# 基于改进 Clifford 混沌系统的图像加密算法*

张文宇,幸荣盈,李国东
(桂林电子科技大学 数学与计算科学学院,广西 桂林 541004)

**摘 要:** 信息安全是人们日益关注的问题,在大数据时代,很多信息的传输都是通过数字图像进行的。为了减少数字图像在信息传递过程中存在的安全隐患,改进了 Clifford 系统,通过混沌吸引子图和 Lyapunov 指数分析改进的 Clifford 系统的混沌特性,并且基于改进的 Clifford 系统设计了一种图像加密新算法。该算法先将明文图像像素矩阵转化为二进制矩阵,对二进制矩阵的行和列分别进行循环位移;然后再将明文图像分成 9 个大小不同的矩阵块,对每个矩阵块进行置乱操作,在块置乱时,块间结合混沌序列进行置乱,块内进行循环位移,保证了每个像素点的位置都发生了变化;最后用混沌序列和置乱后的图像进行异或运算,得到最终的密文图像。仿真实验以及安全性分析说明该算法具有良好的加密效果。

**关键词:** 混沌系统;Clifford 系统;图像加密;分块置乱;扩散
**中图分类号:** TP391 **文献标识码:** A **DOI:** 10.16157/j.issn.0258-7998.211584

**中文引用格式:** 张文宇,幸荣盈,李国东. 基于改进 Clifford 混沌系统的图像加密算法[J].电子技术应用,2022,48(6):73-78.
**英文引用格式:** Zhang Wenyu,Xing Rongying,Li Guodong. Image encryption algorithm based on improved Clifford chaotic system[J]. Application of Electronic Technique,2022,48(6):73-78.

# Image encryption algorithm based on improved Clifford chaotic system

Zhang Wenyu,Xing Rongying,Li Guodong
(School of Mathematics and Computing Science,Guilin University of Electronic and Technology,Guilin 541004,China)

**Abstract:** Information security is an increasingly concerned issue. As the carrier of information transmission, digital image contains a large amount of information. In order to improve the security of digital image transmission, this paper improves the Clifford system, analyzes the chaotic characteristics of Clifford system through chaotic attractor graph and Lyapunov exponent, and designs a new image encryption algorithm based on the improved Clifford system. Firstly, the plaintext is transformed into a binary matrix. The rows and columns of the binary matrix are circularly shifted. Then, the plaintext is divided into nine matrix blocks with different sizes, and each matrix block is scrambled. In block scrambling, chaotic sequences are used to scramble between blocks, while cyclic displacement scrambling is used to scramble within blocks which ensures that the position of each pixel has changed. Finally, the image is diffused to get the ciphertext. Simulation experiments and security analysis show that the algorithm is safe and reliable for image encryption.

**Key words:** chaotic system;Clifford system;image encryption;block scrambling;diffuse

## 0 引言

大数据时代的发展有利有弊,信息高速传递的时候也导致了大量的安全漏洞,越来越多的学者也将保护数据化的隐私问题当成核心研究。与文字信息相比,数字图像相邻像素间的相关性较大、所含信息容量大并且数据冗余性强,所以数字图像加密不适合应用传统加密技术(如 AES 和 DES)。而混沌系统有伪随机性和初始值很敏感等特性,很适合用来图像加密,而应用混沌系统对图像加密也成为现代科研的热点。赵洪祥等人[1]针对以往的 Henon 映射存在的混沌空间小,在加密时安全性低的问题,对传统的 Henon 映射进行了创新,并利用创新型 Henon 映射对图像进行加密,其采用分块的方式对图像进行加密处理,很大程度上减少了算法的运行时间;马开运等人[2]针对明文图像与加密密钥无关引起的安全性问题,提出了将 Logistic 映射所迭代的混沌序列和明文图像相结合生成的密钥当作三维 Chen 系统迭代的初始值,再运用 Fisher-Yates 算法对图像进行置乱操作,该算法可以抵御大多数攻击;Wang 等人[3]针对低维混沌系统安全性不高,设计了一个新型的六维混沌系统,结合比特置乱和 DNA 编码技术对图像进行加密;Xian 等

* 基金项目:国家自然科学基金(11461063)

