

## 新的基于双混沌系统和压缩感知的图像加密算法

杨宇光, 曹国栋

(北京工业大学信息学部, 北京 100124)

**摘要:** 图像加密技术在当今多媒体应用和互联网信息安全传输中发挥着重要作用, 但存在一些问题。多数图像加密算法存在密文图像在传输过程中占用带宽较高、图像加密速度慢、图像加密算法没有与明文关联、没有完备密文反馈机制等问题, 这些问题影响着图像加密算法的安全性和易用性。为了解决上述问题, 对压缩感知技术和混沌系统进行了研究, 提出了一种新的基于双混沌系统和压缩感知的明文关联的图像加密算法。采用明文图像关联密钥, 将明文图像哈希值与 Logistic 混沌系统参数进行关联; 采用离散小波变换对明文图像进行稀疏处理; 通过 Logistic 混沌系统生成随机测量矩阵, 结合压缩感知技术和随机测量矩阵对图像进行一次加密, 得到中间图像; 对中间图像再次进行哈希, 与明文图像哈希值共同关联 Rucklidge 混沌系统初值; 使用 Rucklidge 混沌系统和加密算法控制中间图像进行二次加密, 得到密文图像。加密算法是一种新的明文关联加密算法, 该算法使用图像自身像素值控制中间图像置乱, 可以增强明文关联, 建立密文反馈机制。仿真结果和性能分析表明, 所提算法加密性能良好, 加密后图像可按照压缩比例进行压缩, 有效减小密文图像尺寸, 且可以很好地抵抗已知明文攻击、选择明文攻击、差分攻击等常见攻击, 优于其他常见图像加密算法。

**关键词:** 图像加密; 压缩感知; 双混沌系统; 明文关联; 离散小波变换

**中图分类号:** TP309

**文献标志码:** A

**DOI:** 10.11959/j.issn.2096-109x.2022058

## New image encryption algorithm based on double chaotic system and compressive sensing

YANG Yuguang, CAO Guodong

Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

**Abstract:** Image encryption technology plays an important role in today's multimedia applications and Internet information security transmission. However, most image encryption algorithms still have problems, for example, cipher images occupied high bandwidth during transmission, image encryption speed is slow, image encryption algorithms are not associated with plain image, and there is no complete ciphertext feedback mechanism. These prob-

收稿日期: 2022-01-20; 修回日期: 2022-05-12

通信作者: 杨宇光, yangyang7357@bjut.edu.cn

基金项目: 国家自然科学基金 (62071015)

**Foundation Item:** The National Natural Science Foundation of China (62071015)

**引用格式:** 杨宇光, 曹国栋. 新的基于双混沌系统和压缩感知的图像加密算法[J]. 网络与信息安全学报, 2022, 8(5): 88-97.

**Citation Format:** YANG Y G, CAO G D. New image encryption algorithm based on double chaotic system and compressive sensing[J]. Chinese Journal of Network and Information Security, 2022, 8(5): 88-97.

lems all affect the security and easy use of image encryption algorithms. In order to solve the above problems, the compressive sensing technology and chaotic system were studied, and a new image encryption algorithm based on double chaotic system and compressive sensing with plaintext association was proposed. The plaintext image association key was used to associate the plain image hash value with the Logistic chaotic system parameters. Discrete wavelet transform, was used to sparse the plain image. Then the random measurement matrix was generated by the Logistic chaos system, and the image was encrypted once by combining the compressive sensing technique and the random measurement matrix to obtain the intermediate image. The intermediate image was hashed again, and the Rucklidge chaos system initial value was associated with the plain image hash value together. The Rucklidge chaotic system and encryption algorithm were used to control the intermediate image for secondary encryption and accordingly obtain the cipher image. The encryption algorithm was a new plaintext correlation encryption algorithm, which used the image's own pixel value to control the scrambling of the intermediate image. It also enhanced the plaintext association and established a ciphertext feedback mechanism. Simulation results and performance analysis show that the algorithm has good encryption performance. The encrypted image can be compressed according to the compression ratio, effectively reducing the size of the cipher image. Moreover, it is resistant to common attacks such as known plaintext attack, selective plaintext attack and differential attack, which is better than other common image encryption algorithms.

**Keywords:** image encryption, compressive sensing, double chaotic system, plaintext association, discrete wavelet transform

## 0 引言

图像是互联网时代众多信息传输载体中的多媒体形式之一。然而, 由于互联网的开放性和带宽资源的稀缺性, 图像的安全性和传输效率问题备受关注。因此, 在传输过程中对图像进行加密和压缩就显得尤为重要。图像加密技术保护图像信息不被泄露和篡改<sup>[1]</sup>, 而图像压缩技术有效减少图像的冗余信息, 从而减小图像的存储空间, 提高其在网络中的传输效率。

压缩感知 (CS, compressive sensing) 是一种将高维稀疏信号通过随机采样生成低维信号的算法, 其采样频率远低于奈奎斯特频率<sup>[2]</sup>, 因此常被用来压缩信号。许多基于 CS 的加密算法被提出, 且安全性和鲁棒性都被验证良好<sup>[3]</sup>。例如, 文献[4]将改进的混沌映射和 CS 结合提出了一种快速加密算法。文献[5]结合 CS 和奇异值分解 (SVD, singular value decomposition), 提出了一种视觉有意义的图像加密算法。文献[6]结合超混沌系统提出一种有效的图像加密算法。文献[7]提出一种基于 CS 和三维离散余弦变换 (3D-DCT, three dimensional discrete cosine transform) 的三图像加密算法, 算法使用 2D 混沌系统生成测量矩阵,

