文章编号:1007-5321(2021)06-0040-08 DOI:10.13190/j.jbupt.2021-061

结合 S 盒与混沌映射的图像加密算法

张 雷[1], 陈 川[1,2], 谭淇匀[1], 郝茂鑫[1], 杨学康[1]
(1. 齐鲁工业大学(山东省科学院) 网络空间安全学院, 济南 250353;
2. 齐鲁工业大学(山东省科学院) 山东省计算机网络重点实验室, 济南 250014)

摘要: 针对现有图像加密算法存在的加密质量低、明文敏感性差等问题,提出了一种结合 S 盒与混沌映射的图像加密算法. 对明文图像的散列值进行运算,得到混沌系统的密钥,以进行置乱和扩散,S 盒通过 Logistic 映射生成. 利用二维 Logistic 映射和 Chen 混沌系统生成 2 个与明文图像大小相同的混沌序列,用来对图像的每个像素进行互换和一阶扩散,并利用混沌序列选择 S 盒元素与各像素值进行比特异或与同或运算,再对整体的各像素作二阶、三阶扩散处理. 仿真测试和安全性能分析结果表明,所提算法具有良好的加密效果、鲁棒性和明文敏感性,也能较好地抵抗各类攻击.

关 键 词: 图像加密算法; 混沌系统; S 盒; 置乱扩散; 安全性分析
中图分类号: TP309 **文献标志码**: A

An Image Encryption Algorithm Combining S-Box and Chaotic Mapping

ZHANG Lei[1], CHEN Chuan[1,2], TAN Qi-yun[1], HAO Mao-xin[1], YANG Xue-kang[1]
(1. School of Cyber Security, Qilu University of Technology (Shandong Academy of Sciences), Jinan 250353, China;
2. Shandong Provincial Key Laboratory of Computer Networks, Qilu University of Technology (Shandong Academy of Sciences), Jinan 250014, China)

Abstract: To solve the problems of low encryption quality and poor plaintext sensitivity in the existing image encryption algorithms, an image encryption algorithm combining S-box and chaotic mapping is proposed. The Hash value of the plaintext image is used to generate the key of the chaotic system, which can operate scrambling and diffusion. In addition, the S-box is generated through the Logistic chaotic system. By using the two-dimensional Logistic mapping and Chen chaotic system to generate two chaotic sequences, which have the same image size with the plaintext image, the algorithm operates exchange and the first-order diffusion for each pixel of the image. Then, the algorithm selects the S-box elements based on the chaotic sequences to do bit XOR and XNOR operations for each pixel value, and operates the second-order and third-order diffusion on all the pixels. Simulation results and security performance analysis show that, the proposed algorithm has good encryption effect, robustness and plaintext sensitivity, and thus it can resist various attacks.

Key words: image encryption algorithm; chaotic system; S-box; scrambling and diffusion; security analysis

收稿日期: 2021-04-09
基金项目: 国家自然科学基金面上项目(62172244); 2020 年齐鲁工业大学(山东省科学院)大学生创新创业训练计划项目; 齐鲁工业大学(山东省科学院)教改项目(201804)
作者简介: 张 雷(1999—), 男, 本科生.
通信作者: 陈 川(1982—), 男, 讲师, E-mail:chenchuan.3000@163.com.

随着移动通信网络和互联网的快速发展，诸如图片、视频等多媒体信息网络资源已经成为人们日常生活中不可或缺的一部分. 相比于文字信息，图像信息更直观，交互性更强[1]. 但在数字图像的传递中，若不对图像进行处理，极有可能泄漏数据乃至个人隐私，从而导致无法估测的后果[2].

传统的加密算法对冗杂数据的处理能力有限. 而自混沌系统因其具有随机性、可遍历性等特征，在图片加密处理上拥有传统加密算法所没有的优势，在安全性上也得到了一定的提升[3].

随着混沌图像加密算法的不断完善，图像加密逐渐对高维、置乱等方面提出了要求[4]. 徐杨等[5]提出了一种使用量子混沌映射技术的算法，通过更高维度的映射，在加密的复杂度、计算能力等方面加以优化，但其数字图像混乱度低，缺乏随机性，在安全性表现上仍存在问题. 平萍等[6]提出的一种新型的基于比特重组的图像加密算法中，映射产生的 2 组混沌序列被应用于明文图像的行列置乱，得到的结论在统计特性和差分特性上表现较好，但在图像像素的扩散程度上尚有提升的空间. Talhaoui 等[7]提出了一种新型的一维混沌映射技术，并应用于混沌图像处理中，该算法在敏感度、抗差分能力以及加密速度上有显著的提升，但在鲁棒性上仍存在缺陷.

在此前的研究中，S 盒大多基于单一的运算规则，且对较大的图像处理具有一定的局限性[1,8]，存在扩散随机性差异. 如 Wang 等[9]提出的双混沌循环移位加密方案难以保证扩散中的随机性. Mousavi 等[10]提出在 Feistel 网络中对 S 盒和 P 盒产生的密码块进行迭代，虽然易于实现，但在复杂性上进行了取舍，有待进一步分析.

