基于改进 Logistic 混沌和交叉混沌扩散的强鲁棒性图像加密

郭 媛, 贾德宝, 王 充, 翟 平

齐齐哈尔大学 计算机与工程学院 齐齐哈尔 中国 161006

摘要 针对现有部分图像加密算法鲁棒性弱的问题, 本文提出了一种基于改进 Logistic 混沌和交叉混沌序列扩散的强鲁棒性加密算法。首先, 对 Logistic 一维混沌进行变换, 构造出一种混沌序列分布更加随机的新混沌系统; 然后, 利用螺旋矩阵变换进行第一次置乱, 利用明文的哈希值构造混沌的初始密钥, 引入明文相关的两个数值 val_1 和 val_2 结合新混沌系统构造交叉混沌序列; 接着对置乱后的序列进行交叉混沌的扩散。为克服螺旋矩阵变换部分像素未发生改变的问题, 再进行一次交叉混沌置乱, 形成置乱-扩散-置乱的加密框架。最后对本算法进行仿真模拟, 其中本文密文图像的平均相关系数为–0.0027, 更加趋近于 0, 大大的破坏了图像内部之间的相关性, 达到图像加密的效果。像素变化率 NPCR 为 99.61%, 归一化强度 UACI 为 33.36%, 都分别接近于理想值 99.60%和 33.34%; 密文图像的信息熵为 7.9975, 接近于理想值 8, 密钥的敏感性为 10^{-17}; 能够在椒盐噪声和高斯噪声强度为 0.2 的情况下, 仍然能够识别出解密图像。而且加密图像剪切 1/2 时, 仍然能够恢复出明文图像; 实验结果表明, 本文算法具有较高的安全性, 能够抵御选择明文攻击和穷举攻击, 具有较强的抗噪声和抗剪切能力, 对于图像传输过程中的安全性提供一定的保障, 能够对于灰度图像达到安全稳定的加解密效果。

关键词 图像加密; 鲁棒性; 混沌系统; 交叉混沌扩散; 螺旋矩阵置乱

中图法分类号 TP309.7 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2024.09.13

Robust Image Encryption Based on Improved Logistic Chaos and Cross-Chaos Diffusion

GUO Yuan, JIA Debao, WANG Chong, ZHAI Ping

College of Computer and Engineering, Qiqihar University, Qiqihar 161006, China

Abstract Aiming at the weak robustness of some existing image encryption algorithms, a robust encryption algorithm based on improved Logistic chaos and cross chaotic sequence diffusion is proposed in this paper. Firstly, the Logistic one-dimensional chaos is transformed to construct a new chaotic system with more random distribution of chaotic sequences. Then, the spiral matrix transformation is used for the first scrambling, the plaintext hash value is used to construct the initial key of chaos, and the two plaintext related values val_1 and val_2 are introduced to combine the new chaotic system to construct the crossed chaotic sequence. Then the chaotic sequence is diffused by cross chaos. In order to overcome the problem that some pixels of the helical matrix transformation did not change, the cross chaotic scrambling was carried out again to form a scrambling - diffusion - scrambling encryption framework. Finally, the algorithm is simulated, in which the average correlation coefficient of ciphertext image in this paper is –0.0027, approaching to 0, which greatly destroys the correlation between internal images and achieves the effect of image encryption. The pixel change rate (NPCR) and normalized intensity (UACI) were 99.61% and 33.36%, respectively, close to the ideal values of 99.60% and 33.34%. The entropy of ciphertext image is 7.9975, which is close to the ideal value 8, and the sensitivity of key is 10^{-17}. It can recognize the decrypted image when the intensity of salt and pepper noise and Gaussian noise is 0.2. In addition, the plaintext image can still be recovered when the encrypted image is cut by half. Experimental results show that the proposed algorithm has high security, can resist the selection of plaintext attack and brute force attack, has strong anti-noise and anti-shearing ability, for image transmission security to provide a certain guarantee, can achieve a safe and stable encryption and decryption effect for gray image.

Key words image encryption; robustness; chaotic system; cross chaotic diffusion; spiral matrix scrambling

通讯作者: 贾德宝, Email: 981788677@qq.com。

本课题得到国家自然科学基金(No. 61872204)、黑龙江省自然科学基金(No. LH2021F056)、黑龙江省省属高等学校基本科研业务费科研项目(No. 135509113)、研究生创新科研项目(No. YJSCX2022049)资助。

收稿日期: 2022-11-17; 修改日期: 2023-02-11; 定稿日期: 2024-06-17

1 引言

随着云计算和大数据的发展, 数字图像作为主流的媒体传输在日常生活中十分广泛, 图像的安全是一个重要的领域, 图像加密在医疗、科技等方面有显著的作用。香农首先提出基于置乱-扩散的加密框架[1], 文献[2-3]论述了一个安全的加密方案必须同时包含置乱和扩散机制。2020 年, 黄欣[4]基于约瑟夫置乱和混沌系统提出了基于置乱扩散机制的混沌图像加密算法研究, 与传统算法相比具有一定的安全性, 能够抵御选择明文攻击。2021 年, 何鹏程[5]提出了一种置乱-混淆-扩散的体系加密方法, 利用延迟的 SIMM 系统进行加密, 证明了加密算法的有效性。Zhu[6]在 2020 年提出了一种压缩-混淆-扩散的图像压缩加密框架, 论述了算法的可行性与安全性。Liu 等人[7]提出了一种同时置换-扩散运算的快速混沌图像加密方案, 加密时间快, 具有良好的加密性能, 满足安全性要求。

传统加密算法以零损失方式进行恢复明文数据, 当其密文图像在噪声信道中传输时, 则无法解密恢复原始图像。鲁棒性图像加密主要是指明文图像采取某种加密算法, 对于密文图像经过噪声, 剪切等损坏后, 使其解密图像与明文图像之间的误差尽可能小。于是, 一些鲁棒性的图像加密算法广泛被提出来[8-14]。为了保障数据的可靠传输, Singh 等人[15]提供了一个新颖的医学图像鲁棒安全框架, 证明了所提出框架的有效性和可行性。Muhammad 等人[16]结合混沌系统和密码基元的类随机特征设计了一种鲁棒性的加密算法, 该算法可以用于图像安全领域。Rawat 等人[17]利用压缩感知结合多光谱进行双图像的鲁棒加密, 利用常规的 DRPE 系统提供了额外的安全层保证了图像在噪声信道传播中的安全性。为了获得更高的鲁棒性, Mohamed 等人[18]利用超高维的混沌映射结合 DNA 编码, 图像的哈希值提出了一种彩色图像加密方法, 具有良好的加密效果和安全性, 但是高维混沌系统复杂性较高, 需要硬件的支撑。

为保证图像在噪声信道中安全传输, 本文主要做了三方面的工作。第一, 对现有的一维混沌系统 Logistic 进行改进, 改造后的混沌序列分布更加随机, 直方图和混沌分叉图更优于之前的混沌, 更适合于图像加密。第二, 为增强系统的健壮性, 提出了一种置乱-扩散-置乱的加密框架, 通过实验分析验证了该框架在加密中的可行性。第三, 本文提出了一种新的混沌序列交叉扩散机制, 通过对混沌产生的序列进行明文上的改造, 增强了明文的敏感性, 能够抵御选择明文攻击, 具有较强的鲁棒性。

2 基本理论

2.1 改进 Logistic 混沌映射

Logistic 混沌是最简单的一维混沌映射, 此系统具有极其复杂的动力学行为, 在图像加密领域应用比较广泛[19], 其定义为公式(1)。

$$Z_{n+1} = \alpha \times Z_n \times (1 - Z_n) \tag{1}$$

其中, $\alpha \in (3.5699, 4)$ 是控制参数, $Z_n \in (0,1)$ 为初始条件, Z_n 在 Logistic 映射作用下产生非周期、不收敛的序列, 而在范围之外, 生成的序列就会收敛于某一个特定的值。

图 1 中 a, b 是 Logistic 映射的分叉图和直方图, 从图中可见, Logistic 混沌直方图存在着初始值和末值非常敏感, 分叉图进入混沌区间窄, 混沌序列分布没有充斥整个混沌区间。为了克服上述问题, 本文对 Logistic 混沌进行改进, 改进后的混沌映射如公式(2)。

$$Z_{n+1} = \alpha \times \left(1 - \frac{\pi}{\sin Z_n^2}\right) \bmod 1 \tag{2}$$