分别对 3 幅图像进行 CS, 得到 3 幅密文图像, 最终使用 3D-DCT 将密文图像嵌入单张彩色载体图像中。

然而, CS 处理图像时, 本质上是一种线性测量和压缩<sup>[8]</sup>, 易遭受已知明文攻击<sup>[9]</sup>和选择明文攻击<sup>[10]</sup>。为了更好地抵抗各种攻击, 本文提出了一种新的明文关联初值生成算法, 进而提出了一种新的基于双混沌系统和 CS 的图像加密算法。仿真结果和性能分析表明所提算法可更好地抵抗已知明文攻击、选择明文攻击、差分攻击<sup>[11]</sup>等常见攻击, 图像重构质量较好。

## 1 相关理论

### (1) Logistic 混沌系统

Logistic 混沌系统是一维混沌系统<sup>[12]</sup>, 有着良好的混沌特性, 具有对初值敏感和计算速度快等优点, 定义如下:

$$x_{n+1} = \mu x_n (1 - x_n), x_n \in (0, 1) \quad (1)$$

其中,  $x_n$  为系统变量,  $\mu$  为系统参数, 当且仅当  $\mu \in [3.57, 4]$  时, 该系统具有混沌行为。本文使用 logistic 混沌系统生成 CS 的随机测量矩阵。

### (2) Rucklidge 混沌系统

Rucklidge 混沌系统是一种非线性动力系统<sup>[13]</sup>,

该系统对初值敏感, 有着优秀的混沌特性, 其表达式如下:

$$\begin{cases} \dot{x} = -ax + by - yz \\ \dot{y} = x \\ \dot{z} = -z + y^2 \end{cases} \quad (2)$$

其中,  $x$ 、 $y$ 、 $z$  是状态变量,  $a$ 、 $b$  是系统参数。当系统参数  $a=2$ ,  $b=6.7$  时, 该混沌系统的最大李雅普诺夫指数为 0.064 3, 系统处于混沌状态。本文使用 Rucklidge 混沌系统控制中间图像二次加密。

## 2 新的图像加密算法

### 2.1 明文关联分块置乱算法

为了更好地抵抗选择明文攻击和差分攻击, 本文提出一种新的明文关联分块置乱算法, 步骤如下。

**步骤 1** 给定  $M \times N$  的矩阵  $A$ , 将矩阵  $A$  由竖直方向划分为两块, 得到两个大小为  $M \times N/2$  的矩阵  $B$  和矩阵  $C$ , 令  $m=M$ ,  $n=N/2$ 。

**步骤 2** 给定矩阵  $B$  中任意一个像素坐标点  $(i, j)$ ,  $i \in [1, N/2]$ , 计算矩阵  $B$  中第  $i$  行的和 (除去  $B(i, j)$ ), 记为  $H_i$ 。计算矩阵  $B$  中第  $j$  列的和 (除去  $B(i, j)$ ), 记为  $L_j$ , 根据式(3)计算  $i'$  和  $j'$  的值。

$$\begin{cases} i' = (D(i, j) + H_i) \bmod m \\ j' = (E(i, j) + L_j) \bmod n \end{cases} \quad (3)$$

其中, 矩阵  $D$  和  $E$  为给定的随机矩阵。计算出新坐标后, 交换  $B(i, j)$  和  $C(i', j')$  的值。

**步骤 3** 按从左至右、从上至下的扫描方式遍历矩阵  $B$ , 依次循环执行步骤 2, 实现由矩阵  $B$  向矩阵  $C$  置乱。

**步骤 4** 将矩阵  $B$  和矩阵  $C$  位置对调, 由矩阵  $C$  向矩阵  $B$  进行置乱, 并给定两个新的随机矩阵  $F$ 、 $J$  替换  $D$  和  $E$ , 重复步骤 2 和步骤 3。

**步骤 5** 将大小为  $M \times N/2$  的矩阵  $B$  和矩阵  $C$  重组成大小为  $M \times N$  的新矩阵  $I$ 。

使用明文关联分块置乱算法是为了对中间图像进行置乱操作, 加强置乱环节的明文关联, 更好地抵抗选择明文攻击和已知明文攻击。

### 2.2 图像加密算法描述

#### 2.2.1 参数生成

在加密明文图像之前, 使用原始明文图像来计算 SHA-256 函数哈希值。经过计算得到 256 位哈希值, 该值以每 8 位一组划分用于计算密钥, 将其转换为 32 个十进制数  $K = \{k_1, k_2, \dots, k_{32}\}$ , 使用式(4)生成 Logistic 混沌系统初始值, 式中  $lx_t$  为指定值。

$$lx_0 = \bmod \left( lx_t + \frac{1}{256} (k_1 \oplus k_2 \oplus \dots \oplus k_{32}), 1 \right) \quad (4)$$

在本文算法进行 CS 操作后会生成一个中间图像  $P'$ , 同理, 计算  $P'$  的 SHA-256 哈希值生成  $KA = \{ka_1, ka_2, \dots, ka_{32}\}$ , 将  $K$  和  $KA$  使用式(5)得到  $KB$ 。

$$KB = \{k_1 \oplus ka_1, k_2 \oplus ka_2, \dots, k_{32} \oplus ka_{32}\} \quad (5)$$

使用  $KB$  计算以下初值:

$$\begin{cases} rx_0 = rx_t + \frac{1}{256} (kb_1 \oplus kb_2 \oplus \dots \oplus kb_8) \\ ry_0 = ry_t + \frac{1}{256} (kb_9 \oplus kb_{10} \oplus \dots \oplus kb_{16}) \\ rz_0 = rz_t + \frac{1}{256} (kb_{17} \oplus kb_{18} \oplus \dots \oplus kb_{32}) \end{cases} \quad (6)$$