笔者设计了一种结合 S 盒与混沌映射的三阶扩散图像加解密算法，针对当下混沌系统敏感度低、置乱度低等问题进行改进. 在设计中采用传统的置乱扩散模式，并创新性地进行三阶扩散，以图像散列值作为混沌系统的密钥，在总体加密性能上，通过去除混沌序列的干扰项，命中 256 个区间，生成 S 盒，具有更均匀和更优的严格雪崩准则(SAC, strict avalanche criterion)测试结果，利用 Chen 混沌序列构建块矩阵，选择 S 盒元素，可以短时间内达到多个 S 盒的效果，有更高的随机性，使之具有较好的加密性能和安全性. 根据理论仿真结果，对 512 × 512 图像的加密效果良好，且密钥精度高，在同类型算法中具有良好的完整性、鲁棒性，其信息熵等参数优于其他算法，在对 S 盒的 SAC 测试中达到了较高水平.

1　基础分析

S 盒通常是分组密码算法中的非线性部分，主要的功能便是实现“代替”操作，能起到混乱和扩散的作用. 利用具有良好伪随机性的混沌系统构造 S 盒，可以高效地提升其安全性.

1.1　Logistic 混沌映射

Logistic 映射是一种形式简单，使用普遍的混沌系统，定义为

$$x_{n+1}=\mu x_n(1-x_n) \tag{1}$$

其中：$x\in[0,1]$，$\mu\in[0,4]$ 被称为分支参数. 当 μ 的值变化时，该迭代方程会展现出不同的动力学极限行为. 当 $\mu\in(3.569\,945\,6,4]$ 时，logistic 映射是非周期，不收敛，处于混沌状态.

二维 logistic 映射是基于一维 logistic 映射构造出来的，其在继承一维 logistic 映射优点的基础上具有更好的随机性. 定义一次耦合项二维 logistic 混沌系统为

$$\left.\begin{aligned}x_{n+1}&=4\mu_1 x_n(1-x_n)+\gamma y_n\\ y_{n+1}&=4\mu_2 y_n(1-y_n)+\gamma x_n\end{aligned}\right\} \tag{2}$$

其中：γ 为耦合控制参数，与分支参数共同控制系统的动力学行为.

1.2　超混沌 Chen 映射

超混沌 Chen 映射有 4 个维度，复杂性高，抗攻击能力强，其动力学方程式定义为

$$\left.\begin{aligned}\dot{y}_1&=m(y_2-y_1)\\ \dot{y}_2&=-y_1y_2+qy_1+py_2\\ \dot{y}_3&=y_1y_2-ny_3\\ \dot{y}_4&=y_2y_3+ry_4\end{aligned}\right\} \tag{3}$$

其中：y_1,y_2,y_3,y_4 为系统状态变量，m,q,p,y 为系统的控制参数. 当 $m=35$，$n=3$，$p=12$，$q=7$，$r\in(0.085,0.798]$ 时，该超混沌系统处于混沌状态.

2　图像混沌加密算法描述

笔者提出了结合 S 盒与混沌映射的图像加解密算法，加密算法流程如图 1 所示. 对明文图像取散列值生成密钥，再对密钥运算生成 3 种混沌系统的初值，通过 Chen 映射产生 4 个混沌序列，形成 16 种组合，依次选择 16 × 16 的 S 盒元素与明文图像每像素值进行异或、同或运算，实现图像内容的加密.

解密过程与加密过程类似，执行加密的反操作

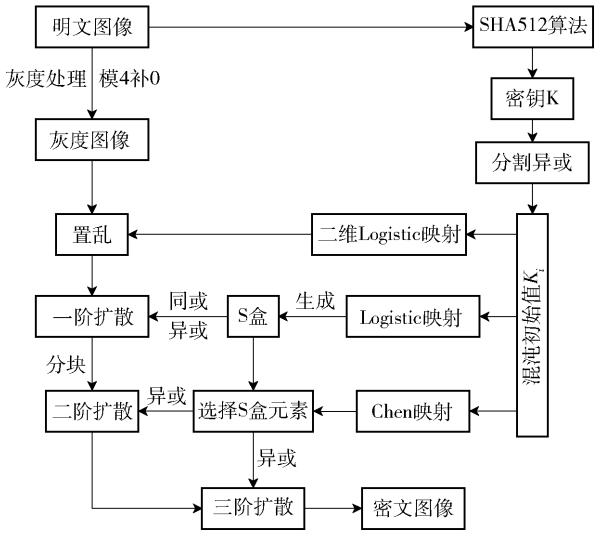


图1 加密算法流程

即可解密图像.