人[4]提出一种基于螺旋变换的置乱方法，该方法在一次加密过程中可以引起所有像素点位置的变化，巧妙地简化了图像置乱过程。扩散算法利用两个混沌序列来提高扩散过程的效率。

对图像加密常用的操作主要有两种：(1)置乱，即打乱图像像素点的初始位置；(2)扩散，即改变图像像素值的大小。目前，针对应用混沌系统进行图像加密算法设计研究中所存在的混沌系统低维、加密步骤过于简单而使安全性低以及加密步骤过于繁琐而导致的加密效率不高等问题，本文改进了 Clifford 系统，并利用改进的 Clifford 系统对图像进行加密。先将原图的像素图像转化为二进制，再分别对行和列进行循环位移置乱，然后对所得图像进一步分块置乱，最后利用混沌序列进行扩散。仿真实验所得结果表明该算法具有较高的安全性，可以抵抗各种典型攻击。

## 1 Clifford 系统

目前，Lyapunov 指数可以用来鉴定一个系统是否混沌的。若该指数为正值，则说明这个系统为混沌系统；若存在两个及以上大于零的 Lyapunov 指数，那么可以说这个系统是超混沌的[5-7]。

Clifford 系统的表达式如下：

$$\begin{cases} x_{k+1}=\sin(ay_k)-z_k\cos(bx_k) \\ y_{k+1}=z_k\sin(cx_k)-\cos(dy_k) \\ z_{k+1}=e\sin(bx_k) \end{cases} \tag{1}$$

当给出式(2)的初始值时，系统(1)处于超混沌状态。

$$\begin{cases} x=-10 \\ y=-0.1 \\ z=-1.0 \\ a=2.24 \\ b=0.43 \\ c=-0.65 \\ d=-2.43 \\ e=1.0 \end{cases} \tag{2}$$

此时，使用雅克比矩阵乘积方法计算出系统的近似 Lyapunov 指数分别为 0.0836、0.2924 和 0.4518[5]。因此，可以将 Clifford 系统用于图像加密。利用式(2)的参数和初始值，将 Clifford 系统迭代 1 000 次的混沌吸引子图如图 1 和图 2 所示。

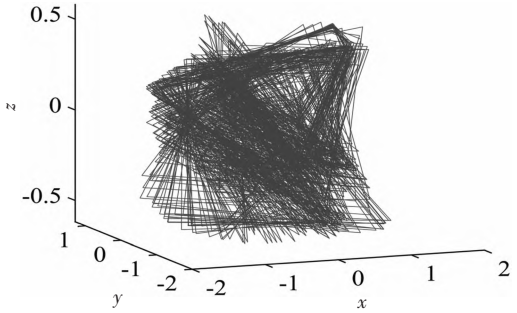



图 1 Clifford 系统

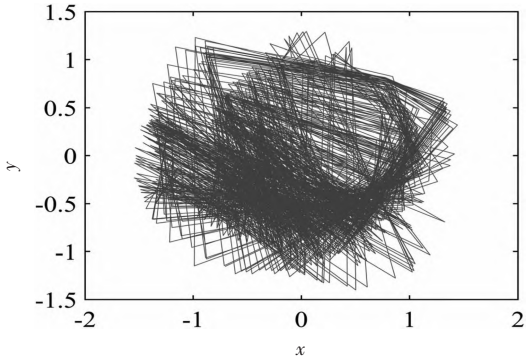



图 2 Clifford 系统 $X$、$Y$ 方向相图

由图 1 可以看出混沌吸引子中间是空心的，有一块空白区域；图 2 是 Clifford 系统在 $X$、$Y$ 方向的分布，可以看出混沌系统的分布并不均匀。

## 2 基于改进 Clifford 系统的伪随机序列发生器设计

### 2.1 改进的 Clifford 系统

由于 Clifford 系统的控制参数有 5 个，那么用其进行混沌加密时所需设置的密钥会比较多。所以针对 Clifford 系统混沌吸引子分布不均且初始参数较多这两点问题，对 Clifford 系统进行改进，让它的分布比较均匀并且减少控制系统的参数。改进的 Clifford 系统表达式如式(3)所示。

$$\begin{cases} x_{k+1}=\sin(ay_k)-bz_k \\ y_{k+1}=z_k(\sin(cx_k)-\cos y_k)\cos(\dfrac{1}{z_k}) \\ z_{k+1}=\arctan(bx_k)\sin(\dfrac{1}{y_k}) \end{cases} \tag{3}$$

