

## Image Encryption Algorithm Based on Improved Joseph Traversal and Piecewise Logistic Mapping\*

ZHAO Xiaolong<sup>1</sup>, LI Bo<sup>1\*</sup>, JIA Peng<sup>1</sup>, YANG Yaosen<sup>2</sup>

(1. Key Laboratory of Instrumentation Science & Dynamic Measurement of Ministry of Education, North University of China, Taiyuan Shanxi 030051, China; 2. North Institute of Automatic Control Technology, Taiyuan Shanxi 030051, China)

**Abstract:** In order to meet the security of network communication and image transmission, an image encryption algorithm with improved Joseph traversal and segmented logistic mapping is proposed. In the process of scrambling, the global pixel scrambling of the encrypted image is performed by improving Joseph traversal. The image is decomposed into two four-bit high and low matrices. The low four-bit matrix uses the segmented logistic chaotic map to perform the diffusion operation. The high four-bit matrix is changed to the original matrix by XOR operation, and then the two four-bit matrices are combined to obtain encryption image. The improved Joseph traversal can effectively resist periodic attacks. The segmented logistic mapping introduces the element value of the image to enhance the uniqueness of the key. The experimental results prove that the encryption algorithm has a large key space and good security performance, which can resist various attacks such as exhaustion and histogram statistics.

**Key words:** piecewise logistic; Joseph traversal; image encryption; introducing image element; exclusive or operation  
EEACC: 6135; 0290Z doi: 10.3969/j.issn.1005-9490.2021.01.024

## 改进约瑟夫遍历和分段 Logistic 映射的图像加密算法\*

赵晓龙<sup>1</sup>, 李博<sup>1\*</sup>, 贾芃<sup>1</sup>, 杨耀森<sup>2</sup>

(1. 中北大学仪器科学与动态测试教育部重点实验室, 山西太原 030051; 2. 北方控制技术研究所, 山西太原 030051)

**摘要:** 为了满足网络通信和图像传输的安全, 提出了一种改进约瑟夫遍历和分段 Logistic 映射的图像加密算法, 在置乱过程中通过改进约瑟夫遍历对待加密图像进行全局像素置乱, 将置乱像素按照矩阵排列, 分解成两个四位的高低矩阵, 低四位矩阵利用分段的 Logistic 混沌映射进行加密处理, 对高四位矩阵通过异或运算改变原来矩阵, 再将两个四位矩阵结合起来得到加密图像。改进的约瑟夫遍历可以有效抵御周期性攻击, 分段 Logistic 映射引入图像的元素值增强了密钥的独特性, 实验结果证明, 该加密算法密钥空间大, 安全性能好, 可以抵御穷举, 直方图统计等各种攻击。

**关键词:** 分段 Logistic; 约瑟夫遍历; 图像加密; 引入图像元素; 异或运算

中图分类号: TP309.7

文献标识码: A

文章编号: 1005-9490(2021)01-0125-06

随着互联网技术和多媒体技术的快速发展, 人与人之间交流方式也发生了很大变化, 数字图像能够生动地表达人们的意思, 因此图像传输也成为信息交流的主要方法之一。但传输过程如果不对图像进行加密处理, 很容易被窃取和盗用。数字图像其实就是二维的序列, 其数据内容丰富, 包含信息量大。传统的加密算法会导致计算量大, 效率低, 难以适应现在图像加密的需求。而混沌系统具有于随机性, 遍历性, 规律性等优点, 同时具有初值敏感性和伪随机性等特征, 可以产生复杂多变的伪随机序列, 使得混沌系统非常适合应用于图像加密。

近些年来, 伴随着许多研究者深入研究, 混沌系统越来越多的被应用到加密图像中来。但是现在已

有的图像加密算法在实际使用中存在很大的安全隐患, 还有很大的改进空间。文献[1]提出了基于逻辑映射的图像加密算法, 实际操作起来较简单, 从结果来看具有良好的加密效果, 但是仅仅是一种映射加密, 安全性不足。文献[2]利用 Logistic 混沌映射对图像的像素位置置乱, 在像素置乱中再次利用 Logistic 混沌映射, 通过二次混沌映射达到良好的加密效果, 但这还是单一的混沌映射, 算法密钥空间小, 不能有效抵御暴力攻击。文献[3]中置乱与扩算方法采用的都是不同初始条件和不同的参数值生成的两个 Logistic 混沌映射。但仅仅依赖外部给定密钥, 容易被明文攻击, 通过检索对应步骤的密码流可以被破解。文献[4]利用效率较高的分块图像置乱算法,

