性分析。为了分析两个相邻像素(包括垂直相邻、水平相邻、对角相邻、斜对角相邻)的相关性,分别从原始图片和加密图片中选择 3000 对相邻的像素,根据式(5)计算其相关性。

$$r_{xy}=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{5}$$

其中,$cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y))$,$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i$,$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2$。图 6 分别展示了原始图像和密文图像的相邻像素相关性,可以看出加密后的图像像素间不再具有可观察的相关性,表 3 展示了更多的实验结果。



(a)原始图像像素相关性　　(b)密文图像像素相关性

图 6　加密前后图像像素相关性对比

表 3　图像加密前后 3 个方向的像素相关度统计

| | 原始图像 | 密文图像 |
|---|---|---|
| 水平相关度 | 0.9581 | 0.0032 |
| 垂直相关度 | 0.9705 | 0.0037 |
| 对角线相关度 | 0.9540 | −0.0046 |

### 4.3　差分攻击分析

除了暴力攻击和统计分析攻击外,另一种常见的攻击加密方案的方法是差分攻击。通常攻击者会对原始图片进行微小的篡改(比如一个像素),然后观察加密后的密文图像之间的差别,从而寻找两者之间的相关性,进一步对加密系统进行破解。如果原始图像的微小改变能使加密后的图像有 50% 以上的像素发生改变,则此时差分攻击将变得低效甚至无用。

为了测试本文方案中当原始图片有一个像素改变时,密文图片像素改变的情况,我们利用两个指标来衡量,分别是像素数量变化率(NPCR)和统一平均变化率(UACI),其定义为式(6)和式(7):

$$NPCR=\frac{\sum_{i,j}D(i,j)}{W\times H}\times 100\% \tag{6}$$

$$UACI=\frac{1}{W\times H}\left[\sum_{i,j}\frac{|C(i,j)-C'(i,j)|}{255}\right]\times 100\% \tag{7}$$

其中,$W$ 和 $H$ 分别是图像的宽度和高度,$C(i,j)$和 $C'(i,j)$分别是原始图像和密文图像对应位置的像素值,对于灰度图像,其取值为 0 至 255。对于原图和密文图像同一位置$(i,j)$的两个像素,若 $C(i,j)=C'(i,j)$,则 $D(i,j)=1$,否则 $D(i,j)=0$。表 4 列出了利用本文算法进行加密后,图像的 NPCR 和 UACI 与其它方案的对比。

表 4　4 种加密方案的 NPCR 和 UACI 值的比较

| | 本文方案 | 文献[1] | 文献[10] | 文献[4] |
|---|---|---|---|---|
| NPCR(%) | 99.67 | 99.79 | 99.96 | 99.61 |
| UACI(%) | 33.34 | 33.35 | 33.44 | 33.47 |

结果显示,本文提出的加密方案的 NPCR 超过了 99%且 UACI 非常接近 33.33%。因此,提出的方案对原始图像的改变是非常敏感的,满足雪崩效应,可以很好地抵御差分攻击。

### 4.4　信息熵分析

信息熵的大小能够极佳地反映出随机性,是加密效果的一个重要特征。信息熵的计算通常利用式(8)表示。

$$H(m)=-\sum_{i=0}^{2^n-1}p(m_i)\log_2\frac{1}{p(m_i)} \tag{8}$$

其中,$m$ 为信息,$p(m_i)$表示符号 $m_i$ 出现的概率,熵的大小以比特来表示。当一个灰度值用 8 位表示时,若其出现情况是完全随机的,则熵为 8。通常情况下,这个值是小于 8 的,但越接近 8 越好。表 5 对比了本文加密方案和其他几种方案产生的密文图片的信息熵。

表 5　4 种加密方案产生的密文图片的信息熵对比

| 图片 | 本文方案 | 文献[1] | 文献[10] | 文献[4] |
|---|---|---|---|---|
| Lena | 7.9972 | 7.9992 | 7.9368 | 7.9997 |
| Sailboat | 7.9973 | 7.9973 | 7.9643 | 7.9957 |
| Pepper | 7.9970 | 7.9993 | 7.9487 | 7.9961 |