其中, $Z_n \in (0,1)$, mod 为取模符号。如图 1, c, d 所示, 对 Logistic 映射加入取模函数, 可以使其在遍历性、初值敏感性、伪随机性比未作处理前的序列更加优越。改进后的混沌区间得到了大大的增加, 在整个正区间都是混沌的且直方图分布更加均匀, 更适用于图像加密。

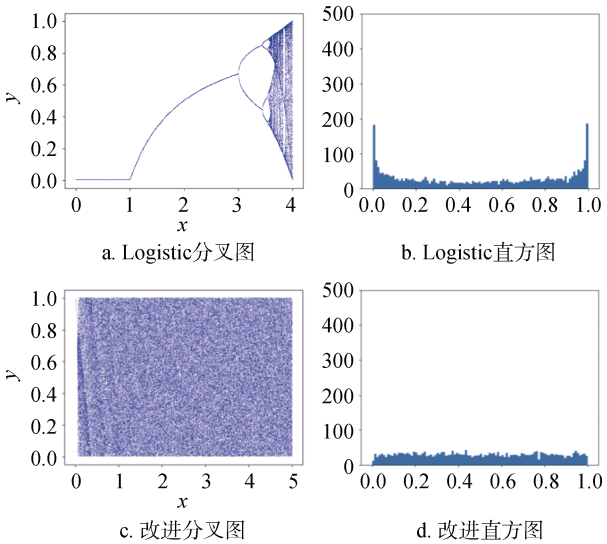

图 1 混沌分叉图和直方图

Figure 1 Chaotic bifurcation diagram and histogram

2.2 Kent 映射

Kent 映射[20]是一种常用的分段混沌映射, 从数

学上讲, Kent 映射与 Logistic 映射是同构的, 但 Kent 映射具有比 Logistic 映射更好的均匀遍历性, 提高算法的全局搜索性能, 其迭代过程同样适合程序化运行, 表达式为(3)。

$$s(m+1)=\begin{cases}\dfrac{s(m)}{\beta}, & 0<s(m)\leqslant\beta\\ \dfrac{1-s(m)}{1-\beta}, & \beta<s(m)<1\end{cases} \tag{3}$$

其中, $\beta\in(0,1)$ 是控制参数, 当 $s(m)\in(0,1)$ 时, 式(3)具有一个正的 Lyapunov 指数, 由此初始条件 s_0 在 Kent 映射中产生的序列具有很好的自相关性、互相关性和平衡性等伪随机性能, 同时 Kent 映射对初始条件极为敏感, 即使初始条件发生极其微小的变化, 其产生的随机序列也将完全不同, 为使得序列分布更加均匀, 本文设定 β=0.5。

2.3 螺旋矩阵变换

螺旋矩阵变换就是把某一矩阵按照“螺旋”方式进行重新排列, 使原有矩阵元素的位置发生了改变, 从而达到置乱的效果, 如图 2 所示为例, 原有矩阵经过中间的螺旋变换操作(以 10 为起点按照图中箭头指示方向进行遍历)得到了一个全新的矩阵[21]。从图中可以看到变换后的矩阵和原矩阵仍然存在着部分像素位置相同的问题, 为了使像素的位置分布更加随机, 本文又进行了一次交叉混沌置乱, 增强了算法的安全性。

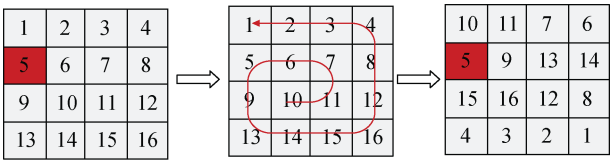

图 2 螺旋变换原理图

Figure 2 Schematic diagram of spiral transformation

2.4 交叉混沌置乱

首先将 $N\times N$ 的图像进行拉伸排列, 得到下标为 $[0: N\times N-1]$的一维数组 M, 数组下标是唯一确定图像像素值标志; 然后, 使用混沌系统得到混沌序列 K, 并对混沌系列进行相应的处理, 得到序列 K_1, 此时 K_1 的长度等于图像数组的长度, 序列 K_1 作为置乱操作的数组下标, 通过顺序序列 i 找到序列 K_1 的值, 该值对应的图像像素与 i 对应的图像像素进行交换; 如图 3 所示, 当 i 取 0 时, $K_1[0]$=5, 通过交叉规则, 将图像 M 中的第 0 个像素和第 5 个像素进行交换。使用 $K_1[i]$ $(0<i<N\times N-1)$可以得到序列的第 i 个值, 并将 $K_1[i]$ 作为图像交换时像素的下标; 最后, 通过 M[i] 与 M[$K_1[i]$] 行像素的互换完成打乱。图像的置乱程度取决于生成的混沌序列混乱程度, 混乱程度越高, 像素置乱越明显。为此, 本文使用两个不同混沌序列进行两次置乱, 完全解决了螺旋变换变换后的矩阵和原矩阵仍然存在着部分像素位置相同的问题。

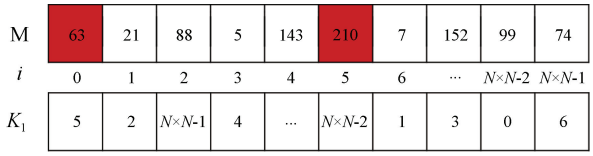

图 3 交叉置乱原理图

Figure 3 Schematic of cross scrambling

3 加解密原理

3.1 加密步骤

Lena 图像的 SHA256 对应的哈希值为 28a7ca4c5210cd84d903c08bf19ed43a62a49846eb1e52b90b4e4997c7d53351, 每 16 位为一组, 划分为 r_1～r_{64} 来构造参数密钥。上述混沌系统所需的密钥参数如公式(4)和(5), mod 符号为求余操作, *int* 为取整运算。

$$\begin{cases}z_0=\mathrm{mod}(\dfrac{r_1r_2\cdots r_{16}}{10^{15}},\ 1)\\ \alpha=\mathrm{mod}(\dfrac{r_{17}r_{18}\cdots r_{32}}{10^{15}},\ 4)\end{cases} \tag{4}$$

$$\begin{cases}\beta=\mathrm{mod}\left(\dfrac{r_{33}r_{34}\cdots r_{48}}{10^{15}},\ 1\right)\\ s_0=\mathrm{mod}\left(\dfrac{r_{49}r_{50}\cdots r_{64}}{10^{15}},\ 1\right)\end{cases} \tag{5}$$

为增强明文的相关性, 引进了与明文相关的常量 val_1 和 val_2, 定义如公式(6)和(7)。构造明文相关的交叉混沌序列引入扩散过程, 增强算法的鲁棒性。其中 sum 为求和运算, P 为明文图像, *row* 和 *col* 分别是明文图像的行数和列数, aver 为求平均值。

$$\mathrm{val}_1=\mathrm{int}\left\{\mathrm{mod}\left(\frac{\mathrm{sum}(p)}{row\times col},\ 256\right)\right\} \tag{6}$$

$$\mathrm{val}_2=\mathrm{int}\left\{\mathrm{mod}\left(\mathrm{aver}\left(\pi*row*\sqrt{p}\right),256\right)\right\} \tag{7}$$

利用改进的 Logistic 混沌系统和 Kent 混沌系统迭代生成长度为 1000 的混沌序列, 并将前 1000 个序列丢弃。接下来改进 Logistic 混沌产生两个长度为 $row\times col$ 的序列 $W_1=\{w_1w_2\cdots w_{row\times col}\}$ 和 $W_2=\{w_{row\times col+1}w_{row\times col+2}\cdots w_{2\times row\times col}\}$, Kent 混沌迭代产生两个长度的混沌序列 $F_1=\{f_1f_2\cdots f_{row\times col}\}$ 和 $F_2=\{f_{row\times col+1}f_{row\times col+2}\cdots f_{2\times row\times col}\}$。