其中,  $rx_t$ 、 $ry_t$ 、 $rz_t$  是指定值。通过密文反馈机制加强明文、密文与密钥流之间的联系。

#### 2.2.2 加密过程

图像加密流程如图 1 所示, 具体流程如下。

- 1) 设输入图像为  $P$ , 且大小设为  $m \times n$ 。
- 2) 计算图像  $P$  的 SHA-256 哈希值得到序列  $K$ , 并使用式(4)得到 Logistic 混沌系统初始值  $lx_0$ 。
- 3) 将图像  $P$  使用离散小波变换 (DWT, discrete wavelet transformation) 变换到稀疏域, 然后使其按绝对值升序排列, 得到序列  $PS$ 。实验验证, 稀疏矩阵 0 值占到整个矩阵的 90% 时的效果较好, 获取位置  $idx = \text{round}(0.9mn)$ , 得到阈值  $TS = PS(idx)$ , 使  $P(\text{abs}(P) < TS) = 0$ , 得到稀疏系数矩阵  $P1$ , 矩阵大小与原图像一致。
- 4) 对稀疏系数矩阵  $P1$  使用 Zigzag 置乱, 得到  $P2$ 。
- 5) 使用 Logistic 混沌系统和其初值  $lx_0$ 、步长  $d=10$  的初始参数, 生成  $100+MN$  长度的混沌序列

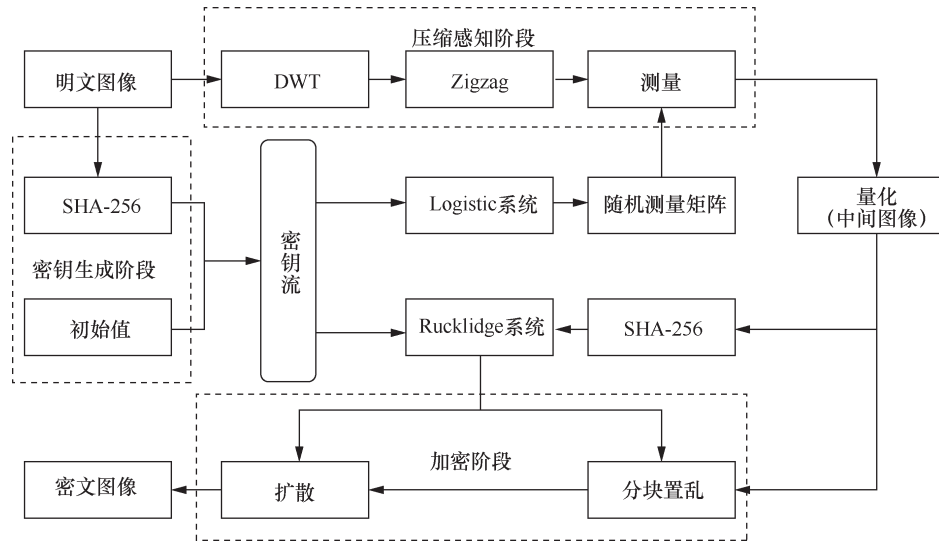


图1 图像加密流程  
Figure 1 Flow chart of image encryption

$S$ , 舍弃前 100 个值, 其次将大小范围为 $[0,1]$ 的序列  $S$  使用式(7)变换到 $[-1,1]$ , 最终按列优先方式将  $S$  重塑成大小为  $M$  行  $N$  列的随机测量矩阵  $\Phi$ , 其取值范围和  $S$  相同。其中  $N=n$ ,  $M=CR \cdot M$ ,  $CR$  为压缩比率。

$$S_i = 1 - S_i \times 2, i \in [1, M \times N] \quad (7)$$

6) 使用  $\Phi$  对  $P_2$  进行测量, 得到测量矩阵  $P_3$ , 其大小为  $M \times N$ 。

7) 使用式(8)将  $P_3$  量化到 $[0 \sim 255]$ 范围, 得到中间图像  $P_4$ , 式中  $\max$  和  $\min$  分别为  $P_3$  的最大值和最小值。

$$P_{4i} = \text{floor} \left( 255 \cdot \frac{P_{3i} - \min}{\max - \min} \right), i \in [1, M \times N] \quad (8)$$

8) 计算中间图像  $P_4$  的 SHA-256 哈希值得到序列  $KA$ 、 $K$  和  $KA$  使用式(5)得到  $KB$ , 使用  $KB$  和式(6)得到 Rucklidge 混沌系统初始值  $rx_0$ 、 $ry_0$ 、 $rz_0$ , 并生成长度为  $1000+MN$  的 4 条混沌序列  $h1$ 、 $h2$ 、 $h3$ 、 $h4$ , 为避免瞬态效应, 均舍弃前 1000 项值。

9) 将长度为  $MN$  的随机序列  $h1$  拆分为两个长度为  $MN/2$  的随机序列, 并将其按列优先方式重塑为两个  $M$  行  $N/2$  列的随机矩阵  $D$ 、 $E$ , 同理, 拆分  $h2$  为两个  $M$  行  $N/2$  列的随机矩阵  $F$ 、 $J$ , 使用 4 个随机矩阵和 2.1 节描述的置乱算法, 对  $P_4$  进行置乱操作, 得到  $P_5$ 。