利用式(4)作为改进 Clifford 系统的迭代的初始值，图 3 是改进 Clifford 系统的混沌吸引子图。

$$\begin{cases} x=8.28 \\ y=-5.71 \\ z=-0.99 \\ a=3.89 \\ b=0.51 \\ c=2.73 \end{cases} \tag{4}$$

由图 3 与图 4 可观察到改进的 Clifford 系统在空间上的分布更加均匀、遍历性更好。此时，计算出的系统近

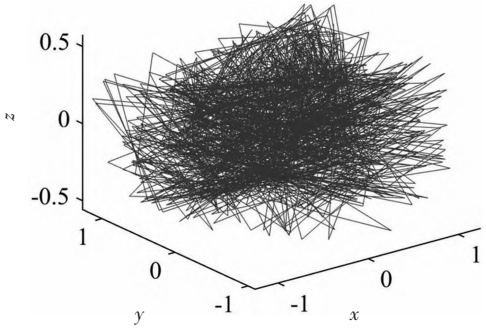



图 3 改进 Clifford 系统

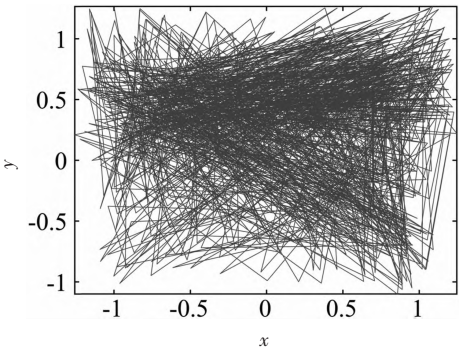



图 4　改进 Clifford 系统 $X$、$Y$ 方向相图

似的 Lyapunov 指数为 0.2213、0.2187、0.1878，说明改进的 Clifford 系统是超混沌系统，具有良好的混沌特性，适合用来进行图像加密。

由图 1 可以看出混沌吸引子中间是空心的，有一块空白区域，图 2 是 Clifford 系统在 $X$、$Y$ 方向的分布，可以看出混沌系统的分布并不均匀。

### 2.2 伪随机序列的获取

为了增加密钥敏感性，达到一图一密的效果，将明文图像和密钥联系起来，根据明文图像得到混沌系统迭代的初始值。给定一个 $m\times n$ 平面图像 $\boldsymbol{A}$，计算 $\boldsymbol{A}$ 中像素的均值 $m_0$，根据式(3)计算混沌系统(2)的初始值 $x_1$、$x_2$、$x_3$。

$$\begin{cases} x_1=\dfrac{m_0}{2^8} \\ x_i=\mathrm{mod}(x_{i-1}\times 10^6,1) \quad i=2,3 \end{cases} \tag{5}$$

令混沌系统的初始控制参数为 $a=3.89$，$b=0.51$，$c=2.73$，迭代混沌系统(3)$200+m\times n$ 次，为了消除瞬态效应，抛弃前 200 个值生成 3 个混沌序列 $\boldsymbol{X}$、$\boldsymbol{Y}$ 和 $\boldsymbol{Z}$，其中，每个混沌序列所包含 $m\times n$ 个元素。为了解决混沌序列所存在的局部连续性问题，对混沌序列 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$ 做离散化处理如式(6)和式(7)所示，得到 $\boldsymbol{T}_1$ 和 $\boldsymbol{T}_2$ 两个混沌序列。选择混沌序列 $\boldsymbol{T}_1$ 的奇数项元素和 $\boldsymbol{T}_2$ 的偶数项元素构成序列 $\boldsymbol{D}_1$。

$$\boldsymbol{T}_1=\mathrm{abs}(\boldsymbol{X})-\mathrm{fix}(\mathrm{abs}(\boldsymbol{X})) \tag{6}$$

$$\boldsymbol{T}_2=\mathrm{abs}(\boldsymbol{Y})-\mathrm{fix}(\mathrm{abs}(\boldsymbol{Y})) \tag{7}$$