对 W_1, W_2 和 F_1, F_2 按照公式(8)进行重新排列。

$$\begin{cases} H_1 = W_1[1] + F_1\begin{pmatrix} i \leqslant row*col-1, j \leqslant row*col \\ i\text{取奇数}, j\text{取偶数} \end{pmatrix} \\ H_2 = W_1[i] + F_2[j]\begin{pmatrix} i \leqslant row*col, j \leqslant row*col-1 \\ i\text{取偶数}, j\text{取奇数} \end{pmatrix} \\ H_3 = W_2[i] + F_1[j]\begin{pmatrix} i \leqslant row*col-1, j \leqslant row*col \\ i\text{取奇数}, j\text{取偶数} \end{pmatrix} \\ H_4 = W_2[i] + F_2[j]\begin{pmatrix} i \leqslant row*col, j \leqslant row*col-1 \\ i\text{取偶数}, j\text{取奇数} \end{pmatrix} \end{cases} \tag{8}$$

接着对 H_1 和 H_2 进行式(9)的操作。其中，mod 为取余运算，floor 为向下取整。

$$\begin{cases} E_1 = \mathrm{mod}\left(\mathrm{floor}\left(row \times col \times H_1\right), 256\right) \\ E_2 = \mathrm{mod}\left(\mathrm{floor}\left(row \times col \times H_2\right), 256\right) \\ E_3 = \mathrm{mod}\left(\mathrm{floor}\left(row \times col \times H_3\right), 256\right) \\ E_4 = \mathrm{mod}\left(\mathrm{floor}\left(row \times col \times H_4\right), 256\right) \end{cases} \tag{9}$$

对序列 E_1，E_2，E_3，E_4 按照公式(10)进行操作，得到序列 K_1，K_2，K_3，K_4，其中，$\mathrm{astype}(\mathrm{int})$ 为取整。其中 K_1，K_2 用于扩散过程中，K_3，K_4 同于第二次混沌置乱过程中。

$$\begin{cases} K_1 = \mathrm{mod}\left(\mathrm{val}_1 \times \left(\frac{E_1 + P_l}{2}\right), 256\right).\mathrm{astype}(\mathrm{int}) \\ K_2 = \mathrm{mod}\left(\mathrm{val}_2 \times \left(\frac{E_2 + P_l}{2}\right), 256\right).\mathrm{astype}(\mathrm{int}) \\ K_3 = \mathrm{mod}\left(\mathrm{val}_1 \times \left(\frac{E_3 + P_l}{2}\right), 256\right).\mathrm{astype}(\mathrm{int}) \\ K_4 = \mathrm{mod}\left(\mathrm{val}_2 \times \left(\frac{E_4 + P_l}{2}\right), 256\right).\mathrm{astype}(\mathrm{int}) \end{cases} \tag{10}$$

该算法采用置乱-扩散-置乱框架进行加密，首先，对明文图像进行螺旋变换，得到置乱后的矩阵，再通过引入明文相关的交叉混沌序列进行异或扩散。最后，为了克服螺旋矩阵变换时个别像素位置未发生改变的问题，引入了第二次的交叉混沌置乱，得到最终的加密图像。加密流程如图 4 所示。

对于明文图像首先按照 Algorithm 1 进行螺旋变换，得到置乱后的序列 P_1。

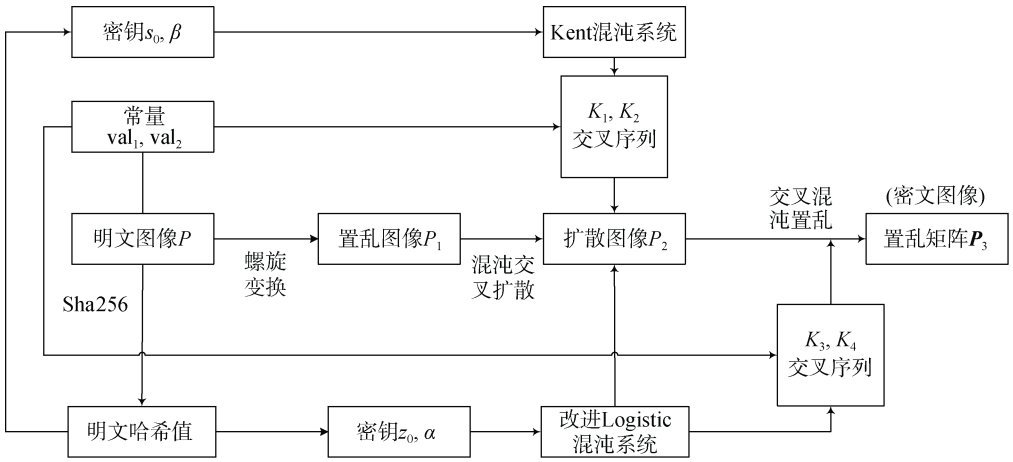

图 4　加密流程图

Figure 4　Encryption flow chart

```
Algorithm1: Helical matrix transformation
Input: P (plaintext)
Output: P1(after helical matrix transformation)
m = len(P)
n = len(P[0])
b = []
i, k, l = 0, 0, 0
while (k < m and l < n):
    for i in range(l, n):
        b.append(P[k][i])
        k += 1
# Print the last column from the remaining columns
    for i in range(k, m)
        b.append(P[i][n - 1])
        n -= 1
# Print the last row from the remaining rows
    if (k < m):
        for i in range(n - 1, l - 1, -1):
            b.append(P[m - 1][i])
            m -= 1
# Print the first column from the remaining columns
    if (l < n):
        for i in range(m - 1, k - 1, -1):
```

21: b.append($P[i][l]$)
22: l += 1
23: P_1= b[::-1]
24: return P_1

经过螺旋矩阵变换后, 对于序列 P_1 进行扩散操作, 得到扩散矩阵 $\boldsymbol{P}_2$。其中⊕为异或运算, en 为交叉混沌扩散后得到的序列, reshape[row,col] 表示把一维序列 en 转换为二维矩阵。按照公式(11)扩散。

$$\begin{cases} en[0]=P_1[0]\oplus K_1\oplus K_2 \\ en[i]=K_1\oplus K_2\oplus\left(P_1[i]+K_1[i]\right)\oplus en[i-1] \\ \boldsymbol{P}_2=en.\text{reshape}[row,col] \end{cases} \tag{11}$$

经过扩散后的矩阵, 密文的前一像素和后一像素相互联系, 达到雪崩效应, 增强了密文的敏感性。最后, 对扩散矩阵按照 Algorithm 2 进行交叉混沌序列置乱, 其中利用构造的具有明文影响的混沌交叉序列分别交换两次, 得到置乱图像 P_3。至此, 图像加密的整个过程已经完成, P_3 即为最终的密文图像。

Algorithm 2:Chaotic scrambling algorithm
Input: P_2, chaos sequence(K_3, K_4)
Output :P_3(the encrypted image with size row*col)
01: D = (P_2.T).reshape(row * col)
02: Q = np.zeros((row * col))
03:for i in range(row * col):
04 Q[i] = D[i]
05: D[i] = D[K_3[i]]
06: D[K_3[i]] = Q[i]
07: # The second mess
08: Q[i] = D[i]
09: D[i] = D[K_4[i]]
10: D[K_4[i]] = Q[i]
11: P_3 = D.reshape(row, col)
12: return P_3

3.2 解密步骤

解密过程是加密的逆过程。首先进行交叉混沌序列的逆操作得到一个置乱矩阵, 具体操作按照 Algorithm3 进行, 从而得到置乱前图像 P'$_2$, 再对 P'$_2$ 进行拉伸操作得到 P_2。

Algorithm 3:Chaotic scrambling algorithm
Input: P_3, chaos sequence(K_3, K_4)
Output :P_2(the encrypted image with size row*col)
01: D = (P_3.T).reshape(row * col)
02: Q = np.zeros(row * col)
03:for i in range(row * col):
04 Q[i] = D[K_3[i]]
05: D[K_3[i]] = D[i]
06: D[i] = Q[i]
07: # The second mess
08: Q[i] = D[K_4[i]]
09: D[K_4[i]] = D[i]
10: D[i] = Q[i]
11: P_2 = D.reshape(row, col)
12: return P_2

然后对置乱矩阵 $\boldsymbol{P}_2$ 按照公式(12)进行扩散得到 P_1

$$\begin{cases} \boldsymbol{P}_2=\boldsymbol{P}_2.\text{reshape}(row\cdot col) \\ P_1[0]=\boldsymbol{P}_2[0]\oplus K_1\oplus K_2 \\ P_1[i]=K_1\oplus K_2\oplus\left(\boldsymbol{P}_2[i]+K_1[i]\right)\oplus P_1[i-1] \end{cases} \tag{12}$$