项目来源: 国家自然科学基金项目(61471325); 山西省重点计划研发项目(201803D121061)

收稿日期: 2020-05-23 修改日期: 2020-07-30

提高了加密效率,但没有解决 Arnold 变换周期的问题,当扩散加密被破解后,置乱加密也会随之被攻破。

## 1 理论基础

### 1.1 约瑟夫遍历

约瑟夫环问题原本是一个数学问题:假设有  $n$  个人他们围着一张圆桌坐在一起,给他们编号从 1 到  $n$ 。任意取一个编号  $n_0$ ,从第  $n_0$  个人由 1 开始报数,数到  $a$  的那个人出局;由出局后的下一个人开始继续从 1 开始报数,数到  $a$  的人接着出局;遵循这一规则进行重复报数,一直持续到圆桌最后一个人也出局,求出最后出局的人的序号。运用递归算法可以解决这个问题,首先把  $m$  个人的序号重新编号由 1 到  $n-1$ ,根据式(1)计算,最后出局的人的编号为  $f(n)+1$ 。

$$\begin{cases} f(1) = 0 \\ f(n) = [f(n-1) + a] \end{cases} \quad (1)$$

将每个人的编号按照出局的顺序排列出来的序列,称为约瑟夫遍历。

约瑟夫遍历:通过对原来的序列  $A_n$  进行  $n$  次的  $f_{\text{replace}}(A_n, m_0, a)$  运算,将计算出的每个  $a_{\text{out}}$  根据出局的顺序排序,得到新的序列  $B_n$ ,即:

$$B_n = \{a_{\text{out}1}, a_{\text{out}2}, \dots, a_{\text{out}n}\} \quad (2)$$

例如当  $n=8, m_0=1, a=4$ ,约瑟夫遍历的轨迹图如图 1 所示。

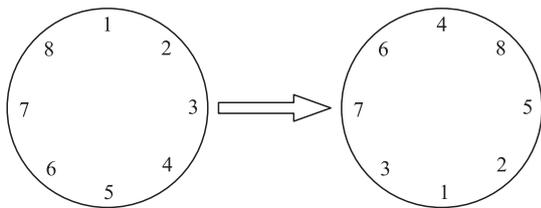


图 1  $n=8$  时的经典约瑟夫轨迹

根据上述可知约瑟夫环问题包含三个变量,起始位置  $m_0$ ,出局的间隔  $a$ ,参与总人数  $n$ 。该序列由于具有周期性,容易被人通过其周期性的特点而被破解,本文为了使得该变换产生的置乱空间更大,提出增加两个变量  $i$  和  $t$  作为参数, $i$  是约瑟夫遍历映射的报数间隔, $t$  表示报数的方向, $t \geq 0$  为顺时针方向, $t < 0$  为逆时针方向。即:

$$\begin{cases} i = 5, t = 0 \\ f_{\text{replace}}(a_n, m_0, a) = B_n \end{cases} \quad (3)$$

引入这两个参数可以增加密钥空间,改善了其周期性的特点而且将加密图像与密钥联系起来,从而提高了加密图像的安全性。

### 1.2 Logistic 映射

Logistic 混沌映射其实就是生态学中的虫口模

型,可以用如下公式表示:

$$x_{k+1} = \mu x_k (1 - x_k) \quad (4)$$

当  $3.569 < \mu \leq 4$  时,Logistic 混沌映射此时处于混沌状态。在该公式下生成的伪随机序列是非周期性、非收敛而且对初值十分敏感<sup>[13]</sup>。如图 2 所示。