并对于序列 $\boldsymbol{D}_1$ 做以下处理：

$$B_1=\mathrm{mod}(\mathrm{ceil}(\boldsymbol{D}_1\times 10^6),7)+1 \tag{8}$$

将混沌序列 $\boldsymbol{X}$ 的每个元素与混沌序列 $\boldsymbol{Y}$ 的每个元素对应相乘构成混沌序列 $\boldsymbol{D}_2$，选取 $\boldsymbol{D}_2$ 的后 8 个数构成序列 $\boldsymbol{D}_3$ 并对序列 $\boldsymbol{D}_3$ 做以下处理：

$$B_2=\mathrm{mod}(\mathrm{ceil}(\boldsymbol{D}_3\times 10^7),m\times n-1)+1 \tag{9}$$

其中，abs(·)表示取绝对值，fix(·)表示向 0 靠近取整，ceil(·)表示向上取整，mod(·)是取模运算。

## 3 基于改进 Clifford 系统的随机分块置乱算法设计

在混沌序列 $\boldsymbol{X}$ 中选取前 8 个偶数项元素组成一维向量 $\mathbf{XS}=(\mathrm{xs}_1,\mathrm{xs}_2,\mathrm{xs}_3,\mathrm{xs}_4,\mathrm{xs}_5,\mathrm{xs}_6,\mathrm{xs}_7,\mathrm{xs}_8)$，并对序列 $\mathbf{XS}$ 进行处理，如式(10)所示。

$$B_3=\mathrm{mod}(\mathrm{ceil}((\mathrm{abs}(\mathbf{XS})-\mathrm{ceil}(\mathrm{abs}(\mathbf{XS})))\times 10^{12}),n-2) \tag{10}$$

令 $\boldsymbol{d}=\max(B_1(2i-1),B_1(2i))+1$，其中，max(·)是取最大值函数，$i=1,2,3,4$，$\boldsymbol{d}$ 是一个 1×4 的一维向量。

利用将图像分为 9 个尺寸不同的矩阵块，具体分块模型如图 5 所示。

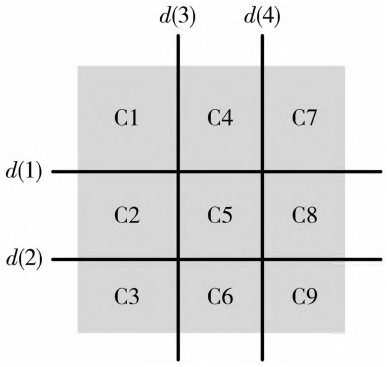



图 5　分块模型

在混沌序列 $\boldsymbol{Y}$ 中选取前 9 个奇数项元素组成一维向量 $\mathbf{YS}=(\mathrm{ys}_1,\mathrm{ys}_2,\mathrm{ys}_3,\mathrm{ys}_4,\mathrm{ys}_5,\mathrm{ys}_6,\mathrm{ys}_7,\mathrm{ys}_8,\mathrm{ys}_9)$，然后对 $\mathbf{YS}$ 中的元素进行升序排列，记其索引序列为 $\boldsymbol{S}_0$，再将 $\boldsymbol{S}_0$ 按照一列接一列的方式重构成 3×3 大小的索引矩阵 $\boldsymbol{S}$，使用索引矩阵 $\boldsymbol{S}$ 对矩阵块进行置乱操作，具体块置乱情况如图 6 所示。

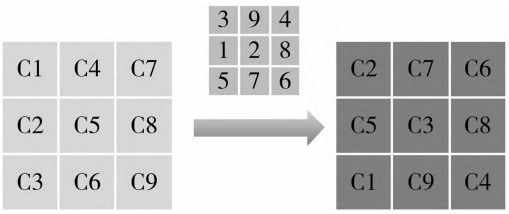



图 6　块间置乱

依次统计每一个矩阵块中奇数像素的个数 $u_1$ 和偶数像素的个数 $u_2$，如果 $u_1>u_2$，则对其矩阵块中的元素按照列逆时针循环移动一位；如果 $u_1<u_2$，则对其矩阵块中的元素按照行顺时针循环移动一位。把每一个矩阵块内部的像素点按照一列接一列的方式重构成一维行向量。再将所有的行向量组合成一个大小为 $1\times mn$ 的一维行向量，最后将这个一维向量重构成大小为 $m\times n$ 的矩阵 $\boldsymbol{Q}$，则 $\boldsymbol{Q}$ 为置乱后的图像。