最后对 P_1 按照 Algorithm4 再进行螺旋变换得到最终的明文 P。

Algorithm 4:Helical matrix transformation
Input: P_1 (plaintext)
Output :P(after helical matrix transformation)
01: m = len(P_1)
02: n = len(P_1[0])
03: b = []
04: i, k, l = 0, 0, 0
05: while (k < m and l < n):
06: for i in range(l, n):
07: b.append(P_1[k][i])
08: k += 1
09:# Print the last column from the remaining columns
10: for i in range(k, m)
11: b.append(P_1[i][n - 1])
12: n -= 1
13: # Print the last row from the remaining rows
14: if (k < m):
15: for i in range(n - 1, l - 1, -1):
16: b.append(P_1[m - 1][i])
17: m -= 1
18: # Print the first column from the remaining columns
19: if (l < n):
20: for i in range(m - 1, k - 1, -1):
21: b.append(P_1[i][l])
22: l += 1
23: P= b[::-1]
24:return P

4 实验分析

为验证本文基于改进 Logistic 混沌和交叉混沌扩散的强鲁棒性图像加密的有效性和可行性, 采用 Pycharm 作为实验平台, python 作为语言环境,

通过实验效果展示与文献对比的方式来突出本文算法的优势。

4.1 加解密与直方图

为了验证所提出算法的可行性, 分别选取 512×512 大小的 lena 图像、cameraman 图像和 peppers 图像。如图 4 所示, a、b、c 三列分别对应待加密的原图像, 密文图像以及解密图像, 从图中可以清楚看到原图像执行本文算法后已经达到了类似噪声的密文图像, 从而在图像传输的时候, 起到保护图像安全的作用。直方图反映了图像像素之间的相关联系, 是反映加密效果好坏的重要标准。如图 5 所示, d、e、f 三列分别为原图像、密文图像、解密图像的直方图。由于原始图像没有被破坏, 像素之间紧密联系容易被统计攻击, 而经过本文加密后的图像, 像素值趋于平均, 可以抵御攻击者的统计攻击, 表明本文算法保障了图像传输过程中的安全。

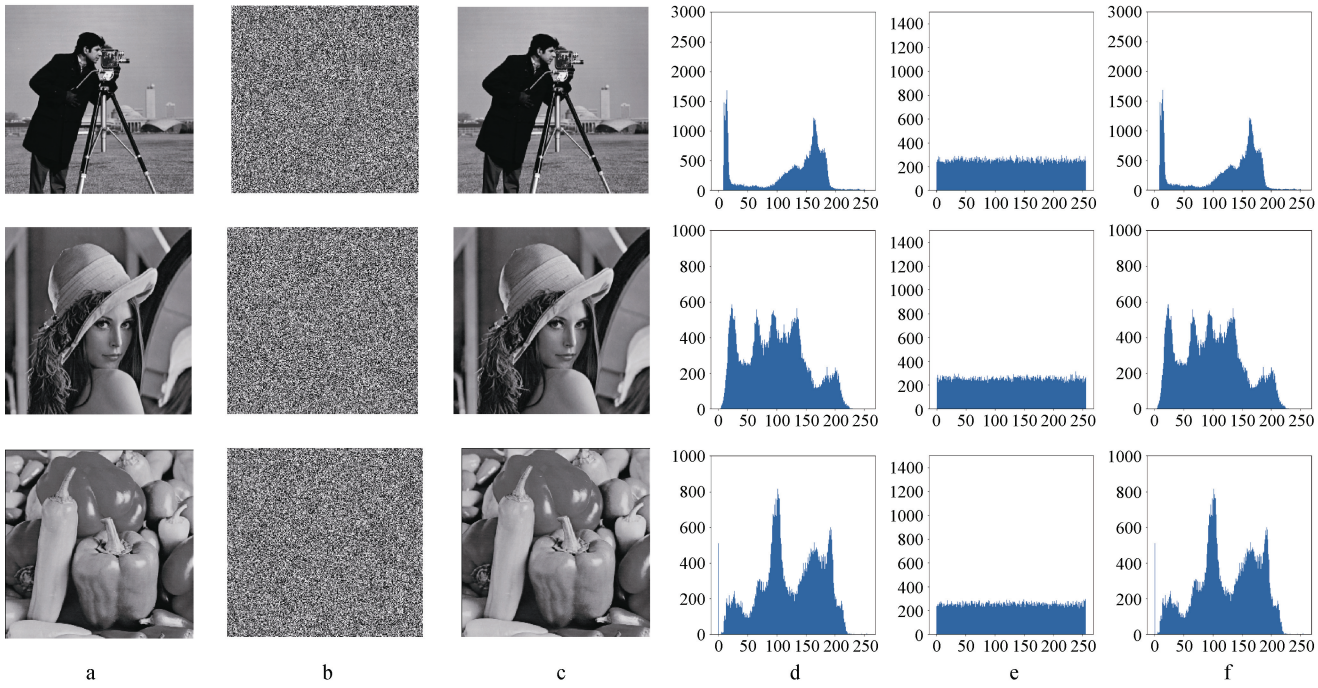

图 5 加解密与直方图分析

Figure 5 Encryption and decryption and histogram analysis

4.2 密钥空间

理想的图像加密算法必须有足够的密钥空间来抵抗暴力攻击。一般来说, 密钥空间大于 2^{100}, 就能够保证其安全性[22]。本文的密钥主要包括改进的 Logistic 混沌的参数 z_0,α。Kent 混沌中的 α, s_0 密钥精度为 10^{15}, 密钥空间 $10^{15\times4}=10^{60}\gg2^{100}$, 远远大于安全所需的密钥空间, 能够抵御穷举攻击。

4.3 相关性分析

相关性是描述图像相邻像素之间的关系。一般来说, 原始图像之间相邻像素之间彼此相关, 有很大的相关性。相关性包括正相关和负相关, 相邻像素相关性很强则会接近于±1。反之, 趋近于 0 则表现为不相关。图像加密则是打破这种强相关关系, 达到保护图像的安全, 像素相关性的衡量可以通过水平、垂直和对角线这几个方向上的数值进行描述。相关系数 r 如公式(13)。

$$r_{x,y}=\frac{\sum XY-\frac{1}{N}\sum x\sum y}{\sqrt{\left(\sum x^2-\frac{1}{N}(\sum x)^2\right)\left(\sum y^2-\frac{1}{N}(\sum y)^2\right)}} \tag{13}$$

为验证本文算法的可行性, 随机选取 2000 对相邻像素对 lena、camerman、peppers 进行相关性测试分布实验, 图 6 中 a、b、c 三列分别对应待加密的原图像, 密文图像以及解密图像, 图 6 中 d、e、f 三列分别为原图像、密文图像、解密图像的相邻像素关系图。由图可见, 图像的明文相邻像素主要分布在对角线上, 说明相邻像素基本相同, 而密文分布的更加均匀, 说明相邻像素的关系更加随机。

表 1 给出了本文算法和文献[8,10,12]相关系数比较, 从表中发现, 本文和文献的明文相邻像素在三个方向的相关性都接近于 1, 没有明显差距, 未加密之间图像中相邻像素之间具有极高的相关性。而