2.1 生成密钥

散列算法能将消息生成定长的摘要,常用于消息认证和数字签名等,选取 SHA512 算法对明文图像 I 生成 128 位的 16 进制安全散列值 K.

2.2 图像分块补零

加密算法的第三阶扩散会通过对 4×4 的块矩阵进行整体异或运算,来提高像素间的混乱度. 将分块大小设为4,按式(4)对原图(M,N)进行补零,直至满足行和列均能被4整除,共分$(M/4)(N/4)$块.

$$\left.\begin{aligned}\mathrm{mod}\ (M,4)=0\\ \mathrm{mod}\ (N,4)=0\end{aligned}\right\} \tag{4}$$

2.3 生成 S 盒

1) 对待每一幅明文灰度图像,根据其散列值生成 Logistic 混沌系统初始值,设混沌系统 $\mu=3.9999$,生成混沌序列 d 并去除前 256 个值.

2) 定义一个空序列 s,再定义一个序列 $Y=[0,1,\cdots,255]$,将$(0,1]$区间划分成 256 个小区间[11],并表示为

$$\left(0,\frac{1}{256}\right],\left(\frac{1}{256},\frac{2}{256}\right],\cdots,\left(\frac{255}{256},1\right]$$

3) 迭代混沌序列 d 得到$(0,1]$间的数值,假如数值在 $\left(\frac{i-1}{256},\frac{i}{256}\right]$,$i\in[1,256]$区间内,并且 $Y[i]$ 不在序列 s 中,那么把 $Y[i]$ 添加至序列 s 的末尾.

4) 如果序列 s 内元素个数小于 256,重复步骤3),直至序列 s 内元素个数等于 256.

5) 把序列 s 变换成 16×16 矩阵,即 S 盒.

2.4 加密过程

将图像 I 转化为 $M\times N$ 的灰度图像,加密包括8个步骤.

1) 对安全散列值 K 每 18 位依次进行异或运算,最后再与其平均值相加求平均,按式(5)产生(0,1)间的初始值,共生成7组初始密码.

$$\boldsymbol{k}_i=\frac{1}{512}\left(\boldsymbol{K}_n\oplus\cdots\oplus\boldsymbol{K}_{n+17}\oplus\frac{1}{18}\times\sum_{n}^{17}\boldsymbol{K}_n\right) \tag{5}$$

其中 $i=1,2,\cdots,7$;$n=0,18,\cdots,108$,同时为7组初始密码按式(6)增加偏置值.

$$\boldsymbol{k}_i=\boldsymbol{k}_i-\frac{K_{126}+K_{127}}{4\times10^{14}} \tag{6}$$

2) 将 k_1 作为 Logistic 混沌系统的初始值,生成 S 盒.

3) 将 k_2,k_3,k_4,k_5 作为 Chen 混沌系统的初始值,生成4个混沌序列 X,Y,Z,H,去除前1 001项,可得更好的随机性. 每个混沌序列的长度为$(M/4)(N/4)$,M,N 为灰度图像 I 的高和宽,分块大小为4,并依据式(7)作相应处理.

$$\left.\begin{aligned}X&=\lfloor X\times10^4\rfloor\bmod 16+1\\ Y&=\lfloor Y\times10^4\rfloor\bmod 16+1\\ Z&=\lfloor Z\times10^4\rfloor\bmod 16+1\\ H&=\lfloor H\times10^4\rfloor\bmod 16+1\end{aligned}\right\} \tag{7}$$

将 k_6,k_7 作为二维 Logistic 混沌系统初始值生成2个混沌序列 C、G,去除前1 001项,并依据式(8)作相应处理,获得 M 行 N 列矩阵,其中 res 表示将序列转化成矩阵.

$$\left.\begin{aligned}C&=\mathrm{res}(C,M,N)\\ G&=\mathrm{res}(G,M,N)\end{aligned}\right\} \tag{8}$$

4) 对灰度图像像素依次进行置乱和一阶扩散处理,对各像素按式(9)、式(10)进行替换扩散,其中 $i=1,2,\cdots,M$,$j=1,2,\cdots,N$,Sbox 表示选择 S 盒内的元素,将 x 值与 255 进行模运算选择 S 盒内的元素与$I(x,y)$像素异或运算后,替换 $I(i,j)$,将 y 值与 255 进行模运算选择 S 盒内元素与原先 $I(i,j)$ 像素同或运算后,替换 $I(x,y)$.

$$\left.\begin{aligned}x&=\lfloor C(i,j)M\rfloor+1\\ y&=\lfloor G(i,j)N\rfloor+1\end{aligned}\right\} \tag{9}$$

$$\left.\begin{aligned}I(i,j)&=\mathrm{Sbox}(\bmod\ (x,256)+1)\oplus I(x,y)\\ I(x,y)&=\mathrm{Sbox}(\bmod\ (y,256)+1)\odot I(i,j)\end{aligned}\right\} \tag{10}$$

5) 为改善序列的随机性能,对混沌序列 X,Y,Z,H 分别进行如下预处理:

$$Q = \mathrm{avg}(X + Y + Z + H) \bmod 24 \tag{11}$$

其中 avg 为取平均值，Q 为选择不同排列组合序列的种子.