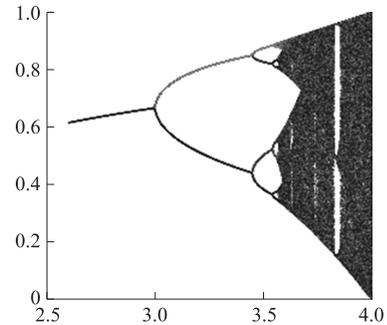


图 2 Logistic 混沌映射

Logistic 混沌映射属于一维混沌系统,作为图像加密中最常见的一种方法<sup>[6]</sup>,它的特点是系统参数较少,混沌区间小,函数形式简单,混沌复杂程度低,由上图可以看出 Logistic 混沌映射的参数范围较小,这是该混沌系统现有的缺点,通过对该混沌映射的公式改进可以有效扩大其参数范围,如文献[5]中改进 Logistic 混沌映射的方程式:

$$\begin{cases} x_{n+1} = L(\mu, x_n) \cdot G(k) - (\text{floor } L(\mu, x_n) \cdot G(k)) \\ L(\mu, x_n) = \mu x_n (1 - x_n) \\ G(k) = 2^k, k \in \mathbb{Z}^+, k \geq 8 \end{cases} \quad (5)$$

式中:floor 函数是向下取整函数,式(5)是式(4)的一种改进形式, $L(\mu, x_k)$  就是  $\mu x_k (1 - x_k)$ 。

经过改良 Logistic 混沌映射公式,混沌映射参数  $\mu$  的取值范围得到有效扩大,在  $0 < \mu \leq 4$  的范围之间该公式有良好的混沌状态,在  $[0, 1]$  的范围之间混沌序列呈现出均匀分布,但该混沌序列仅仅依靠  $\mu$  和  $x_0$  的初值,为了进一步增强混沌序列的伪随机性,将上述混沌映射设计成一个分段函数,将原始图像的部分元素值作为一个密钥参数引入到方程式中,经过改进后的分段 Logistic 映射公式可表示为:

$$\begin{cases} x_{n+1} = L(\mu, x_n) \cdot G(k) - (\text{floor } L(\mu, x_n) \cdot G(k)) \\ (\mu, x_n) = \mu x_n (1 - x_n) \\ G(k) = 2^k, k \in \mathbb{Z}^+, k \geq 8 \\ k = \begin{cases} j & i \leq m \\ j + d(i) & m \leq i \leq m + lp \\ j \in \mathbb{Z}^+, j \geq 8 \end{cases} \end{cases} \quad (6)$$

这里  $i$  是迭代次数, $m$  是因为 Logistic 映射会存在暂态效应故舍去混沌序列的前  $m$  项, $d(i)$  是加密

图像的元素值,  $lp$  是待加密图像的像素总数。与 Logistic 混沌映射相比, 分段 Logistic 映射的 Lyapunov 指数更高, 说明其混沌性更好, 表明加密后的混沌序列更具有随机性。

## 2 加密算法的设计

### 2.1 像素全局置乱

输入原始图像的  $256 \times 256$  的灰度图像 peppers, 令  $lp = 256 \times 256$ , 将灰度图像 peppers 按照列优先的顺序将图像转化成一维向量  $P_1$ ,  $P_1 = \{a_1, a_2, \dots, a_{lp}\}$  且初始参数取值范围分别为: 序列  $A_n$  长度  $\in [0, lp-1]$ , 取合理的初始参数  $m_0 = 1$ ,  $step = 11$ ,  $i = 5$ ,  $t = 0$ , 将向量  $P_1$  代入式(3)可得

$$P_2 = \{a_{out1}, a_{out2}, \dots, a_{outn}\} \quad (7)$$

通过上述对  $P_1$  进行置乱, 可以得到图像  $P$ 。

### 2.2 矩阵扩算和像素值替换

(1) 将图像  $P$  分解为两个 4 位的矩阵  $H$  和  $L$ , 矩阵  $H$  与  $L$  分别是高四位和低四位的位平面矩阵。

(2) 输入参数  $\mu_1, x_1$ , 利用式(6)和矩阵  $H$  迭代  $n+lp$  次得图像的部分元素值  $d(i)$ , 舍去前  $n$  个值得到密钥序列  $K$ 。

(3) 利用序列  $K$  对矩阵  $L$  进行位置扩散, 得到矩阵  $L_1$ , 置乱方法如下式:

$$P_{2i} = P_{1i}, i = 1, 2, 3, \dots, lp \quad (8)$$

序列  $K$  按照从大到小的顺序排列可以得到位置序列  $T: T = \{t_1, t_2, t_3, \dots, t_{lp}\}$ , 利用序列  $K$  对矩阵  $L$  进行位置扩散。