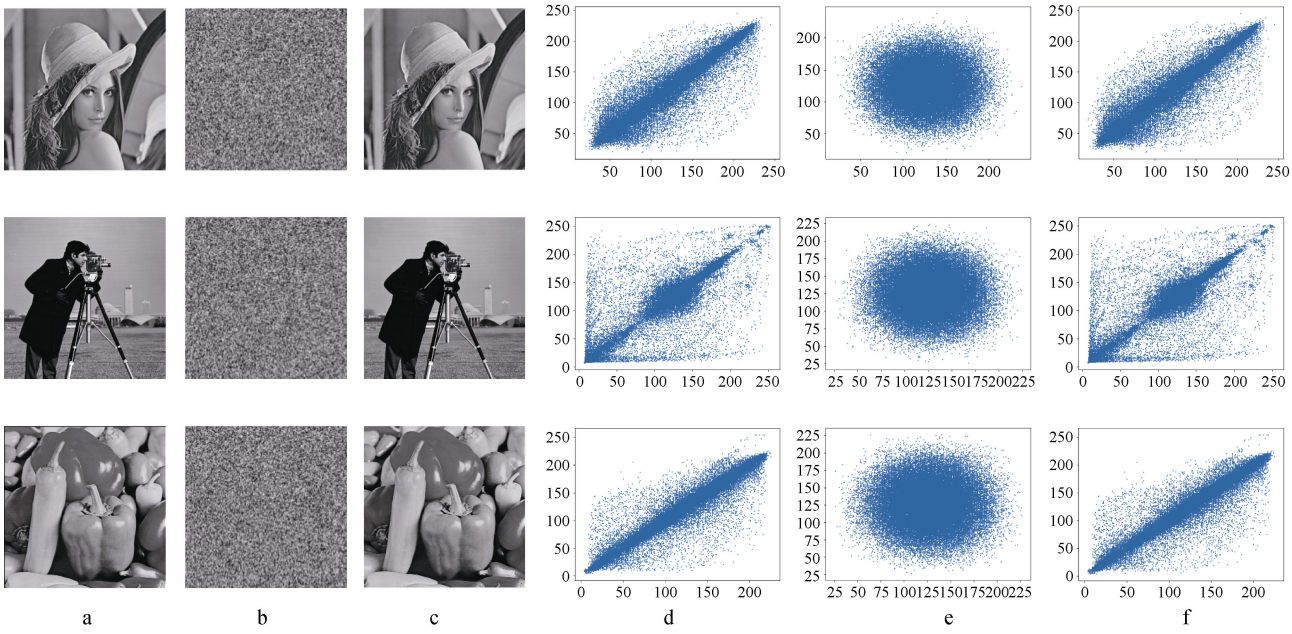

图 6　相邻像素相关性

Figure 6　Correlation of adjacent pixels

表 1　相关系数的分析

Table 1　Correlation coefficient analysis

		本文	文献[8]	文献[10]	文献[12]
明文图像(lena)	水平	0.9341	0.9663	0.9701	0.9433
	垂直	0.9678	0.9789	0.9827	0.9666
	对角线	0.9107	0.9843	0.9659	0.9186
	平均值	0.9375	0.9865	0.9729	0.9428
密文图像(lena)	水平	–0.0030	–0.0036	0.0068	0.0015
	垂直	–0.0031	–0.0028	0.0024	0.0090
	对角线	0.0021	–0.0021	0.0259	0.0120
	平均值	0.0027	–0.0028	0.0138	0.075

经过加密后的图像相邻像素无规律分布本文算法相关系数最低, 平均值为 0.0027, 更接近于 0, 优于文献[8,10,12], 说明该算法很好地破除了明文的相邻像素相关性。

4.4　明文敏感性及信息熵分析

明文敏感性指明文图像某个位置的像素值发生了改变, 改变的的密文图像与原来明文图像所对应的密文之间的差异, 用像素变化率(NPCR)和归一化强度(UACI)来评估抗差分攻击的能力[23]。公式为(14)。

$$\begin{cases} NPCR = \dfrac{1}{h\times w}\sum D(i,j)\times 100\% \\ UACI = \dfrac{1}{h\times w}\sum \dfrac{\left|C_1(i,j)-C_2(i,j)\right|}{255}\times 100\% \end{cases} \tag{14}$$

$$\begin{cases} C_1(i,j)-C_2(i,j)=0, D(i,j)=0 \\ C_1(i,j)-C_2(i,j)\neq 0, D(i,j)=1 \end{cases} \tag{15}$$

其中, h 和 w 是图像的行数和列数, $C_1(i,j)$ 和 $C_2(i,j)$ 分别表示原图像像素值改变前后所对应的密文图像。

本文通过 lena、cameraman、peppers 图像与文献[8,10,12]进行实验对比, 实验数据如表 2 所示。可以看到本文的 NPCR 与 UACI 都接近于理想值, 明文信息对变化敏感能有效抵抗差分攻击。

表 2　NPCR 与 UACI 分析

Table 2　NPCR and UACI analysis

		Lena	Camera man	Peppers	Average
本文	NPCR	0.9962	0.9959	0.9961	0.9961
	UACI	0.3328	0.3337	0.3334	0.3336
文献[8]	NPCR	0.9961	0.9960	0.9961	0.9961
	UACI	0.3349	0.3348	0.3346	0.3347
文献[10]	NPCR	0.9955	0.9955	0.9953	0.9954
	UACI	0.3346	0.3348	0.3345	0.3346
文献[12]	NPCR	0.9962	0.9961	0.9962	0.9962
	UACI	0.3333	0.3334	0.3335	0.3334

信息熵是一个系统信息含量量化的指标。在图像加密中, 常用来表示图像整体的随机性。信息熵越大, 表明图像像素越混乱, 加密效果越好。信息熵 E_n 为式(16)。

$$E_n(m) = \sum_{i=0}^{M-1} p(c_i)\log_2 p(c_i) \tag{16}$$

本文通过 lena、cameraman、peppers 图像与文献

[8,10,12]进行实验对比, 实验数据如表 3 所示。可以看到本文信息熵高于文献[8,10,12], 比同类加密算法更加接近于 8, 加密效果更好。

表 3 信息熵分析

Table 3 Information entropy analysis

		Lena	Camera man	Peppers	Average
本文	信息熵	7.9976	7.9975	7.9974	7.9975
文献[8]	信息熵	7.9973	7.9972	7.9972	7.9973
文献[10]	信息熵	7.9973	7.9972	7.9972	7.9973
文献[12]	信息熵	7.9939	7.9972	7.9973	7.9961

4.5 密钥敏感性分析

密钥敏感性指加密算法中的密钥参数发生细微的变化时加密同一明文图像得到的解密图像之间的变化。采用单一变量的方式给出加解密过程中密钥改变前后的两密文和两解密图像间的相关系数, 如表 4。选取改进的 Logistic 混沌映射的初始值 z_0 进行视觉上的实验, 其他密钥值保持不变, 改变量分别为 $\Delta z_0=10^{-16}$、$\Delta z_0=10^{-17}$、$\Delta z_0=10^{-18}$ 和正确密钥所分别对应的解密效果如图 7 所示。表明本文算法的密钥为 10^{-17}, 具有极高的敏感性。

表 4 密钥敏感性分析

Table 4 Key sensitivity analysis

改变量	加密 Lena	解密 Lena	加密 Peppers	解密 Pepper
$\Delta z_0=10^{-16}$	0.0002	0.0011	–0.0001	0.0021
$\Delta\alpha=10^{-14}$	–0.0006	0.0050	0.0004	0.0017
$\Delta\beta=10^{-15}$	0.0003	0.0082	–0.0091	–0.0002
$\Delta s_0=10^{-18}$	0.0065	–0.0001	0.0079	0.0035
$\Delta H_1=10^{-12}$	–0.0041	–0.0088	0.0057	0.0009
$\Delta H_2=10^{-14}$	0.0077	0.0029	0.0007	0.0011
$\Delta H_3=10^{-15}$	0.0048	0.0026	–0.0092	0.0060
$\Delta H_4=10^{-13}$	0.0020	0.0014	–0.0008	0.0019

图 7 密钥敏感性分析

Figure 7 Key sensitivity analysis

由表 4 可知, 无论是在加密还是在解密过程中, 密钥改变前后, 密文和解密图像的相关系数都很接近 0, 说明加密出来的密文或解密图像完全不同, 说明本文对密钥极其敏感。

4.6 鲁棒性分析

图像的鲁棒性分析是衡量加密算法标准不可或缺的分析指标之一。鲁棒性的好坏取决于当密文图像在传输中被攻击者破坏, 而在解密方能够解密出满足于生产或者生活所需的要求。比如图像传输中遭遇攻击者的破坏, 在接收方收到一个被破坏的加密图像, 这时候利用解密方法能够完美的重构出所需的图像就显得至关重要。当然, 解密图像越清晰噪声越少, 证明算法的鲁棒能力越强。基于上述理论, 本文以椒盐噪声、高斯噪声和图像的剪切攻击来模拟图像传输中可能遭遇的情况, 进行实验分析本文算法的鲁棒性能力。

4.6.1 椒盐噪声

椒盐噪声是一种随机出现的黑点或者白点的脉冲噪声, 图像在传输中可能会遇到椒盐噪声的影响进而失真, 无法正确解密明文信息。本文通过对密文图像中分别加入强度 s 为 0.05、0.10、0.15、0.2 的椒盐噪声。经过解密算法后, 得到的解密图像如图 8 所示。