对 4 个序列进行排列组合共有 $A_4^4 = 24$ 种，根据 Q 值对每次扩散选择不同排列组合的 4 个序列.

6）将 $[M,N]$ 进行分块，以 4 × 4 块为单位，选择 S 盒内元素与块内元素依次做异或运算，进行二阶扩散，构建 S 盒选择矩阵：

$$\boldsymbol{T} = \begin{bmatrix} X & Y & Z & H \\ X & Y & Z & H \\ X & Y & Z & H \\ X & Y & Z & H \end{bmatrix} \tag{12}$$

再将 $\boldsymbol{T}$ 根据式(13)和式(14)选择 S 盒横列对应元素，与块内 16 个元素逐个进行异或运算.

$$\begin{bmatrix} XX & XY & XZ & XH \\ YX & YY & YZ & YH \\ ZX & ZY & ZZ & ZH \\ HX & HY & HZ & HH \end{bmatrix} \tag{13}$$

$$I(i,j) = \mathrm{Sbox}(T(i,j), T(i,j)) \oplus I(i,j) \tag{14}$$

7）第三阶扩散以块整体为单位，根据式(15)产生随机位，再根据式(16)产生异或值和块整体异或值，有

$$\left.\begin{aligned} a &= (XY) \bmod 256 + 1 \\ b &= (ZH) \bmod 256 + 1 \end{aligned}\right\} \tag{15}$$

$$I(B) = I(B) \oplus \mathrm{mod}\ (\mathrm{Sbox}(a,b), 256) \tag{16}$$

其中 B 为 4 × 4 块矩阵的数量. 将第 6）步中所用的 S 盒元素和块按式(17)进行异或偏置运算：

$$I(B) = I(B) \oplus \sum_{i=1,j=1}^{16} \mathrm{Sbox}(T(i,j), T(i,j)) \tag{17}$$

8）将各块进行整合可得密文图像，解密过程执行加密的反操作即可解密图像.

3　实验仿真与分析

实验选取像素大小为 512 × 512 的 Lena、peppers 两幅图片进行仿真与分析实验，设置 Logistic 混沌系统 $\mu = 3.9999$，二维 Logistic 混沌系统 $\mu_1 = 0.9$，$\mu_2 = 0.9$，$r = 0.1$，以图片的 SHA512 算法散列值为密钥，实验硬件环境为 8 GB 内存，Windows10 操作系统，软件仿真平台为 Matlab 2016b. 为了整体评价加密算法的效果，下面从 S 盒 SAC、直方图、信息熵、相关系数分析、鲁棒性、密钥空间及敏感性、抗差分攻击等方面作安全性能分析.

3.1　SAC

严格雪崩准则即雪崩效应是由 Webster 和 Tavares 在 1985 年提出的，指出任何一个输入位发生反转时，输出中的每一位均有 1/2 的概率变化，这是最理想的情况.

对于严格雪崩准则，每当一个输入位被补充时，一半输出位的平均值应该改变，对不同的 2 个 S 盒 W_1，W_2，其 SAC 值(F)应接近 0.5，有

$$F = \frac{f(\mathrm{bin}(W_1) \oplus \mathrm{bin}(W_2))}{\mathrm{len}(\mathrm{bin}(W_1))} \tag{18}$$

其中 $f(x)$ 为变化个数，$\mathrm{len}(x)$ 为 x 长度.

针对 S 盒生成算法，随机生成多个 S 盒，两两进行 SAC 值测试，测试结果如图 2 所示. 当初始密钥发生变化时，基本满足 50% 的概率发生变化，SAC 值都分布在理想值(见图 2 中的水平线)附近. 通过表 1 的对比结果可见，本算法设计的 S 盒具有良好的性能和强度.