(4) 选取随机序列  $K$  小数点后第 9~11 位数字, 对 16 取模, 得到 0~15 的一个伪随机整数序列  $K_1$ , 用  $K_1$  与  $H$  作异或运算, 得到高四位位平面的加密

矩阵  $H_1$ 。

(5) 把  $H_1$  和  $L_1$  合成一个 8 位矩阵, 得到最终加密图像  $E$ 。加密算法流程图如图 3 所示。

### 2.3 解密算法

解密的过程就是加密的逆过程, 只要按照之前加密的方法输入正确的密钥参数, 进行相反的操作就可以解密出原始图像。

## 3 仿真结果

本文采用了大小为  $256 \times 256$  的 peppers 图像作为加密图像, 采用 Win7 系统的电脑, 内存为 4G, 通过 MATLAB2014b 进行仿真实验, 利用 MATLAB 做完仿真试验后得到如下的图像结果。图 4 为 peppers 的灰度原始图像, 图 5 为改进约瑟夫遍历置乱后的图像, 图 6 是加密后的最终图像, 图 7 是解密后正确图像。



图 4 原始图像

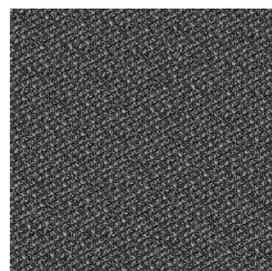


图 5 置乱图像

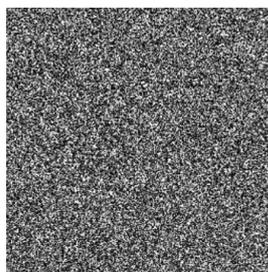


图 6 加密图像



图 7 解密图像

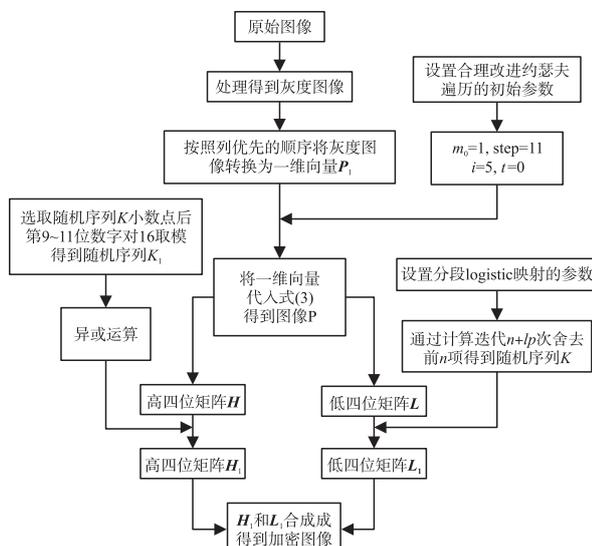


图 3 加密算法流程图

## 4 算法分析

### 4.1 密钥空间分析

一个好的加密算法必须拥有足够大的密钥空间<sup>[7]</sup>, 本文的算法密钥是由两个不同的混沌映射控制的, 密钥的组成有  $\mu_1, x_1, m_0, step, i$ , 假设计算机的储存精度是  $10^{-15}$ , 所以该改进算法的密钥空间为  $10^{75}$ , 另外还有约瑟夫报数的方向与它的间隔等, 因此该算法的加密空间估计为  $10^{100}$ , 因此可以更好地抵御穷举等暴力攻击。

### 4.2 密文统计特性

#### 4.2.1 直方图分析

直方图可以直观地反映图像不同灰度级像素出

现的频率<sup>[8]</sup>,原始图像的明文分布具有自己独特的特殊性,在不同的区域明文分布大不相同,像素分布不均容易被人破解,通过加密方法可以有效改善图像像素的分布,可以很好地对明文图像进行隐藏,达到了预期加密的效果。