10) 分别使用  $h3$ 、 $h4$  作为扩散算法的正向扩

散和逆向扩散混沌序列, 对  $P_5$  使用式(9)、式(11)的扩散算法对图像进一步置乱得到  $P_6$ , 即最终的秘密图像  $C$ 。

本文采用的扩散算法是与明文相关联的双向加取模运算, 该算法简单且可以很好地将像素值扩散到尽可能多的像素点。公式描述如下。

正向扩散如下:

$$C_i = (C_{i-1} + S_i + P_i) \bmod 256 \quad (9)$$

$$P_i = (2 \times 256 + C_i - C_{i-1} - S_i) \bmod 256 \quad (10)$$

逆向扩散如下:

$$C_i = (C_{i+1} + S_i + P_i) \bmod 256 \quad (11)$$

$$P_i = (2 \times 256 + C_i - C_{i+1} - S_i) \bmod 256 \quad (12)$$

其中,  $P$  为给定的待扩散明文图像,  $S$  为给定的控制扩散的混沌序列,  $C$  为扩散后的密文图像。式(9)、式(10)分别是正向扩散算法和与之对应的还原算法。式(11)、式(12)分别是逆向扩散算法和相应的还原算法。

### 2.2.3 解密过程

解密过程是加密过程的逆过程, 其流程如图 2 所示, 其过程简述如下。

1) 读取秘密图像  $C$ , 记为  $P_6$ , 设大小为  $M \times N$ 。

2) 使用 Rucklidge 混沌系统按照接收到的密钥生成长度为  $1000+M \times N$  的混沌序列  $h1$ 、 $h2$ 、 $h3$ 、 $h4$ , 丢弃前 1000 项。

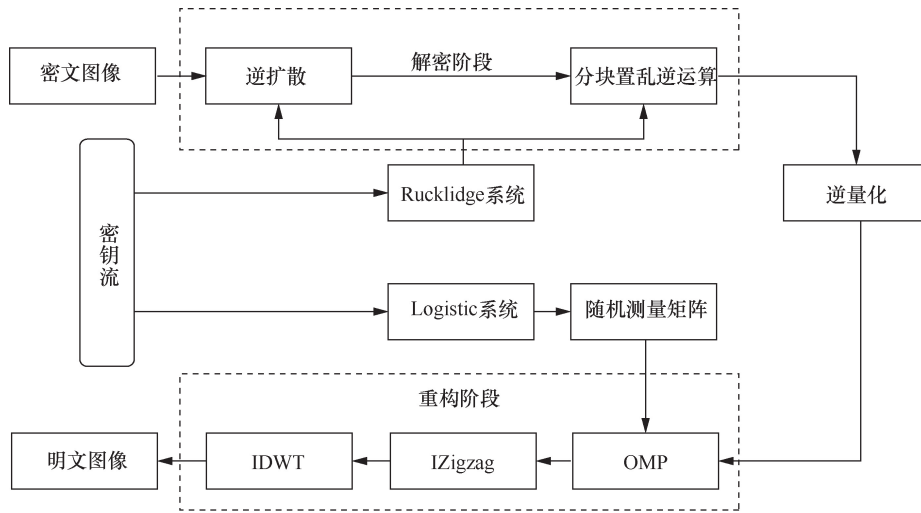


图2 图像解密算法流程

Figure 2 Flow chart of image decryption algorithm

3) 结合  $h_3$  和  $h_4$  对  $P_6$  使用式(10)、式(12)进行扩散的还原操作, 得到  $P_5$ 。

4) 使用  $h_1$  和  $h_2$  生成 4 个随机矩阵  $D$ 、 $E$ 、 $F$ 、 $J$ , 并使用置乱算法逆运算将  $P_5$  还原为  $P_4$ 。

5) 使用式(13)将图像  $P_4$  进行逆量化, 得到  $P_3$ 。

$$P3_i = \frac{P4_i \cdot (\max - \min)}{255} + \min, i \in [1, M \times N] \quad (13)$$

6) 使用 Logistic 混沌系统生成长度为  $100+M \times N$  的混沌序列, 按列优先将其变换为  $M$  行  $N$  列的随机测量矩阵  $\Phi$ , 使用  $\Phi$  和重构算法对  $P_3$  进行重构。常用的重构算法有正交匹配追踪 (OMP, orthogonal matching pursuit) 算法<sup>[14]</sup>、匹配追踪 (MP, matching pursuit) 算法<sup>[15]</sup>以及平滑  $l_0$  范数 (sl<sub>0</sub>, smoothed  $l_0$ ) 算法<sup>[16]</sup>等, 这里使用 OMP 重构算法, 得到  $P_2$ 。

7) 对  $P_2$  进行 Zigzag 逆变换得到  $P_1$ 。

8) 对  $P_1$  使用离散小波逆变换, 得到明文图像  $P$ 。

换选择离散小波变换, 重构算法使用 OMP。图 3 为仿真图像, 图 4~图 6 为仿真结果。



(a) Lena明文图像 (b) Cameraman明文图像 (c) House明文图像

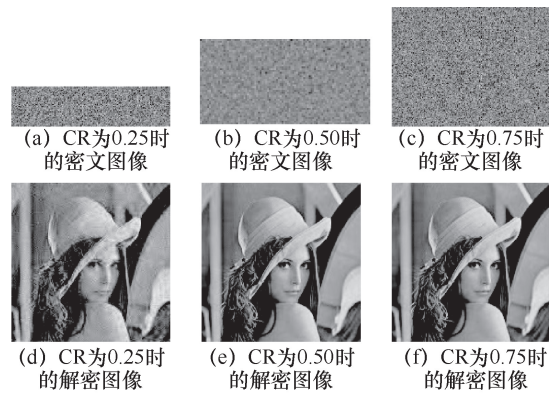
图3 明文测试图像  
Figure 3 Plain test image

图4 Lena 加解密结果

Figure 4 Lena encryption and decryption results

### 3 实验仿真及其安全性能分析

#### 3.1 仿真实验

本文选用常见的经典灰度图像进行仿真实验。实验采用的硬件配置为 Intel(R) Core (TM)i7-9750H CPU@2.60 Hz、16 GB RAM, 软件配置为 Windows10、MATLAB R2021a 的实验环境进行仿真。分别设置初始指定值  $\{lx_i, rx_i, ry_i, rz_i, CR, d, tstep, a, b\}$  为  $\{0.2, 1, 2, 3, 0.5, 10, 0.001, 2, 6.7\}$ , 稀疏变