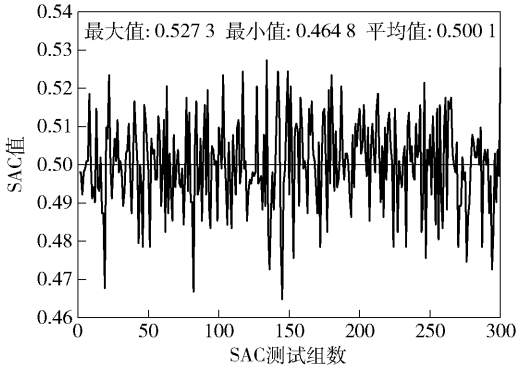


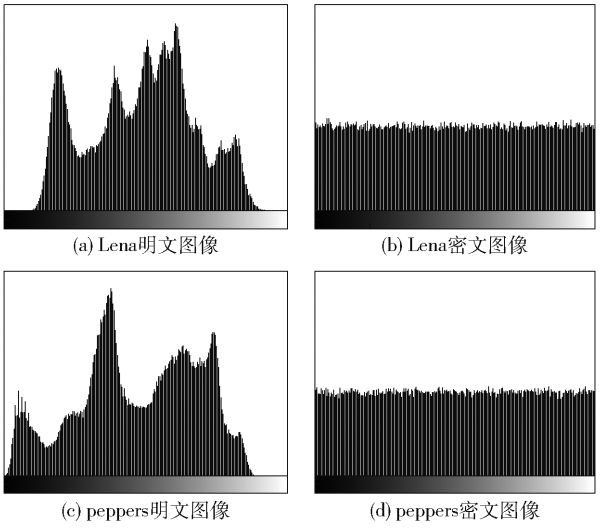
图 2　SAC 测试

表 1　S 盒的 SAC 值对比

算法	平均值	最大值	最小值
所提算法	0.499 6	0.527 3	0.467 8
文献[1]	0.506 3	0.578 1	0.421 8
文献[3]	0.505 6	0.509 0	0.504 0
文献[8]	0.500 5	0.563 0	0.438 0
文献[12]	0.506 6	0.609 4	0.421 9

3.2　图像直方图

一般而言，直方图分布比较均匀，能够有效防止攻击者通过分析直方图来获取明文信息. 图 3(a)～(d)所示为 Lena 和 peppers 图像的明文、密文直方图，可以观察到密文直方图的分布较为均匀. 因此，本加密算法能够有效抵御通过直方图分析进行攻击和遮掩明文图像的统计特性.



(a) Lena明文图像 (b) Lena密文图像

(c) peppers明文图像 (d) peppers密文图像

图3 明文和密文直方图

3.3 信息熵

信息熵主要用于衡量信息源的不确定性或随机性. 反映在图像上,像素灰度值分布越均匀,则熵值越高,随机性越强,也更安全. 对于8位图像,熵值应尽可能接近其理想值8. 信息熵的计算方法为

$$H(R) = -\sum_{i=0}^{255} p(R_i)\mathrm{lb}(p(R_i)) \qquad (19)$$

其中 $p(R_i)$ 为密文图像 R 中像素值 i 出现的频率. 表2所示为全局信息熵的比较.

表2 全局信息熵的比较

算法	Lena	peppers
所提算法	7.999 4	7.999 4
文献[4]	7.997 1	7.999 3
文献[5]	7.999 1	7.999 2
文献[7]	7.997 6	7.997 6

全局信息熵存在不足,偶尔对加密前后的图像测量不准确,因此,在全局信息熵的基础上,Wu等[13]提出了一个更严格的局部信息熵检验方法. 其核心思想是在目标图像中随机选择非重叠子块,表示为 $L_1, L_2, \cdots, L_k$,每个子块包含 W_b 像素;再计算每个子块的全局信息熵,图像的局部信息熵为

$$\overline{H}_{k,W_b} = \sum_{i=1}^{k} \frac{H(L_i)}{k} \qquad (20)$$

选取 $k=30$, $W_b=1\,936$,对灰度图像的局部信息熵进行检验,结果显示,只有当 $\overline{H}_{k,W_b}$ 落在区间(7.901 515 698, 7.903 422 936)上,图像才能通过局部信息熵检验,理想值为7.902 469 317. 通过局部信息熵检验,将所提算法与其他算法的信息熵进行了比较. 从表3所示的结果可见,所提算法局部信息熵检验的通过率相对较高.

表3 “杂项”图像数据集局部信息熵比较

文件名	尺寸	明文信息熵	文献[7]	文献[9]	所提算法
5.1.09	256×256	6.709 3	7.903	7.903 3	7.901 6
5.1.10	256×256	7.311 8	7.902 4	7.902 8	7.903 1
5.1.11	256×256	6.452 3	7.904 8	7.900 1	7.902
5.1.12	256×256	6.705 7	7.890 3	7.902 5	7.902 1
5.1.13	256×256	1.548 3	7.903 2	7.901 3	7.905 1
5.2.08	512×512	7.201	7.903 5	7.902 5	7.902 9
5.2.09	512×512	6.994	7.902 6	7.901 7	7.903 4
5.2.10	512×512	5.705 6	7.902 8	7.904 2	7.903 5
7.1.01	512×512	6.027 4	7.903 3	7.903 2	7.903 1
7.1.02	512×512	4.004 5	7.901 7	7.903 5	7.901 9
7.1.03	512×512	5.495 7	7.904 0	7.901 9	7.903 4
7.1.04	512×512	6.107 4	7.901 9	7.902 8	7.903 8
7.1.05	512×512	6.563 2	7.902 0	7.900 8	7.902 6
7.1.06	512×512	6.695 3	7.902 5	7.901 7	7.902 9
7.1.07	512×512	5.991 6	7.902 0	7.902 3	7.902 1
7.1.08	512×512	5.053 4	7.902 0	7.903 7	7.902
7.1.09	512×512	6.189 8	7.902 0	7.903 0	7.901 8
boat.512	512×512	7.191 4	7.902 7	7.901 5	7.901 6
gray21.512	512×512	4.392 3	7.902 2	7.902 4	7.902 7
ruler.512	512×512	0.500 0	7.902 1	7.902 8	7.903 1
通过率	–	–	16/20	13/20	17/20
平均	–	–	7.902 1	7.9024	7.902 7