## 4 加密算法设计

### 4.1 加密算法

(1)基于原图像素矩阵 $\boldsymbol{A}$ 计算混沌系统的初始值，并将 $\boldsymbol{A}$ 转化为一维向量 $\boldsymbol{P}=(p_1,p_2,\cdots,p_{m\times n})$。

(2)将 $\boldsymbol{P}$ 转为二进制矩阵得到矩阵 $\boldsymbol{A}_1$，$\boldsymbol{A}_1$ 第 $i$ 行行向量按照顺时针循环移动 $\boldsymbol{B}_1(i)$ 个位置得到 $\boldsymbol{A}_2$，再将 $\boldsymbol{A}_2$ 第 $j$ 列列向量按照顺时针循环移动 $\boldsymbol{B}_2(j)$ 个位置得到矩阵 $\boldsymbol{A}_3$。

(3)把 $A_3$ 转化为十进制矩阵，并将按照一列接一列的方式将其重构为大小为 $m\times n$ 的矩阵 $A_4$，利用向量 $d$ 将 $A_4$ 划分为 9 个大小不同的矩阵块，用上述的随机分块置乱算法对 $A_4$ 进行像素置乱得到 $A_5$。

(4)对混沌序列 $Z$ 进行以下处理：

$$T_3=\mathrm{mod}(\mathrm{floor}(Z\times 10^{15}),256) \tag{11}$$

其中，floor(·)表示向下取整。将 $T_3$ 重构成一个 $m\times n$ 大小的混沌矩阵 $F$ 进行扩散变换，具体操作如下所示：

$$H=F\oplus A_5 \tag{12}$$

则 $H$ 为最终的密文图像，其中⊕表示异或操作，图7是本文加密算法的流程图。

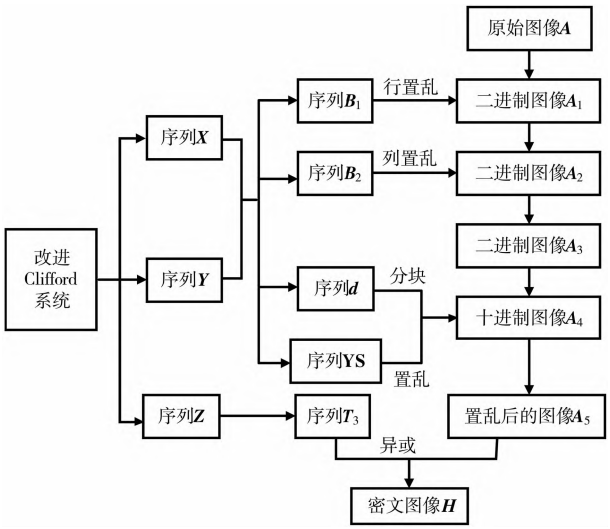



图 7 加密流程图

### 4.2 解密算法

解密算法是加密算法的逆过程，先由密文图像像素矩阵 $H$ 与 $F$ 进行异或运算，然后对扩散后的图像进行分块置乱的逆运算，再将所得矩阵转成二进制进行循环位移逆操作，最后把二进制矩阵转成十进制矩阵就是最终解出来的明文图像。

## 5 仿真实验分析

为了验证本文加密算法的安全性，选择 256×256 的“Lena”“Cameraman”“Airplane”图像，明文图像如图 8(a)、(b)、(c)所示，密文图像如图 8(d)、(e)、(f)所示。加密后的密文图像呈现出雪花状的噪声信号形式，完全看不出原图的特征。

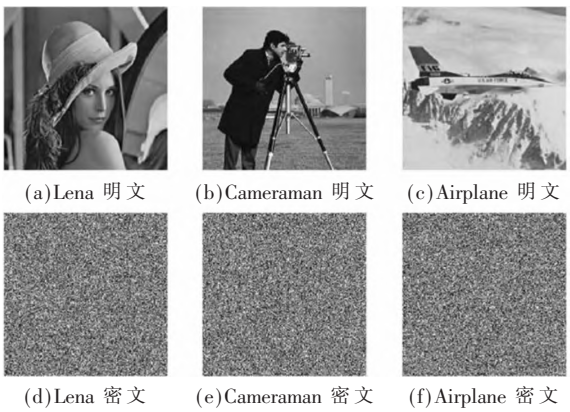
### 5.1 密钥空间

本文中，明文图像像素均值 $m_0$ 和混沌系统控制参数 $a$、$b$、$c$ 组成了算法的密钥。若 $m_0$ 全部可取的值为 $m_0'$，并且使用精度 $10^{16}$ 来估计，则密钥空间可达 $10^{48}\times m_0'$。由此可见本文算法的密钥空间足够大。