由表 5 可以看出,本文方案能够产生近乎随机的密文图像,很好地隐藏原始信息,几乎不会产生信息泄露。

**结束语**　本文创造性地结合了 3D 混沌映射和 2D 二阶细胞自动机在图像加密中的优点,设计并实现了一种新的图像加密方案,具有长达 288 位的密钥空间。相对于通常的加密方案,本方案可以在较少的迭代次数内达到理想的加密效果,并且不会带来密文图像的扩张。通过安全性实验分析可以发现,本文提出的方案具有较好的图像加密能力,在混淆度和置乱程度上都满足了加密算法的需求,可以抵御常见的暴力破解、统计分析和差分分析等攻击手段。未来希望能够进一步地提高其加密速度和安全性。

## 参 考 文 献


[1] Wang X, Luan D. A novel image encryption algorithm using chaos and reversible cellular automata[J]. Communications in Nonlinear Science and Numerical Simulation, 2013, 18(11): 3075-3085

[2] Patidar V, Pareek N K, Sud K K. A new substitution diffusion based image cipher using chaotic standard and logistic maps[J]. Commun Nonlinear Sci Numer Simul, 2009, 14(7): 3056-3075

[3] Patidar V, Pareek N K, Purohit G, et al. Modified substitution-diffusion image cipher using chaotic standard and logistic maps [J]. Commun Nonlinear Sci Numer Simul, 2010, 15(10): 2755-2765

[4] Kanso A, Ghebleh M. A novel image encryption algorithm based on a 3D chaotic map[J]. Commun Nonlinear Sci Numer Simul, 2012, 17(7): 2943-2959

[5] Chen G, Mao Y, Chui C. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos Soliton Fract 2004, 21: 749-761

[6] Peng Chuan, Li Yuan-xiang. Chaos and cellular automata based image encryption algorithm[J]. Computer Engineering and Design, 2012, 33(7): 2526-2529

[7] Von Neumann J, Burks A W. Theory of Self reproducing Automata[M]. USA: University of Illinois Press, 1966

[8] WolframS. Cryptography with cellular automata[C]// Crypto. 85. 1985: 429-432


(下转第 203 页)

安全态势感知内容做出更为及时的估计。

**结束语** 在网络安全态势感知中的数据融合的大背景下，本文针对 D-S 证据合成规则不能正确处理冲突证据的缺陷进行了深入的研究，针对冲突证据源的预处理提出了新的解决方法。最后利用数值算例进行了证明，结果表明本文方法能够有效地解决证据冲突问题，并且具有更好的收敛性和高效性，更加适用于网络安全态势感知环境。当然，我们也考虑过将证据支持度的处理方法运用到合成规则的改进上，但是还不够成熟。在下一步工作中，将着重针对合成规则本身的改进进行研究。

## 参 考 文 献


[1] Wang Ping, Zhu Xue-mei. Fact Reasoning with Reliable D-S Evidence Theory[C]// Proceedings of the 3rd International Conference on Intelligent Information Technology Application. 2009: 441-444

[2] 赵争业，夏远，钟求喜. 基于 D-S 证据理论的脆弱性态势数据融合方法研究[J]. 计算机应用与软件，2013，30(9)：80-86
Zhao Zheng-ye, Xia Yuan, Zhong Qiu-xi. Research on vulnerability situational data fusion method based on D-S evidence theory [J]. Computer Applications and Software, 2013, 30(9): 80-86

[3] 杨国胜，窦丽华. 数据融合及其应用[M]. 北京：兵器工业出版社，2004
Yang Guo-sheng, Dou Li-hua. Data Fusion and Its Application [M]. Beijing: Weapon Industry Press, 2004

[4] 刘效武. 基于多源融合的网络安全态势量化感知与评估[D]. 哈尔滨：哈尔滨工程大学，2009
Liu Xiao-wu. Network Security Situation Quantification Awareness and Evaluation Based on Multi-source Fusion[D]. Harbin: Harbin Engineering University, 2009

[5] Chen Yi, Huang Qing, Chen Yan-lan. An Improve Information Fusion Algorithm Based on BP Neural Network and D-S Evidence Theory[C]// 2012 Third International Conference on Digital Manufacturing & Automation. 2012: 179-181

[6] 朱静. 基于 D-S 证据理论的网络安全风险评估模型[D]. 保定：华北电力大学，2008
Zhu Jing. Network Security Risk Assessment Model Based on D-S Evidence Theory[D]. Baoding: North China Electric Power University, 2008