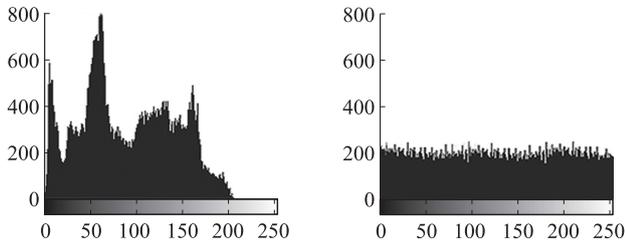


图 8 明文灰度直方图

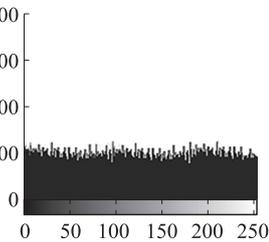


图 9 密文灰度直方图

#### 4.2.2 信息熵

信息熵是加密算法中一个常用的量化指标,也可以评价一个系统的复杂程度,加密图像像素分布越均匀,图像的信息熵越大,信息熵最大值为 8,由式(9)可以计算出加密图像的信息熵:

$$H_{(m)} = \sum_{i=1}^{2^N-1} p(m_i) \log_2 \frac{1}{p(m_i)} \quad (9)$$

式中: $m_i$  是图像灰度值,本文改进后的算法信息熵为 7.997 5,图像加密效果与其信息熵的值越接近 8,图像加密效果越好,说明每个像素值分布的概率非常相似,加密效果好,结果表明熵攻击并不能对加密图像造成破坏。

#### 4.2.3 相邻像素点的相关性

图像加密前后的相关性也是衡量加密效果的一个重要参数<sup>[9]</sup>,明文图像通常是较为清晰的画像,图像相邻像素点之间的相关性高,而密文图像破坏了原来图像的相邻像素的相关性,密文相关性越接近于 0,加密效果越好。利用仿真实验,以垂直,水平,对角线三个不同方向为例, $x, y$  是相邻两个像素值的灰度值,根据式(10)随机选取 1 000 对相邻像素计算其相关性:

$$\begin{cases} D_x = \frac{1}{n} \sum_{i=1}^n [x_i - E(x)]^2 \\ \text{cov}(x, y) = \frac{1}{n} \sum_{i=1}^n [x_i - E(x)][y_i - E(y)] \\ \gamma = \frac{\text{cov}(x, y)}{\sqrt{D(x)} \sqrt{D(y)}} \end{cases} \quad (10)$$

式中: $D_x$  是方差, $E(x), E(y)$  是相邻像素值的期望, $n$  是像素点的个数, $\text{cov}(x, y)$  是它的协方差; $\gamma$  是相关系数。

图像加密前后在三个不同方向像素点的分布情况可由图 10~图 12 表示,这是分别从三个不同角度

分析得出其相关性的分布。图 10~图 12 中左边代表了原始图像在 3 个不同方向像素点分布的密度,右边代表加密图像在 3 个不同方向的像素点分布的密度。从图中可以看出无论是水平方向,垂直方向还是在  $y=x$  方向,原始图像的点都集中在对角线的范围内,呈线性分布,显而易见明文图像的相邻像素点具有很强的相关性。而加密图像的像素点的分布是随机无序的分布在图中,所以加密图像的相邻像素点相关性很弱。