3.4 相关系数分析

相邻像素的相关系数能够反映出像素的扩散程度[5],其值越接近于0,图像像素点之间相关性越弱;越接近于1,则像素点之间越相关. 相关系数越低,更能避免攻击者从密文图像中获取有意义的信息.

随机选取 N 对相邻的像素点,将其灰度值记为 (u_i, v_i), $i=1,2,\cdots,N$,则相关系数的计算公式为

$$r_{xy} = \frac{\mathrm{cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}}$$

$$\mathrm{cov}(u,v) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(u))(y_i - E(v))$$

$$D(u) = \frac{1}{N}\sum_{i=1}^{N}(u_i - E(u))^2$$

$$E(u) = \frac{1}{N}\sum_{i=1}^{N} u_i$$

测试图像与密文的相关系数测试结果如表4、表5所示. 可以观察到,明文测试图像相邻像素具

有较强的相关性，而密文图像相邻像素点之间基本不具备相关性.

表 4　Lena 图像相邻像素的相关系数

方向	所提算法		文献[5]	文献[9]	文献[10]
	明文	密文			
水平	0.974 22	−0.000 6	0.001 9	−0.000 3	−0.000 8
垂直	0.985 92	0.002 5	0.009 8	0.010 4	0.013 9
对角	0.962 75	0.000 2	−0.004 9	0.007 7	−0.000 6

表 5　peppers 图像相邻像素的相关系数

方向	所提算法		文献[5]	文献[6]	文献[14]
	明文	密文			
水平	0.977 61	0.000 1	0.001 7	0.002 9	0.019 4
垂直	0.977 42	0.003 6	−0.009 8	−0.000 7	−0.009 1
对角	0.961 26	−0.002 5	0.001 1	0.000 9	0.016 5

图 4 所示为 Lena 明文、密文图像在 3 个方向上的相图. 由图可知，明文图像在每个方向上相邻像素点间的关系呈线性，而密文图像相邻像素点间的关系较为离散，基本不具备相关性，加密效果良好.

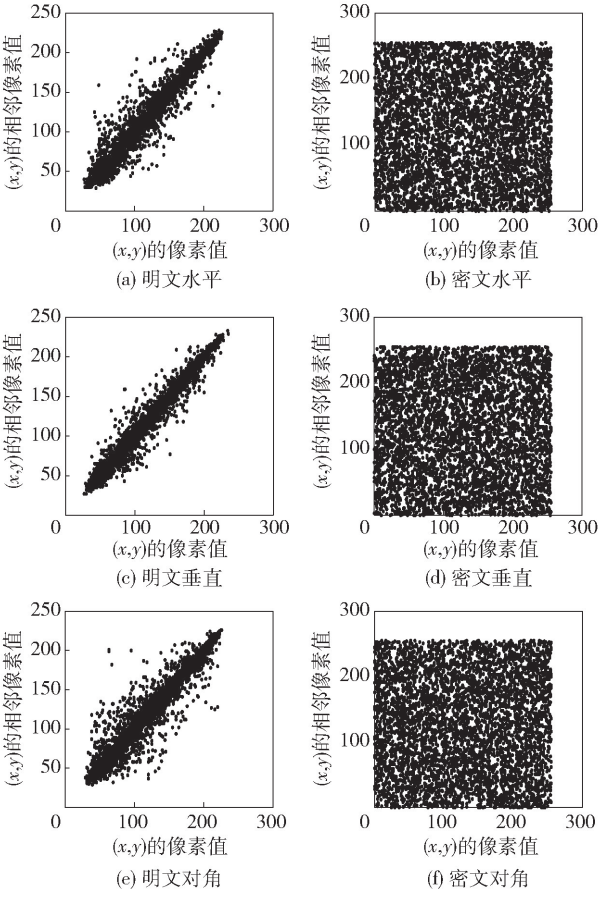


图 4　Lena 明文和密文像素间的相关性

3.5　鲁棒性

随着计算机和密码破解技术水平的提高，攻击者能够通过截获、增添、修改密文图像，来攻击密文图像，对解密造成干扰. 一个良好的加密算法对明文图像进行加密后应当具有较强的鲁棒性，能够抵御种种攻击，成功解密. 对密文图像进行裁剪攻击、噪声攻击、JPEG 压缩后的结果如图 5(a) ~ (c)所示.