[7] Huang Yan-bo, Lan Yu-bin, Hoffmann W C, et al. Multisensor Data Fusion for High Quality Data Analysis and Processing in Measurement and Instrumentation[J]. Journal of Bionic Engineering, 2007, 4(1): 53-62

[8] Miao Yan-zi, Ma Xiao-ping, Zhang Jian-wei. Research on the Combination Rules of the D-S Evidence Theory and Improvement of Extension to Fuzzy sets[C]// Proceedings of 2010 Chinese Control and Decision Conference. 2010: 2143-2149

[9] Wu Wen-jie, Huang Da-gui, Dong Zheng. Fault Diagnosis of the Aeroengine Based on Neural Network and D-S Evidence Theory [C]// Proceedings of 2011 ICCSIT. 2011

[10] Xing Xiao-qin, Wang Wei-dong, Wang Zhe, et al. Weighted Cooperative Spectrum Sensing Based on D-S Evidence Theory and Double-Threshold Detection[C]// 2013 IEEE 5th International Symposium on Microware, Antenna, Propagation and EMC Technologies for Wireless Communication. 2013: 145-149

[11] 陈炜军，景占荣，袁芳菲，等. D-S 证据理论的不足及其数学修正[J]. 中北大学学报，2010，31(2)：162-168
Chen Wei-jun, Jing Zhan-rong, Yuan Fang-fei, et al. Shortcoming of D-S Evidence Theory and Its Mathematic Modification[J]. Journal of North University of China, 2010, 31(2): 162-168

[12] 王洪发，王先义. D-S 证据理论在多源数据融合中的应用及改进[J]. 现代电子技术，2009，32(15)：7-9
Wang Hong-fa, Wang Xian-yi. Development and Problems of D-S Evidential Reasoning in Multisensor Data Fusion[J]. Modern Electronics Technique, 2009, 32(15): 7-9

[13] Miao Yan-zi, Ma Xiao-ping, Zhang Jian-wei. Research on IDS Data Fusion Model Based on D-S Evidence Theory[C]// Proceedings of 2010 International Conference on Services Science. 2010

[14] Liu Ping, Zhang Ling-xiao, Yang Xin-feng. Data Fusion of Distributed D-S Evidence Theory Based on Predicted Reliability[C]// Proceedings of 2011 International Conference on Computer and Automation Engineering. 2011: 131-135

[15] 邓勇，施文康，朱振福. 一种有效处理冲突证据的组合方法[J]. 红外与毫米波学报，2004，23(1)：27-32
Deng Yong, Shi Wen-kang, Zhu Zhen-fu. Efficient combination approach of conflict Evidence[J]. Journal of Infrared and Millimeter Waves, 2004, 23(1): 27-32

[16] 关欣，衣晓，孙晓明，等. 有效处理冲突证据的融合方法[J]. 清华大学学报(自然科学版)，2009，12(1)：138-141
Guan Xin, Yi Xiao, Sun Xiao-ming, et al. Fusion Method of Conflict Evidence[J]. Journal of Tsinghua University (Science and Technology), 2009, 12(1): 138-141


(上接第 185 页)


[9] Xia Xue-wen, Li Yuan-xiang, Zeng Hui. Data Encryption Algorithm Based on Two Dimension Toggle Cellular Automata[J]. Computer Science, 2010, 37(3): 46-48

[10] Abdo A A, Lian S G, Ismail I A, et al. A cryptosystem based on elementary cellular auto-mata[J]. Commun Nonlinear Sci Numer Simul, 2013, 18(1): 136-147

[11] Chen R J, Lai J L. Image security system using recursive cellular automata substitution[J]. Patter Recognit, 2007, 40(5): 1621-1631

[12] Seredynski M, Pienkosz K, Bouvry P. Reversible cellular automata based encryption[M]// Network and Parallel Computing. Springer, 2004: 411-418

[13] Chen G, Dong X. From chaos to order: methodologies, perspectives and applications[M]. Singapore: World Scientific, 1998

[14] Kari J. Reversibility and surjectivity problems of cellular automata[J]. Journal of Computer and System Sciences, 1994, 48(1): 149-182

[15] Toffoli T, Margolus N H. Invertible cellular automata: A review [J]. Physica D: Nonlinear Phenomena, 1990, 45(1): 229-253