仿真结果显示, 经过加密后的密文图像杂乱无章, 并且按照压缩比缩放, 所重构的图像与原图像基本一致, 表明本文算法能同时完成图像的压缩和加密, 图像的重构质量良好。

#### 3.2 直方图分析

直方图表示的是图像中每个灰度值出现

的频率,是像素值分布的规律。一个好的密文图像,其频率直方图应是水平的。图像及其直方图如图 7 所示。

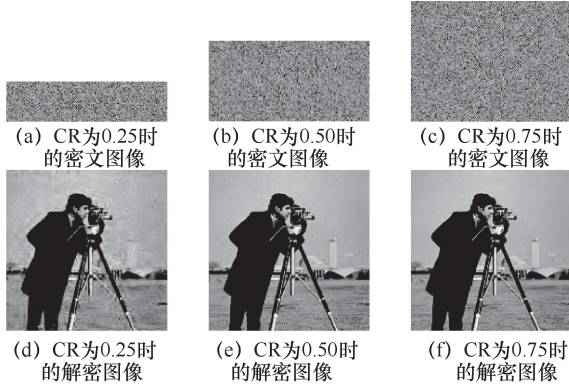


图 5 Cameraman 加解密结果  
Figure 5 Cameraman encryption and decryption results

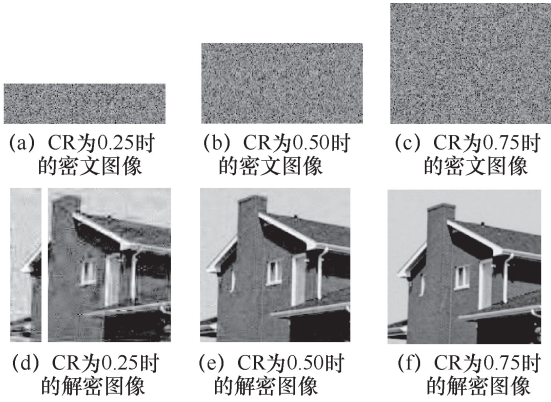


图 6 House 加解密结果  
Figure 6 House encryption and decryption results

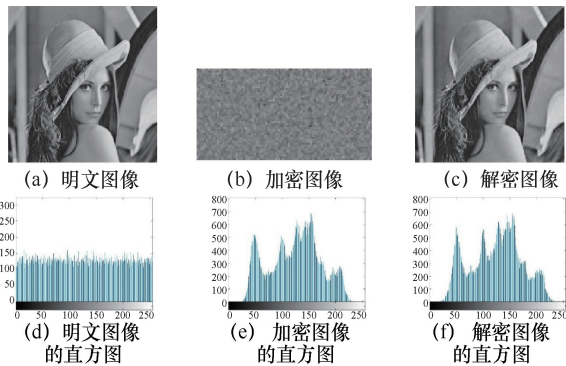


图 7 图像及其直方图  
Figure 7 Image and its histogram

图 7 表明密文图像的直方图是水平的,说明本文算法能很好地抵抗灰度统计攻击,且明文图像和重构图像的直方图分布基本一致,说明本算法很好地还原了明文图像。

### 3.3 相关性分析

一般明文图像在水平方向、垂直方向和对角线方向相邻像素点之间具有高度的相关性。因此图像加密算法应该能够完全打破各个方向的相邻像素间的相关性。计算相关性的公式如下:

$$\gamma_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}} \quad (14)$$

其中,  $x$  和  $y$  是像素值, 且  $\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y))$ ,  $D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2$ ,  $E(x) = \frac{1}{N} \sum_{i=1}^N x_i$ 。

对 Lena 图像的相关性分析如图 8 所示。明文图像的像素点集中地分布在一起, 而密文图像无论是从水平方向、竖直方向和对角线方向上看, 像素点都均匀地分布在图像的各个区域。表 1 分别给出了 10 幅图像的明文图像和密文图像的相关系数, 表 2 给出了表 1 数据的均值与其他文献的对比结果。

分析表 1 可得, 密文图像在 3 个方向上相关性都接近于 0, 且通过表 2 与其他方案的对比, 可看出本文算法略优于其他文献提出的算法。

### 3.4 密钥敏感性分析

密钥敏感性可以表征密钥空间的大小, 密钥敏感性越强, 密钥空间越大。本文算法的密钥为  $\{lx_0, rx_0, ry_0, rz_0, \max, \min, d, \text{tstep}, a, b, \text{CR}\}$ , 其中  $lx_0$ 、 $d$  分别为 Logistic 混沌系统的初始值和步长,  $rx_0$ 、 $ry_0$ 、 $rz_0$  为 Rucklidge 混沌系统的初始值,  $\text{tstep}$  是 Rucklidge 混沌系统的步长,  $a$ 、 $b$  是 Rucklidge 混沌系统的状态参数。 $\max$  和  $\min$  是中间图像量化时生成,  $\text{CR}$  是压缩比。假定计算机精度为  $10^{-15}$ , 忽略对密钥不敏感的值, 计算两个混沌系统相关参数。

图 9 给出了密钥敏感性测试结果, 分别分析了  $lx_0$ 、 $rx_0$ 、 $ry_0$ 、 $rz_0$  共 4 个混沌系统初始值密钥敏感性和 Rucklidge 混沌系统步长  $\text{tstep}$  的密钥敏感性。这里令每个密钥值增加  $10^{-15}$ , 然后解密密文图像。分析仿真测试, 本算法具有较好的密钥敏感性, 且密钥空间理论上达到  $2^{349} \gg 2^{100}$ 。