### 5.2 统计分析

#### 5.2.1 直方图

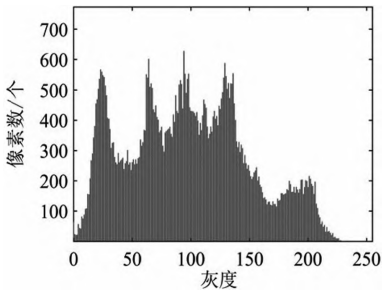
明文图像像素灰度值的分布普遍都具有一定的特点。因此，若图像像素灰度值分布得越匀称表明算法越有效。图 9 是 Lena 图像明文和密文的直方图。图 9(a)反映出像素值分布的平滑、均匀程度都很差；而图 9(b)密文图像像素直方图分布比较平缓，分布均匀。由此看出本文算法不会轻易被破解。



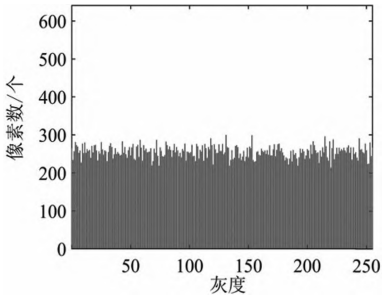
(a)Lena 明文　(b)Cameraman 明文　(c)Airplane 明文

(d)Lena 密文　(e)Cameraman 密文　(f)Airplane 密文

图 8 仿真结果




(a)明文图像




(b)密文图像

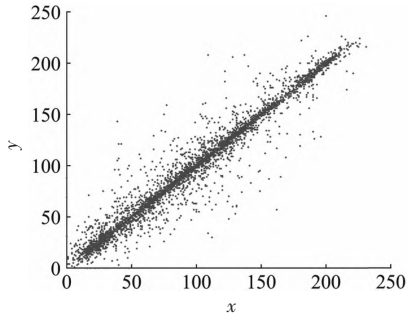
图 9 明密文图像直方图

#### 5.2.2 相邻像素相关性分析

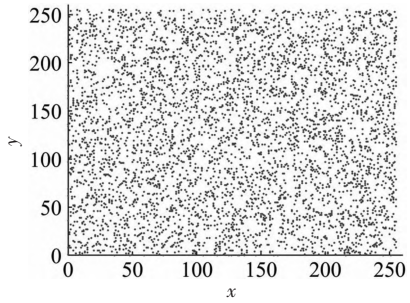
若加密后图像相邻像素对的相关系数几乎为 0，那么说明算法的置乱功效不错。

图 10 是 Lena 明文和密文图像相邻像素在水平方向上的分布情况。由图 10(a)可以看出明文图像相邻像素对基本分布在一条直线上，说明相邻像素的相关性很强；而图 10(b)密文图像相邻像素对均匀分布在矩形区域内，说明相邻像素对间几乎没有相关性。

表 1 是本文算法加密后的 Lena 图像相邻像素对之间的相关系数，加密后图像相邻像素的相关系数基本接




(a)明文图像




(b)密文图像

图 10 明密文图像水平方向相关分布情况

表 1 相关系数

| 算法 | 水平 | 垂直 |
|---|---|---|
| 本文 | 0.005 0 | −0.006 6 |
| 文献[3] | 0.008 5 | 0.005 4 |
| 文献[5] | 0.002 3 | −0.012 9 |
| 文献[8] | 0.021 4 | 0.046 5 |
| 文献[9] | −0.001 8 | 0.034 5 |
| 文献[10] | 0.006 4 | −0.036 8 |