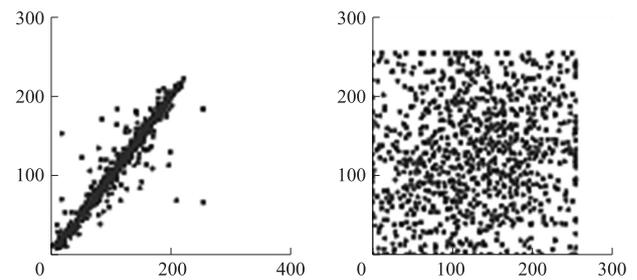


图 10 水平方向相关性

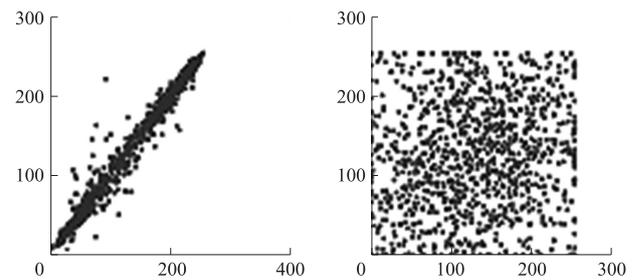


图 11 垂直方向相关性

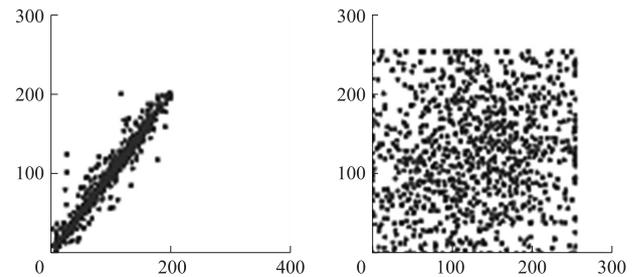


图 12 对角线方向相关性

从表 1 中可以看出,原始图像与加密图像的相关系数的值差别很大,相关系数的数值越接近 1,图像相邻像素的相关性越高,反之数值越小相关性越弱<sup>[12]</sup>,所以可以得出结论:加密图像的相邻像素点之间几乎没有相关性。跟其他算法比较,该算法相关系数小,具有良好的扩散性,加密性能更好。

表 1 相邻像素点的相关系数的比较

方向	原始图像	加密图像	文献 [10]	文献 [11]	文献 [12]
水平	0.976 5	0.009 7	0.002 9	0.021 6	0.013 6
垂直	0.963 7	0.006 5	0.115 0	0.006 5	0.006 2
对角	0.934 2	0.001 6	0.005 9	0.017 5	0.012 9

#### 4.2.4 差分攻击分析

差分攻击是通过对比加密前后图像特定的区域进行比较分析来攻击密码算法的。像素变化率 NPCR (the number of pixels change rate), 归一化平均变化强度 UACI (the unified average changing intensity), 其中 NPCR 表示的不同密文图像在相同位置上灰度值互不相同的比率, 而 UACI 则表示不同密文图像之间的平均变化密度, 通常用于图像加密抗差分性分析。如果单个像素点的变化可以导致加密图像产生明显的改变, 说明算法可以有效抵御差分攻击。所以 NPCR 和 UACI 是有效分析抗差分攻击的重要指标, 由公式(11)和(12)计算可得:

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{m \times n} \times 100\% \quad (11)$$

$$\text{UACI} = \frac{1}{m \times n} \sum_{i,j} \left| \frac{C_1(i,j) - C_2(i,j)}{255} \right| \times 100\% \quad (12)$$

式中:  $D(i,j) = \begin{cases} 1 & C_1(i,j) \neq C_2(i,j) \\ 0 & C_1(i,j) = C_2(i,j) \end{cases}$ ,  $m$  表示图像的行,  $n$  表示列。

为了研究加密算法能否抵御差分攻击, 可以通过改变原始图像中像素点来判断。随机选取 1 个像素点, 对选出的像素值加 1, 对改变像素值后的图像进行加密, 利用式(11)和式(12)计算。通过计算得出 NPCR 和 UACI 的平均值分别是 99.62% 和 31.59%。说明当原始图像中某个像素值被改变后, 会使加密后的图像 NPCR 变化接近 100%, 计算出 UACI 的值也在 31% 以上。通过上面的分析可以得出该加密算法可以有效抵御差分攻击。

## 5 对比分析

为了验证文章算法的创新性和其良好的加密效果, 通过算法多样性, 明文与密钥是否相关, 加密时间, 信息熵还有密钥空间进行分析, 使用大小为  $256 \times 256$  的 Lena 图像作为参考, 通过与文献[10-12]进行对比分析结果如表 2 所示。

表 2 不同算法对比分析结果

	算法多样性	明文密钥是否相关	加密时间 /s	密钥空间
文献[10]	1	无	0.077 34	$10^{45}$
文献[11]	1	无	0.072 96	$10^{75}$
文献[12]	2	有	2.062 74	$10^{135}$
文章算法	2	有	0.058 71	$10^{100}$

由表 2 可以看出文献[12]和本文都是利用不同的加密算法进行加密, 算法的多样性使得加密的

安全性能大大提升。而文献[10]和文献[11]只是单一映射, 容易被人破解。文献[12]和本文都引入明文参数, 使得轻微的改变明文像素会使得密钥大大改变, 从而提升了密钥破解难度, 而文献[10-11]的密钥与明文无关, 关联性不强, 抗差分攻击弱。