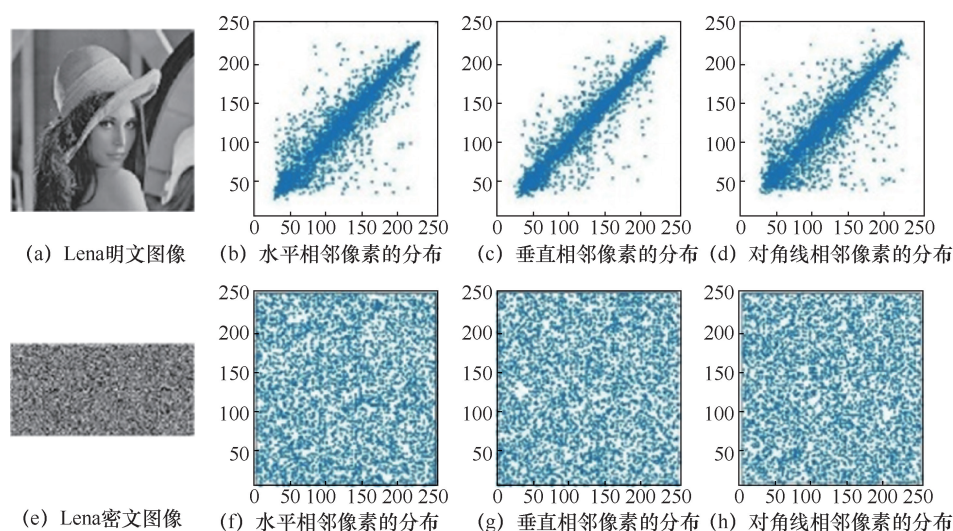


图 8 对 Lena 图像的相关分析

Figure 8 Correlation analysis of Lena images

表 1 明文图像和密文图像不同方向上相邻像素的相关系数

Table 1 Correlation coefficients of neighboring pixels in different directions for plain image and cipher image

| 图像         | 明文图像    |         |         | 密文图像      |          |           |
|------------|---------|---------|---------|-----------|----------|-----------|
|            | 水平方向    | 垂直方向    | 对角线方向   | 水平方向      | 垂直方向     | 对角线方向     |
| Lena       | 0.972 1 | 0.984 7 | 0.956 8 | 0.001     | -0.002 4 | 0.000 8   |
| Cameramen  | 0.982 4 | 0.989 6 | 0.972 2 | -0.000 2  | 0.005 2  | -0.000 8  |
| House      | 0.995 6 | 0.994 5 | 0.990 4 | -0.003 3  | 0.005 2  | -0.000 7  |
| Jetplane   | 0.972 7 | 0.970 3 | 0.948 7 | 0.007 4   | 0.001 1  | -0.004 5  |
| Lake       | 0.975 9 | 0.976 4 | 0.961 2 | -0.001 6  | 0.000 3  | -0.005 5  |
| Livingroom | 0.946 3 | 0.952 9 | 0.912 0 | 0.000 3   | 0.000 9  | -0.007 4  |
| Woman      | 0.996 4 | 0.996 9 | 0.994 5 | -0.001    | -0.002 4 | -0.001 1  |
| Peppers    | 0.980 4 | 0.980 3 | 0.970 6 | -0.001 4  | -0.003 4 | 0.007 7   |
| Pirate     | 0.977 5 | 0.981 3 | 0.967 0 | -0.008 5  | -0.001 5 | -0.003 5  |
| Walkbridge | 0.941 6 | 0.939 4 | 0.904 8 | 0.000 2   | -0.002 4 | 0.001 3   |
| 均值         | 0.972 4 | 0.974 5 | 0.955 5 | -0.000 71 | 0.000 06 | -0.001 37 |

表 2 不同算法相关系数均值比较

Table2 Comparison of mean values of correlation coefficients of different algorithms

| 算法     | 相关系数      |             |           |
|--------|-----------|-------------|-----------|
|        | 水平方向      | 垂直方向        | 对角线方向     |
| 文献[17] | 0.002     | -0.000 7    | -0.001 4  |
| 文献[18] | -0.001 7  | -0.013 2    | 0.008 4   |
| 文献[19] | 0.013 7   | 0.000 217 8 | 0.000 537 |
| 文献[20] | 0.002 6   | -0.003 8    | 0.006 2   |
| 本文     | -0.000 71 | 0.000 06    | -0.001 37 |

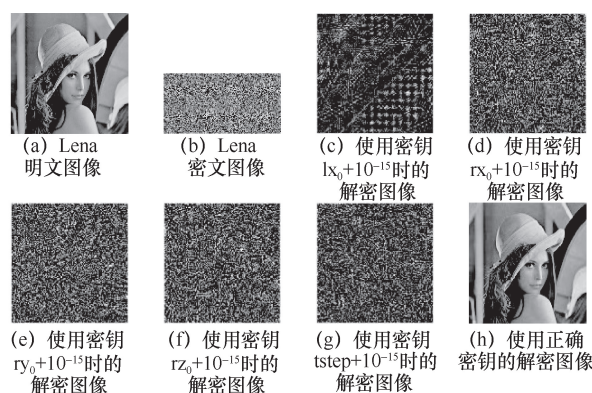


图 9 密钥敏感性测试

Figure 9 Key sensitivity test

### 3.5 信息熵分析

信息熵用来评估图像的随机性。图像的信息越随机, 信息熵越大。信息熵的计算公式如下:

$$H(m) = -\sum_{i=1}^n p(m_i) \log p(m_i) \quad (15)$$

其中,  $m$  是像素值集合,  $p(m_i)$  为像素值  $m_i$  出现的概率,  $n$  为集合  $m$  的大小。对于一个  $256 \times 256$  灰度图像而言, 信息熵的理想值是 8。表 3 分别给出了 5 幅明文图像和密文图像的信息熵值, 表 4 给出了 5 幅密文图像信息熵均值和其他文献对比结果。