近于 0,说明本文算法可以进行有效的加密。

### 5.3 信息熵分析

信息熵反映图像信息的不确定性[6],计算公式为:

$$H=-\sum_{i=0}^{255}p(i)\log2(p(i)) \tag{13}$$

其中,$p(i)$表示像素灰度值为 $i$ 出现的概率。对于一幅8 bit的灰度图像,信息熵理论值为 8。表 2 给出了应用本文算法对 Lena 和 Airplane 进行加密得到的信息熵,相较于其他文献更接近于 8。由此可见,本文算法加密的图像能抵御熵攻击。

表 2 信息熵

| 算法 | Lena | Airplane |
|---|---|---|
| 本文 | 7.997 5 | 7.997 3 |
| 文献[1] | 7.997 0 | – |
| 文献[2] | 7.996 6 | – |
| 文献[9] | 7.996 9 | 7.997 0 |
| 文献[11] | 7.997 4 | 7.997 3 |
| 文献[12] | 7.997 3 | 7.997 1 |

### 5.4 差分攻击测试

差分攻击是检验算法对明文敏感性的重要分析法。一般用像素变化率(NPCR)来度量加密算法对明文图像的敏感程度,NPCR 的计算公式如下:

$$\mathrm{NPCR}=\frac{\sum_{i,j}D(i,j)}{M\times N}\times100\% \tag{14}$$

其中,$M$ 表示原始图像的宽,$N$ 表示原始图像的长。对于有效加密算法,NPCR 值理论上接近 0.996 1 [7]。表 3 是 Lena 图像加密不同次数所计算的 NPCR 值。

由表 3 可知本文算法的 NPCR 平均值为 99.5949%,本文算法对明文图像敏感,能够有效地抵抗差分攻击。

表 3 明文敏感性测试结果

| 算法 | 加密轮次 | NPCR/% |
|---|---|---|
| 本文 | 2 | 99.594 1 |
| | 12 | 99.595 6 |
| | 平均值 | 99.594 9 |
| 文献[3] | | 99.636 0 |
| 文献[11] | | 99.600 0 |
| 文献[13] | | 99.610 5 |
| 文献[14] | | 99.190 0 |
| 文献[15] | | 99.630 0 |

## 6 结论

本文提出了一种基于改进 Clifford 系统的图像加密新算法,对 Clifford 系统做出改进,从混沌吸引子图和 Lyapunov 指数说明改进的 Clifford 系统的混沌特性。利用改进的 Clifford 系统所迭代的 3 个混沌序列对图像进行加密。首先,将明文图像转化为二进制,分别对行和列进行循环位移操作;然后将图像化分为 9 个大小不同的矩阵块,矩阵块的大小是根据混沌序列的元素变化而变化的,并且结合混沌序列的索引序列进行块间置乱;再利用循环位移对每个块内的像素点进行置乱,既保证了每个像素点发生变化,又提高了处理图像的效率;最后,利用剩余的混沌序列与置乱后的图像进行异或运算得到最终的密文图像。仿真实验结果以及安全性分析表明,该算法具有以下特点:(1)改进的 Clifford 系统具有良好的混沌特性,其生成的混沌序列可用于图像加密领域;(2)可以抵抗各种攻击,不会被攻击者轻易破解,具有较高的安全性。

### 参考文献

[1] 赵洪祥,谢淑翠,张建中,等.基于改进型 Henon 映射的快速图像加密算法[J].计算机应用研究,2020,37(12):3726-3730.

[2] 马开运,滕琳,孟娟.费雪耶兹算法结合混沌理论的图像加密方案[J].软件导刊,2020,19(11):189-196.

[3] WANG T,WANG M H .Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding[J].