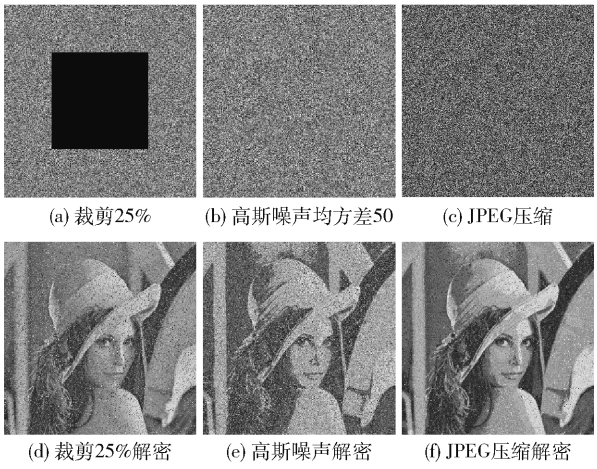


图 5　Lena 鲁棒性检验结果

从图 5(d) ~ (f)可见，即使密文图像有丢失，解密后图像依旧可以恢复且恢复效果良好；当密文图像受到各种噪声攻击时，也能够成功解密，获得一定明文信息；在传输过程中，图像经 JPEG 压缩后也能够很大程度上被解密，从直观视觉角度上，对受到攻击后的密文图像进行解密，仍能分辨出原图的主要信息. 可见，此算法具有较高的鲁棒性.

3.6　密钥空间及敏感性

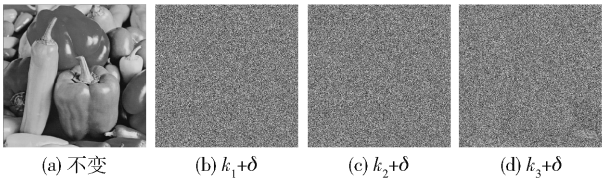
大的密钥空间可以有效抵御密钥穷举爆破. 由文献[5]可知，密钥空间只有大于等于 2^{100}，才能更好地为算法提供可靠安全的保障. 所提算法共使用了 7 组密钥，每组密钥的浮点精度达10^{16}，因此密钥空间为$(10^{16})^7 = 10^{112}$，远远大于 2^{100}，能够抵抗针对密钥的爆破攻击.

对待不同的密钥，即使是微小的变化，最终解密的图像也不应该包含任何有关明文图像的信息，这便要求加密算法对密钥敏感. 对密钥敏感性进行测试的过程中，对 7 组密钥中的某一个密钥作微小改动，$k_i = k_i \pm \delta(\delta = 10^{-16})$，其他密钥不变，与明文图像按均方误差

$$\overline{M} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} |I(i,j) - R(i,j)|^2 \qquad (21)$$

进行对比,R 为待对比的密文图像.

如图6和表6所示,图6(b)~(h)是使用错误密钥解密的图像,通过与图6(a)正确解密的图像对比可以看出,对密钥作微小改动后无法恢复出明文图像,也无法得出与明文相关的信息. 从表6观察到,均方误差值均在8 000以上,与密文图像和明文图像的均方误差值相差无几,熵值也均在7.99以上,接近于8,这证明使用错误密钥解密的图像与明文图像相差很大,说明所提算法具有很高的密钥敏感性.



(a) 不变 (b) $k_1+\delta$ (c) $k_2+\delta$ (d) $k_3+\delta$

(e) $k_4+\delta$ (f) $k_5+\delta$ (g) $k_6+\delta$ (h) $k_7+\delta$

图6 经正确密钥和错误密钥解密的图像

表6 正确密钥和错误密钥解密与明文均方误差

密钥	全局信息熵	均方误差
不变	7.593 7	0(8 428)
$k_1=k_1+\delta$	7.999 3	8 427
$k_2=k_2+\delta$	7.998 9	8 117
$k_3=k_3+\delta$	7.998 8	8 073
$k_4=k_4+\delta$	7.999 0	8 150
$k_5=k_5+\delta$	7.998 9	8 135
$k_6=k_6+\delta$	7.999 1	8 353
$k_7=k_7+\delta$	7.999 0	8 372

3.7 抗差分攻击能力

密文对明文的敏感性越强,越能抵抗差分攻击. 可以用像素数变化率(NPCR, the number of pixels change rate)、归一化平均变化强度(UACI, the unified average changing intensity)指标度量对明文的敏感性. 当2个明文图像仅存在一个不同像素时,加密后得到的密文图像产生了较大变化,密文具有更强的抗差分攻击能力. 设2幅密文图像中第(i,j)点像素为$u_1(i,j)$和$u_2(i,j)$,则NPCR和UACI分别为

$$\left.\begin{aligned}\widetilde{N}&=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)\times 100\%\\ D(i,j)&=\begin{cases}0, & u_1(i,j)=u_2(i,j)\\ 1, & u_1(i,j)\neq u_2(i,j)\end{cases}\end{aligned}\right\} \tag{22}$$

$$\widetilde{U}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|u_1(i,j)-u_2(i,j)|}{255}\times 100\% \tag{23}$$

$\widetilde{N}=99.609\,407\,0$ 和 $\widetilde{U}=33.463\,507\,0$ 是2种指标的期望值,这里选取100组peppers图像进行测试,每组包含原始图像和改变1个比特值的图像. 将测得的2种指标值取平均,明文敏感性测试结果如表7所示. 可见,所提算法所得的NPCR与UACI的均值比其他算法更接近理想值,算法对明文的敏感性更强,可以有效地抵抗差分攻击和选择明文攻击.