表中的加密时间是利用 MATLAB2014b 生成  $10^7$  个序列值的平均时间, 通常密钥空间  $\geq 2^{100}$  (相当于  $10^{30}$ )。由表 2 可知文章的密钥空间处于中上水平, 可以有效抵御穷举攻击。虽然文章密钥空间不如文献[12], 但是由于改进 Logistic 映射简单, 生成序列时间段, 因此本文加密时间会更短, 可以较好地满足实际需要。

## 6 结束语

文章针对网络信息和图像传输安全提出了改进约瑟夫遍历和分段 Logistic 映射的加密算法, 通过利用改进后约瑟夫遍历进行图像的置乱操作, 对于置乱后的图像进行分解, 分解为两个四位的高低矩阵, 对高四位矩阵进行分段 Logistic 映射置乱, 对低四位矩阵进行异或处理, 再将高四位矩阵与低四位矩阵进行结合, 最终得到加密图像。该算法利用约瑟夫遍历, 增加了该算法的加密空间, 引入报数间隔和报数方向改善其周期性的特点, 对分段 Logistic 映射引入加密图像的元素值  $d(i)$ , 使得秘钥不仅仅从外部获取。仿真实验结果表明, 该算法的秘钥空间大, 加密后的图像置乱度高, 将图像中的元素引入算法中, 使得抗攻击性强, 而约瑟夫遍历引入报数间隔和报数方向使得该置乱方法难以从周期性破解, 安全性更高, 因此改进后的算法加密效果更好。

### 参考文献:

- [1] 陶红. 基于 Logistic 混沌序列的图像加密设计[D]. 南京: 东南大学, 2018.
- [2] 胡春杰, 嵇海祥, 牛智星, 等. 基于改进 Arnold 映射二次置乱的图像加密算法[J]. 计算机与数字工程, 2019, 47(7): 1783-1787.
- [3] 牛莹, 张勋才. 基于变步长约瑟夫遍历和 DNA 动态编码的图像加密算法[J]. 电子与信息学报, 2020, 42(6): 1383-1391.
- [4] 殷秋实, 陈建华. 多服务器环境下基于椭圆曲线密码的改进的身份认证协议[J]. 计算机科学, 2018, 45(6): 111-116.
- [5] Wang X, Liu L, Zhang Y. A Novel Chaotic Block Image Encryption Algorithm Based on Dynamic Random Growth Technique [J]. Optics & Lasers in Engineering, 2015, 66: 10-18.
- [6] 郑义. 基于复合混沌序列的融合图像加密系统设计[J]. 电子设计工程, 2019, 27(13): 176-179, 184.
- [7] 柴宗谦. 基于约瑟夫环和细胞自动机的 QR 码加密法研究[D]. 长春: 东北师范大学, 2019.

- [8] Li B, Liao X, Jiang Y. A Novel Image Encryption Scheme Based on Logistic Map and Dynamotic Modular Curve[J]. *Multimedia Tools and Applications*, 2018, 77(7):8911-8938.
- [9] 刘西林, 严广乐. 基于混沌映射与有限域 GF(2~4) 域乘法运算的电子病历图像的加密[J]. *计算机应用与软件*, 2018, 35(12):303-307.
- [10] Slimane N B, Bouallegue K, Machhout M. Designing a Multi-Scroll Chaotic System by Operating Logistic Map with Fractal Process [J]. *Nonlinear Dynamics*, 2017, 88(3):1655-1675.
- [11] Zhang Sen, Zeng Yicheng, Li Zhijun, et al. A Novel 4D No-Equilibrium Hyper-Chaotic System with Grid Multi-Wing Hyper-Chaotic Hidden Attractors [J]. *Journal of Computational and Nonlinear Dynamics*, 2018, 13(9):090908.
- [12] Vidhya R, Brindha M, Ammasai Gounden N. A Secure Image Encryption Algorithm Based on a Parametric Switching Chaotic System [J]. *Chinese Journal of Physics*, 2019, 62:26-42.



赵晓龙(1995—),男,山西省运城市人,研究生,研究方向为嵌入式系统,图像加密;



李 博(1972—),男,山西省太原人,博士,副教授,研究方向为嵌入式系统,DSP 通信,ARM 通信;



贾 芑(1995—),男,山西省忻州人,研究生,研究方向为嵌入式系统,图像加密,451527802@qq.com;



杨耀森(1994—),男,山西太原人,助理工程师,研究方向为视频压缩加密。