Optics & Laser Technology, 2020, 132(2): 106355.
[4] XIAN Y, WANG X, YAN X, et al. Image encryption based on Chaotic sub-block scrambling and Chaotic digit selection diffusion[J]. Optics and Lasers in Engineering, 2020, 134(1-2): 106202.
[5] 杨雪松, 于万波, 魏小鹏. 基于复合超混沌系统且与明文相关联的图像加密[J]. 计算机应用研究, 2011, 28(10): 3807-3810.
[6] 董小雨, 冯秀芳. 基于动态密钥的彩色图像扩散加密算法[J]. 计算机工程与设计, 2021, 42(5): 1383-1391.
[7] MATHIVANAN P, GANESH A B. QR code based color image stego-crypto technique using dynamic bit replacement and logistic map[J]. Optik, 2021, 225: 165838.
[8] ZHEN P, ZHAO G, MIN L, et al. Chaos-based image encryption scheme combining DNA coding and entropy[J]. Multimedia Tools and Applications, 2016, 75(11): 6303-6319.
[9] PARVIN Z, SEYEDARABI H, SHAMSI M. A new secure and sensitive image encryption scheme based on new substitution with chaotic function[J]. Multimedia Tools and Applications, 2014, 75(17): 10631-10648.
[10] 费敏, 李国东. 基于 L-R 混沌系统和双重扩散的图像加密算法[J]. 新疆大学学报(自然科学版)(中英文), 2021, 38(3): 290-299, 333.
[11] UR REHMAN A, Di Xiao, KULSOOM A, et al. Block mode image encryption technique using two-fold operations based on chaos, MD5 and DNA rules[J]. Multimedia Tools and Applications, 2019, 78(7): 9355-9382.
[12] UR REGMAN A, Liao Xiaofeng, HAHSMI M A, et al. An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos[J]. Optik: Journal for Light- and Electronoptic, 2018, 153: 117-134.
[13] YU J, GUO S, SONG X, et al. Image parallel encryption technology based on sequence generator and Chaotic measurement matrix[J]. Entropy, 2020, 22(1): 76.
[14] 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.
[15] 韩雪娟, 李国东. 动态猫变换和混沌映射的图像加密算法[J]. 计算机工程与设计, 2020, 41(8): 2381-2387.

(收稿日期: 2021-04-01)

**作者简介:**

张文宇(1996-), 女, 硕士, 主要研究方向: 图像处理、混沌密码学。

幸荣盈(1998-), 女, 硕士, 主要研究方向: 数据挖掘。

李国东(1972-), 通信作者, 男, 博士, 教授, 主要研究方向: 图像处理、数据挖掘, E-mail:lgdzhy@126.com。

扫码下载电子文档

(上接第 68 页)

chronous panel discussion: What are Cloud-Native applications[J]. IEEE Cloud Computing, 2017, 4(5): 50-54.
[9] 高宇. 基于云原生的拓扑服务系统的设计与实现[D]. 成都: 西南交通大学, 2016.
[10] 梁伟, 杨明川, 冯明. 应用性能管理技术的研发与应用[J]. 电信技术, 2017(6): 42-45.

(收稿日期: 2021-06-06)

**作者简介:**

陈波(1989-), 女, 硕士研究生, 工程师, 主要研究方向: 计算机应用技术及网络安全。

吴云峰(1977-), 男, 硕士研究生, 正高级工程师, 主要研究方向: 控制工程及网络安全。

卢凯(1977-), 男, 本科, 高级工程师, 主要研究方向: 控制工程及网络安全。

扫码下载电子文档

(上接第 72 页)

[10] 李虹, 陆培培. 基于 Unity3D 的虚拟动画系统设计[J]. 现代电子技术, 2021, 44(8): 5.
[11] 闫兴亚, 王馨梅, 魏梦婕. 基于虚拟现实的丝绸之路交互系统的设计与开发[J]. 计算机与数字工程, 2020, 48(4): 838-842.
[12] 李卫强, 曹辉. VR 机舱人机交互姿态追踪器的算法设计[J]. 船海工程, 2018, 47(4): 4.
[13] YANG Y, WENG D, LI D, et al. An improved method of pose estimation for lighthouse base station extension[J]. Sensors(Basel), 2017, 17(10): 2411.
[14] 胡文东, 张利利, 马进, 等. 人体剩余能力检测装置及其灯控阵列: 中国, CN103417227[P]. 2013-12-04.
[15] 唐孟军, 胡文东, 马进, 等. 地面模拟航空险情及有效性评价[J]. 中华航空航天医学杂志, 2017, 28(2): 5.

(收稿日期: 2021-05-19)

**作者简介:**

丛林(1989-), 男, 硕士研究生, 助理研究员, 主要研究方向: 人因与工效学、应用心理学。

杨菁华(1983-), 女, 硕士, 副教授, 主要研究方向: 应用心理学、高教英语。

孙继成(1989-), 通信作者, 男, 博士研究生, 助理研究员, 主要研究方向: 人因与工效学、应用心理学, E-mail: sjcfmmu@163.com。

扫码下载电子文档