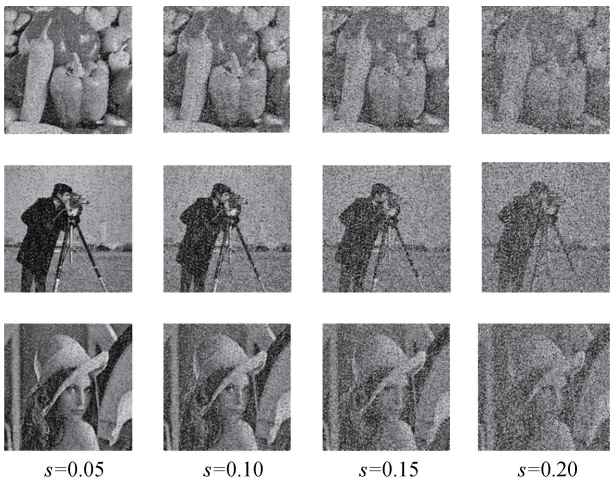

图 8 不同强度椒盐噪声分析

Figure 8 Analysis of pepper and salt noise with different intensities

从中可以看到, 加入强度为 0.05 的椒盐噪声时解密图像几乎不受影响, 可以看到大部分的细节信息。即使加入噪声强度为 0.2 的黑白噪声, 解密图像仍然能看到图像的轮廓信息, 表明本文算法能够抵御一定的椒盐噪声攻击, 具有较强的鲁棒性能。

4.6.2 高斯噪声

高斯噪声是一种概率密度符合高斯分布的常见噪声, 类比椒盐噪声攻击, 本文对加密图像分别加

入强度 s 为 0.05、0.1、0.15、0.2 的高斯噪声, 再对添加噪声后的图像进行解密, 对比分析添加噪声前后的影响程度。解密结果如图 9 所示。

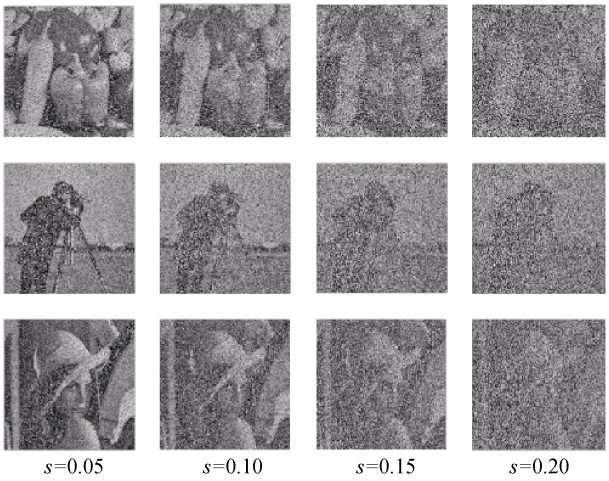

图 9　不同强度高斯噪声分析

Figure 9　Gaussian noise analysis with different intensities

分析可知, 低强度的高斯噪声对本文算法影响较小, 图像的轮廓和细节信息相对清晰, 当强度为 0.2 时, 图像有点模糊但是还能看到图像的轮廓信息, 表明本文算法对于高斯噪声的攻击有一定的防御能力。

4.6.3　剪切攻击

图像在信道进行传输可能会遇到不规则大面积的剪切攻击, 导致解密算法难以恢复出明文的信息。因此, 本文对加密后的三幅图像分别进行 1/16、1/4、5/16、1/2 大小尺寸的剪切。如图 10 所示, 当对图像剪切 1/16 和 1/4 时, 解密图像还是可以明显看出图像的细节.当对图像剪切 1/2 时, 虽然大部分细节已经丢失, 但是可以看到图像的大致轮廓, 能够满足一定的重构要求。另外, 为了消除剪切位置可能带来的影响, 本文对密文图像的四周及中心进行 1/16 的剪切攻击, 结果仍然看到图像的清晰轮廓, 可以看到大部分图像细节。通过对密文图像进行不同尺寸的剪切, 可以表明本文算法能够抵御至少 1/2 的剪切攻击, 具有较强的鲁棒性, 在图像传输中有着很好的保护作用。

4.6.4　鲁棒性效果对比分析

本文以 512×512 大小的 lena 图像为例, 在强度为 0.2 椒盐噪声和高斯噪声, 密文图像被 1/2 遮挡时, 与文献[8,10]进行了对比实验分析。实验结果如图 11 所示, 本文算法在强度为 0.2 的椒盐和高斯噪声下仍可以恢复明文的轮廓, 即使对密文图像进行 1/2 的遮挡, 还是具有不错的鲁棒效果。而文献[8]和文献[10], 虽然在噪声强度为 0.2 的情况下也能看到部分轮廓, 但是当对密文遮挡 1/2 时, 恢复效果明显没有本文算法鲁棒效果好。

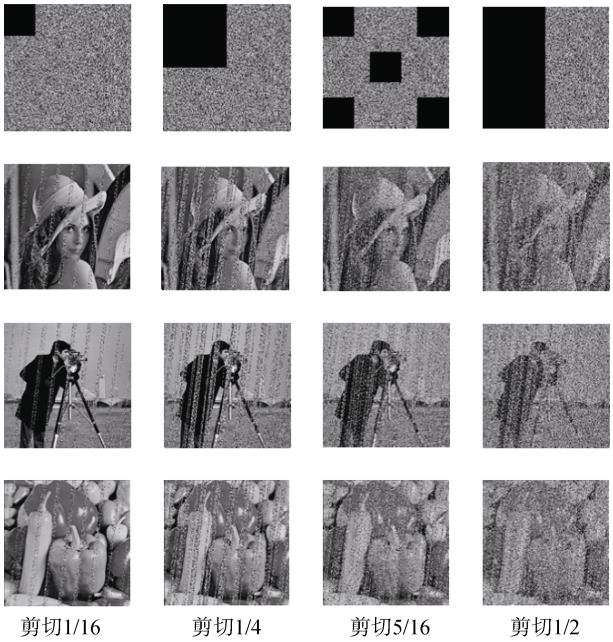

图 10　遮挡攻击分析

Figure 10　Occlusion attack analysis

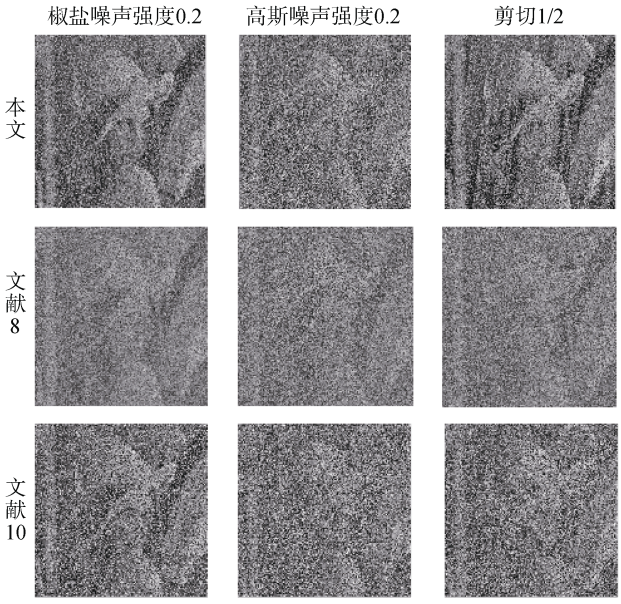

图 11　鲁棒性效果对比分析

Figure 11　Comparative analysis of robustness effect

4.6.5　MSE、PSNR、SSIM 对比分析

对密文图像添加强度为 0.15 的高斯噪声, 然后对比文献[8,10,12]可以得到不同算法的解密图像与明文之间的 MSE、PSNR 和 SSIM, 如表 5 所示。其中 MSE 表示均方误差, 是衡量图像质量的指标之一。计算原理为真实值与预测值的差值的平方然后

求和在平均, 公式如式(17)。PSNR 为峰值信噪比, PSNR 的值越大表示图像重构的质量越高, PSNR 的公式如式(18)。SSIM 为结构相似性, MAX 表示图像点颜色最大值, L 表示损失函数, 本文的损失函数为式 MSE 损失函数, SSIM 的公式如式(19)。