表 3 明文图像与密文图像的信息熵  
Table 3 Information entropy of plain image and cipher image

| 图像        | 明文图像信息熵/bit | 密文图像信息熵/bit |
|-----------|-------------|-------------|
| Lena      | 7.445       | 7.998       |
| Cameramen | 7.048       | 7.998       |
| House     | 5.752       | 7.998       |
| Jetplane  | 6.713       | 7.998       |
| Lake      | 7.482       | 7.998       |

表 4 不同算法信息熵均值比较  
Table 4 Comparison of the mean value of information entropy of different algorithms

| 算法     | 信息熵/bit |
|--------|---------|
| 文献[17] | 7.997 2 |
| 文献[18] | 7.997 2 |
| 文献[19] | 7.999 3 |
| 文献[20] | 7.998 3 |
| 本文     | 7.998 7 |

从表 3 和表 4 可看出, 每幅密文图像的信息熵值都接近于理想值 8, 且本文的信息熵略微优于表 4 给出的对比文献, 表明本文算法生成的密文图像有着良好的随机性。

### 3.6 峰值信噪比分析

峰值信噪比 (PSNR, peak signal to noise ratio) 是描述图像失真或噪声水平的指标, 通常用来评估信号重构效果, 其定义如下:

$$\text{PSNR} = 10 \log \frac{255^2}{\frac{1}{N^2} \sum_{i=1}^N \sum_{j=1}^N [R(i, j) - I(i, j)]^2} \quad (16)$$

其中,  $R(i, j)$  和  $I(i, j)$  分别是重构图像和原始图像的像素点。表 5 给出了不同图像在不同压缩比下重构图像的 PSNR 值。

表 5 不同图像的 PSNR  
Table 5 PSNR of different images

单位: dB

| CR   | Lena    | Cameramen | House    | Jetplane | Lake     |
|------|---------|-----------|----------|----------|----------|
| 0.25 | 24.73   | 26.663 3  | 38.160 9 | 31.426 2 | 25.423 2 |
| 0.50 | 34.6481 | 31.839 1  | 38.002 4 | 34.711 1 | 32.21 8  |
| 0.75 | 34.6526 | 33.109 8  | 37.990 0 | 34.707 5 | 32.159 6 |

分析表 5 和上文仿真结果图像可知, 解密后的图像质量良好, 最高 PSNR 值为 38.160 9 dB, 即使压缩比为 CR=0.25, 重构图像的质量也可以接受。实验表明本文算法的重构效果良好。

### 3.7 抗差分攻击分析

攻击者常常会对明文图像轻微更改像素值, 然后分析密文图像变化情况。因此, 一个好的图像加密算法在明文发生微小的变化后, 密文应该有很大变化。像素变化率 (NPCR, the number of pixels change rate) 和统一平均变化强度 (UACI, the unified average changing intensity) 经常被用来评估像素是否能够抵抗差分攻击。NPCR 和 UACI 的计算公式分别如下:

$$\text{NPCR} = \frac{\sum_{i=1}^M \sum_{j=1}^N D(i, j)}{M \cdot N} \cdot 100\% \quad (17)$$

$$\text{UACI} = \frac{\sum_{i=1}^M \sum_{j=1}^N \frac{C_1(i, j) - C_2(i, j)}{255}}{M \cdot N} \cdot 100\% \quad (18)$$

其中,  $C_1$  是明文像素值改变前的密文,  $C_2$  是明文像素值改变后的密文, 当  $C_1(i, j) - C_2(i, j) = 0$  时,  $D(i, j) = 0$ , 否则  $D(i, j) = 1$ 。表 6 给出了这两个指标在不同图像下的仿真结果。表 7 给出了本文算法与其他文献的对比结果。

表 6 NPCR 与 UACI 值  
Table 6 NPCR and UACI values

| 图像        | NPCR   | UACI   |
|-----------|--------|--------|
| Lena      | 99.62% | 33.41% |
| Cameramen | 99.61% | 33.53% |
| House     | 99.59% | 33.45% |
| Jetplane  | 99.63% | 33.53% |

表 7 不同算法 NPCR 和 UACI 均值比较  
Table 7 Comparison of mean values of NPCR and UACI by different algorithms

| 算法     | NPCR   | UACI   |
|--------|--------|--------|
| 文献[17] | 99.65% | 33.48% |
| 文献[18] | 99.60% | 33.47% |
| 文献[19] | 99.61% | 33.46% |
| 文献[20] | 99.66% | 33.62% |
| 本文     | 99.61% | 33.48% |

在理想状态下, NPCR 和 UACI 的理想值为 99.609 4%和 33.463 5%。从表 6 和表 7 中可看出所例算法的仿真结果都能够满足要求, 表明本文算法对明文图像变化高度敏感, 有着良好的抗差分攻击特性。

### 3.8 时间复杂性分析

图像的加解密时间是衡量一个算法性能的重要指标。表 8 是本文算法在 CR=0.5 时使用不同明文图像计算的加解密时间。表 9 给出了本算法使用 Lena 图像的加解密时间和其他文献的对比结果。

表 8 不同图像的加解密时间, CR=0.5  
Table 8 Encryption and decryption time for different images, CR=0.5

| 图像                 | 加密时间/s    | 解密时间/s    |
|--------------------|-----------|-----------|
| Lena(256×256)      | 0.283 000 | 1.098 359 |
| Cameramen(256×256) | 0.267 795 | 1.083 355 |
| House(256×256)     | 0.760 084 | 2.599 003 |
| Jetplane(256×256)  | 0.732 589 | 2.803 953 |
| Lake(256×256)      | 0.717 937 | 2.842 957 |