表7 明文敏感性测试结果

算法	NPCR	UACI
所提算法	99.610 1	33.465 8
文献[2]	99.565 0	30.913 1
文献[4]	99.599 8	33.460 1
文献[14]	99.618 8	33.482 2

4 结束语

结合S盒和混沌映射的图像加密算法,针对现有混沌系统敏感度低、置乱度低等问题,构建了包含三阶S盒扩散的高维混沌图像加密技术,有效地提升了混沌图像加密算法的敏感性和扩散性. 通过仿真实验从S盒SAC、直方图、信息熵等方面对所提算法进行了性能测试和分析. 结果显示,所提算法拥有良好的加密效果和鲁棒性,且密钥精度很高. 与同类型的算法相比,所提图像加密算法的抗差分能力更强,在加密效果和敏感性处理等方面也有更好的表现.

参考文献:

[1] Çavuşoğlu Ü, Kaçar S, Pehlivan I, et al. Secure image encryption algorithm design using a novel chaos based S-Box[J]. Chaos, Solitons & Fractals, 2017, 95: 92-101.

[2] Aziz H, Gilani S M M, Hussain I, et al. A novel symmetric image cryptosystem resistant to noise perturbation based on S8 elliptic curve S-boxes and chaotic maps[J]. The European Physical Journal Plus, 2020, 135(11):

1-31.

[3] Jamal S S, Attaullah, Shah T, et al. Construction of new substitution boxes using linear fractional transformation and enhanced chaos[J]. Chinese Journal of Physics, 2019, 60: 564-572.

[4] Ye Guodong, Pan Chen, Huang Xiaoling, et al. An efficient pixel-level chaotic image encryption algorithm[J]. Nonlinear Dynamics, 2018, 94(1): 745-756.

[5] 徐扬, 黄迎久, 李海荣. 基于量子 Logistic 映射的图像加密算法研究[J]. 包装工程, 2018, 39(7): 180-186.
Xu Yang, Huang Yingjiu, Li Hairong. Image encryption algorithm based on quantum logistic mapping[J]. Packaging Engineering, 2018, 39(7): 180-186.

[6] 平萍, 李健华, 毛莺池, 等. 混沌映射与比特重组的图像加密[J]. 中国图像图形学报, 2017, 22(10): 1348-1355.
Ping Ping, Li Jianhua, Mao Yingchi, et al. Image encryption algorithm based on chaotic maps and bit reconstruction[J]. Journal of Image and Graphics, 2017, 22(10): 1348-1355.

[7] Talhaoui M Z, Wang Xingyuan. A new fractional one dimensional chaotic map and its application in high-speed image encryption[J]. Information Sciences, 2021, 550: 13-26.

[8] Ullah I, Azam N A, Hayat U. Efficient and secure substitution box and random number generators over Mordell elliptic curves[J]. Journal of Information Security and Applications, 2021, 56: 102619.

[9] Wang Rui, Deng Guoqiang, Duan Xuefeng. An image encryption scheme based on double chaotic cyclic shift and Josephus problem[J]. Journal of Information Security and Applications, 2021, 58: 102699.

[10] Mousavi M, Sadeghiyan B. A new image encryption scheme with Feistel like structure using chaotic S-box and Rubik cube based P-box[J]. Multimedia Tools and Applications, 2021, 80(9): 13157-13177.

[11] 吕群, 薛伟. 结合混沌系统和动态 S-盒的图像加密算法[J]. 小型微型计算机系统, 2018, 39(3): 607-613.
Lü Qun, Xue Wei. Image encryption algorithm combining chaotic system and dynamic S-boxes[J]. Journal of Chinese Computer Systems, 2018, 39(3): 607-613.

[12] Girija R, Singh H. Design of a novel pseudo random generator based on Walsh hadamard transform and Bi S-boxes[J]. Procedia Computer Science, 2018, 132: 795-804.

[13] Wu Yue, Zhou Yicong, Saveriades G, et al. Local Shannon entropy measure with statistical tests for image randomness[J]. Information Sciences, 2013, 222: 323-342.

[14] Wang Xingyuan, Liu Lintao, Zhang Yingqian. A novel chaotic block image encryption algorithm based on dynamic random growth technique[J]. Optics and Lasers in Engineering, 2015, 66: 10-18.