表 5 不同算法 MSE、PSNR 和 SSIM 对比分析

Table 5 Comparison and analysis of MSE, PSNR and SSIM of different algorithms

	本文算法	文献[8]	文献[10]	文献[12]
MSE	6766.4	7492.3	7812.5	7752.6
PSNR	9.8216	9.3842	9.2021	9.2362
SSIM	0.4438	0.4331	0.4268	0.4239

$$MSE=\frac{1}{M\cdot N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[I(i,j)-K(i,j)\right]^2 \tag{17}$$

$$PSNR=10\log_{10}\left(\frac{MAX^2}{L}\right) \tag{18}$$

$$SSIM(x,y)=l(x,y)^{\alpha}\cdot c(x,y)^{\beta}\cdot s(x,y)^{\gamma} \tag{19}$$

$$l(x,y)=\frac{2\mu_x\mu_y+c_1}{\mu_x^2+\mu_y^2+c_1} \tag{20}$$

$$c(x,y)=\frac{2\sigma_x\sigma_y+c_2}{\sigma_x^2+\sigma_y^2+c_2} \tag{21}$$

$$s(x,y)=\frac{\sigma_{xy}+c_3}{\sigma_x\sigma_y+c_3} \tag{22}$$

其中, $c_3=c_3/2$, μ_x 为 x 的均值, μ_y 为 y 的均值, σ_x^2 为 x 的方差, σ_y^2 为 y 的方差, σ_{xy} 为 x 和 y 的协方差, $c_1=(k_1L)^2$ 和 $c_2=(k_2L)^2$ 为两个常数, L 为 255, $k_1=0.01$, $k_2=0.03$。本文 α, β, γ 都取 1。

从表 5 中可以看到本文算法的 PSNR 略高于其他对比文献, 主要在于本文解决了传统一维 logistic 混沌存在较大空白区、直方图分布不均匀的缺点, 为本文算法中交叉混沌的构造提供了很大优势。本文通过置乱-扩散-置乱的交叉扩散置乱使得密文图像变得更加混沌, 极大地增强了图像信息的鲁棒性。

如图 12 所示, 本文算法将不同强度的椒盐噪声和高斯噪声添加到密文图像以及遮挡攻击下解密图像和明文图像之间的 PSNR。从图中可以看出, 当椒盐噪声强度为 0.2 时, 不同图像的 PSNR 仍然大于 10, 高斯噪声对应的 PSNR 要略低于椒盐噪声, 可见本文对椒盐噪声的抵抗性更强, 当对密文图像进行一半的遮挡时, 本文测试的不同图像的 PSNR 都在 10 以上, 说明本文算法具有较强的抗遮挡能力

4.7 抗选择明文攻击

选择明文攻击指通过特殊的明文, 与对应的密文推导出中间密钥。一个良好的加密方法应该具备抵御选择明文攻击的能力。如图 13 所示, 本文选择全黑和全白的两幅图像进行测试, 可以发现通过特殊图像进行明文攻击, 直方图分布均衡, 无法获取有效明文信息。表明本文算法能够抵御明文攻击。

4.8 抗差分攻击分析

差分攻击是指攻击者试图通过修改明文图像的一个像素或一个比特来找出两个密文图像之间的的关系。为了测量明文图像单个像素变化对对应密文的影响, 分别采用了像素变化率 NPCR 和平均变化强度 UACI 方法来定量计算加密算法对差分攻击的抵御能力。用式(14)分别计算出随机一点像素值相差 1, 交换不同像素的位置的两组明文加密出的密文的 NPCR 和 UACI, 如表 6 所示。

由表 6 可见, 只要稍微改变明文像素, 得到的两组密文完全不同, 说明算法能抗差分攻击。

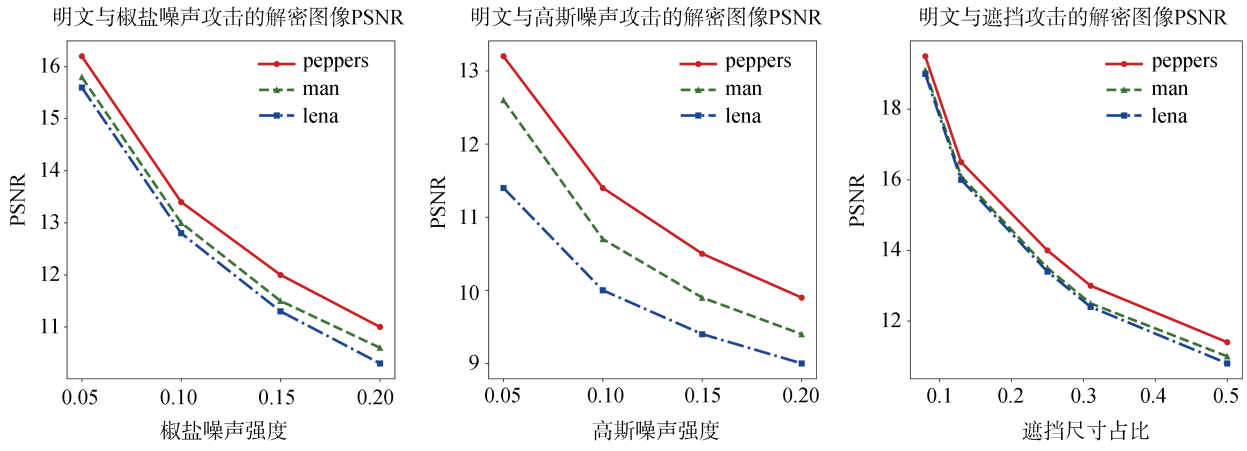

图 12 PSNR 分析

Figure 12 PSNR analysis

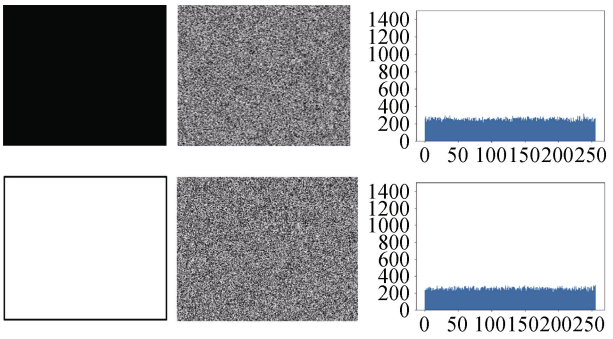

图 13 选择明文攻击分析

Figure 13 Selects plaintext attack analysis

表 6 抗差分攻击

Table 6 Differential attack resistance

改变方式	第一张第一个像素点加 1	交换第一张和第二张第一个像素点位置
NPCR	0.9921	0.9942
UACI	0.1492	0.1503

4.9 抗深度学习攻击

随着深度人工智能的发展, 深度学习也被应用到了图像攻击中[24-25], 深度学习可以通过神经网络自动地分析数据和数据之间的关系, 从而形成映射; 本文使用混沌系统消除了密文与明文在网络训练中的对称关系, 增加训练难度。为证明本文的抗深度学习攻击, 本文采用生成对抗网络对 20000 张明密文图像进行训练, 网络自动学习密文与明文的映射关系, 并使用普通图像、医学图像、生物图像、遥感图像进行测试, 图 14 中 a～d 为测试图像原图像, 分别分普通 lena 图像、医学 CT 图像、生物 Cell 图像和遥感图像, e～h 为测试图像密文图像, i～l 为深度学习恢复图像。可见, 深度学习攻击后的解密图像与明文图像相差很大, 解密图像几乎看不出明文图像信息, 说明本文具有抗深度学习攻击特性, 进一步保证了图像的安全性。

4.10 算法效率分析

以 512×512 大小的 lena 图像进行加解密, 并与文献[8,10,12]对比, 如表 7 所示。可以看出本文算法时间略高于文献[12], 低于文献[8]和文献[10]。由于本算法为消除螺旋变换部分像素未发生改变, 所采用了两次置乱, 提高算法的鲁棒性的同时消耗了一定的时间。