表 9 本文算法与其他算法加密和解密时间的比较结果, CR=0.5  
Table 9 Comparison results of encryption and decryption time between the proposed algorithm and other algorithms, CR=0.5

| 算法     | 加密时间/s | 解密时间/s    |
|--------|--------|-----------|
| 文献[17] | 0.66   | 3.02      |
| 文献[18] | 2.042  | 2.046     |
| 文献[19] | 0.89   | 4.23      |
| 文献[20] | 2.25   | —         |
| 本文     | 0.283  | 1.098 359 |

从表 8 和表 9 可看出, 本文算法分别在图像大小为 256×256 和 512×512 时都有着良好的加解

密速度, 且本文算法的加解密时间均优于表中的对比文献, 具有较好的加解密性能。

## 4 结束语

本文提出了一种新的基于双混沌系统和 CS 的图像加密算法, 该算法使用明文图像和中间图像的哈希值构造密钥流, 提出一种新的与明文关联的分块置乱算法, 可更好地抵抗选择明文攻击和差分攻击。在对图像 CS 后, 又进行了二次加密, 弥补了 CS 线性测量的缺陷。仿真实验和性能分析表明本文算法有着较好的重构质量, 能够有效抵抗各种攻击, 并且具有良好的加密性能。与其他算法对比, 本文算法在加密性能和重构质量上有着更好的实用性和可靠性。

### 参考文献:

- [1] KAUR M, SINGH S, KAUR M, et al. A systematic review of metaheuristic-based image encryption techniques[J]. Archives of Computational Methods in Engineering, 2022, 29(5): 2563-257.
- [2] CANDÈS E J, TAO T. Near-optimal signal recovery from random projections: Universal encoding strategies[J]. IEEE Transactions on Information Theory, 2006, 52(12): 5406-5425.
- [3] ORSDEMİR A, ALTUN H O, SHARMA G, et al. On the security and robustness of encryption via compressed sensing[C]//MILCOM 2008 IEEE Military Communications Conference. 2008: 1-7.
- [4] XU Q, SUN K, CAO C, et al. A fast image encryption algorithm based on compressive sensing and hyperchaotic map[J]. Optics and Lasers in Engineering, 2019, 12(10): 203-214.
- [5] YE G, PAN C, DONG Y, et al. Image encryption and hiding algorithm based on compressive sensing and random numbers insertion[J]. Signal Processing, 2020, 172: 107563.
- [6] XU Q, SUN K, HE S, et al. An effective image encryption algorithm based on compressive sensing and 2D-SLIM[J]. Optics and Lasers in Engineering, 2020, 134: 106178.
- [7] WANG X, LIU C, JIANG D. A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT[J]. Information Sciences, 2021, 574: 505-527.
- [8] LI L, FANG Y, LIU L, et al. Overview of compressed sensing: sensing model, reconstruction algorithm, and its applications[J]. Applied Sciences, 2020, 10(17): 5909.
- [9] AHMID M, KAZAR O. A comprehensive review of the internet of things security[J]. Journal of Applied Security Research, 2021, 5(4): 1-17.
- [10] LIU Y, ZHANG L Y, WANG J, et al. Chosen-plaintext attack of an image encryption scheme based on modified permutation-diffusion structure[J]. Nonlinear Dynamics, 2016, 84(4): 2241-2250.
- [11] CIVINO R, BLONDEAU C, SALA M. Differential attacks: using alternative operations[J]. Designs, Codes and Cryptography, 2019, 87(2): 225-247.

- [12] KSHEERASAGAR T K, ANURADHA S, AVADHOOTHA G, et al. Performance analysis of DS-CDMA using different chaotic sequences[C]//2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). 2016: 2421-2425.
- [13] GONG L H, LUO H X, WU R Q, et al. New 4D chaotic system with hidden attractors and self-excited attractors and its application in image encryption based on RNG[J]. Physica A: Statistical Mechanics and its Applications, 2022, 591: 126793.
- [14] LIU E, TEMLYAKOV V N. The orthogonal super greedy algorithm and applications in compressed sensing[J]. IEEE Transactions on Information Theory, 2011, 58(4): 2040-2047.
- [15] MALLAT S G, ZHANG Z. Matching pursuits with time-frequency dictionaries[J]. IEEE Transactions on Signal Processing, 1993, 41(12): 3397-3415.
- [16] MOHIMANI H, BABAIE-ZADEH M, JUTTEN C. A fast approach for overcomplete sparse decomposition based on smoothed  $l_0$  norm[J]. IEEE Transactions on Signal Processing, 2008, 57(1): 289-301.
- [17] WANG X Y, ZHANG Y Q, BAO X M. A novel chaotic image encryption scheme using DNA sequence operations[J]. Optics and Lasers in Engineering, 2015, 73: 53-61.
- [18] WANG X, CHEN S, ZHANG Y. A chaotic image encryption algorithm based on random dynamic mixing[J]. Optics & Laser Technology, 2021, 138: 106837.
- [19] CHAI X L, GAN Z H, YUAN K, et al. An image encryption scheme based on three-dimensional Brownian motion and chaotic system[J]. Chinese Physics B, 2017, 26(2): 020504.
- [20] AHMAD J, HWANG S O. A secure image encryption scheme based on chaotic maps and affine transformation[J]. Multimedia Tools and Applications, 2016, 75(21): 13951-13976.

#### [作者简介]



杨宇光（1976—），女，河北衡水人，北京工业大学教授、博士生导师，主要研究方向为信息安全。



曹国栋（1997—），男，山东菏泽人，北京工业大学硕士生，主要研究方向为信息安全。