5 结论

本文提出一种置乱-扩散-置乱的加密框架, 改进了一维 Logistic 混沌系统, 混沌序列分布更加随机。利用明文的哈希值来构造混沌系统的初始密钥, 明文像素值引进混沌序列, 提高明文的敏感性, 利用螺旋矩阵变换进行第一次置乱。对置乱后图像进行交叉混沌序列的扩散, 为了避免螺旋矩阵变换个别像素位置未发生改变, 引进混沌系统的第二次置乱。实验结果表明, 本文算法能够抵御暴力攻击, 能够抵御选择明文攻击, 尤其是在鲁棒性方面具有更好的性能, 对于图像安全传输有一定的意义。目前本文只是针对灰度图像进行鲁棒性加密, 未来可以围绕彩色图像, 以及鲁棒性算法进一步优化方面进一步改进和完善。

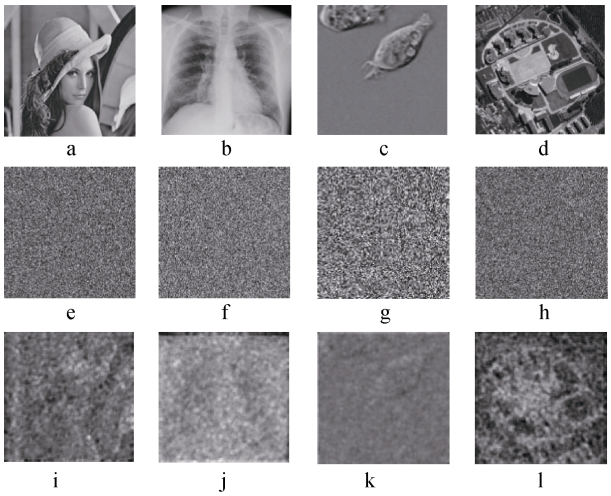

图 14 抗深度学习攻击

Figure 14 Resistance to deep learning attacks

表 7 算法加解密时间对比(s)

Table 7 Comparison of encryption and decryption time of the algorithm (unit:second)

测试图像	本文	文献[8]	文献[10]	文献[12]
lena(512×512)	加解密 3.096	加解密 3.110	加解密 3.680	加解密 3.064

参考文献

[1] Han X J, Li G D. Dynamic Cat Transformation and Chaotic Mapping Image Encryption Algorithm[J]. *Computer Engineering and Design*, 2020, 41(8): 2381-2387.
(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.)

[2] Hussain I, Anees A, Aslam M, et al. A Noise Resistant Symmetric Key Cryptosystem Based on S8 S-Boxes and Chaotic Maps[J]. *The European Physical Journal Plus*, 2018, 133(4): 167.

[3] Shafique A, Ahmed F. Image Encryption Using Dynamic S-Box Substitution in the Wavelet Domain[J]. *Wireless Personal Communications*, 2020, 115(3): 2243-2268.

[4] Huang X. Research on chaotic image encryption algorithm based on scrambling diffusion mechanism[D]. Harbin: Helongjiang University, 2020.

(黄欣. 基于置乱扩散机制的混沌图像加密算法研究[D]. 哈尔滨: 黑龙江大学, 2020.)

[5] He P C, Sun K H, Zhu C X. A Novel Image Encryption Algorithm Based on the Delayed Maps and Permutation-Confusion-Diffusion Architecture[J]. *Security and Communication Networks*, 2021, 2021: 6679288.

[6] Zhu S Q, Zhu C X, Fu Y, et al. A Secure Image Encryption Scheme with Compression-Confusion-Diffusion Structure[J]. *Multimedia Tools and Applications*, 2020, 79(43): 31957-31980.

[7] Liu L D, Lei Y H, Wang D. A Fast Chaotic Image Encryption Scheme with Simultaneous Permutation-Diffusion Operation[J]. *IEEE Access*, 2020, 8: 27361-27374.

[8] Firdous A, Rehman A U, Saad Missen M M. A Gray Image Encryption Technique Using the Concept of Water Waves, Chaos and Hash Function[J]. *IEEE Access*, 2021, 9: 11675-11693.

[9] Roy M, Chakraborty S, Mali K. The MSK: A Simple and Robust Image Encryption Method[J]. *Multimedia Tools and Applications*, 2021, 80(14): 21261-21291.

[10] ur Rehman A, Xiao D, 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.

[11] Li F Y, Wu H B, Zhou G, et al. Robust Real-Time Image Encryption with Aperiodic Chaotic Map and Random-Cycling Bit Shift[J]. *Journal of Real-Time Image Processing*, 2019, 16(3): 775-790.

[12] Wang X Y, Zhao M C. An Image Encryption Algorithm Based on Hyperchaotic System and DNA Coding[J]. *Optics & Laser Technology*, 2021, 143: 107316.

[13] Zolfaghari B, Koshiba T. Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap[J]. *Applied System Innovation*, 2022, 5(3): 57.

[14] [14] Elkandoz M T, Alexan W. Image Encryption Based on a Combination of Multiple Chaotic Maps[J]. *Multimedia Tools and Applications*, 2022, 81(18): 25497-25518.

[15] Singh S P, Bhatnagar G. A Novel Biometric Inspired Robust Security Framework for Medical Images[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2021, 33(3): 810-823.

[16] Muhammad Z M Z, Özkaynak F. An Image Encryption Algorithm Based on Chaotic Selection of Robust Cryptographic Primitives[J]. *IEEE Access*, 2827, 8: 56581-56589.

[17] Rawat N, Kim B, Muniraj I, et al. Compressive Sensing Based Robust Multispectral Double-Image Encryption[J]. *Applied Optics*, 2015, 54(7): 1782-1793.

[18] Mohamed H G, ElKamchouchi D H, Moussa K H. A Novel Color Image Encryption Algorithm Based on Hyperchaotic Maps and Mitochondrial DNA Sequences[J]. *Entropy*, 2020, 22(2): 158.

[19] Zeng X Q, Ye R S. Chaotic Image Encryption Algorithm Based on Improved Logistic Map[J]. *Computer Engineering*, 2021, 47(11): 158-165, 174.
(曾祥秋, 叶瑞松. 基于改进 Logistic 映射的混沌图像加密算法[J]. *计算机工程*, 2021, 47(11): 158-165, 174.)

[20] Xie G B, Chen Z W. Color Image Adaptive Encryption Algorithm Based on Improved CAT Scrambling and Henon_Kent Chaotic System[J]. *Application Research of Computers*, 2019, 36(11): 3369-3372.
(谢国波, 陈志伟. 基于改进的 CAT 置乱与 Henon_Kent 混沌系统的彩色图像自适应加密算法[J]. *计算机应用研究*, 2019, 36(11): 3369-3372.)

[21] 钱晓华, 陈夏晗. 深度学习中螺旋变换数据扩增方法、系统、介质及设备: CN111292230A[P]. 2020-06-16.

[22] LIU Q. Research on image encryption algorithm based on chaotic mapping [D]. Nanchang University.
(刘倩. 基于混沌映射的图像加密算法研究[D]. 南昌大学.)

[23] Ban D H, Lv X, Wang X Y. Efficient Image Encryption Algorithm Based on 1D Chaotic Map[J]. *Computer Science*, 2020, 47(4): 278-284.
(班多晗, 吕鑫, 王鑫元. 基于一维混沌映射的高效图像加密算法[J]. *计算机科学*, 2020, 47(4): 278-284.)

[24] Hai H, Pan S X, Liao M H, et al. Cryptanalysis of Random-Phase-Encoding-Based Optical Cryptosystem *via* Deep Learning[J]. *Optics Express*, 2019, 27(15): 21204-21213.

[25] Xu Z, Zhou X, Bai X, et al. Attacking Asymmetric Cryptosystem Based on Phase Truncated Fourier Fransform by Deep Learning[J]. *Acta Physica Sinica*, 2021, 70(14): 226-232.
(徐昭, 周昕, 白星, 等. 基于深度学习的相位截断傅里叶变换非对称加密系统攻击方法[J]. *物理学报*, 2021, 70(14): 226-232.)

郭媛(1974—), 女, 辽宁台安人, 博士, 教授, 研究生导师, CCF 会员, 1997 年于齐齐哈尔大学获得学士学位, 2004 年和 2008 年于燕山大学获得硕士和博士学位。2012—2013 年霍普金斯大学访问学者。现为齐齐哈尔大学教务处处长。主要从事光电检测与传感器技术, 光学散斑测量, 光学图像加密与隐私保护。Email: guoyuan171@126.com

贾德宝(1996—), 男, 山东曹县人, 硕士研究生, 2021 年于德州学院获得学士学位, 主要从事图像安全和深度学习方面的研究。Email: 981788677@qq.com