基于混沌系统和双向扩散的图像加密算法

费 敏,李国东
(新疆财经大学 统计与数据科学学院,新疆 乌鲁木齐 830012)

摘 要:针对部分图像加密算法与明文无关,安全性差以及加密效率低的问题,设计一种基于分段线性混沌映射且与明文关联的图像加密算法。首先,将初始值和参数作为密钥,迭代分段线性混沌映射,产生混沌序列;其次,利用产生的混沌序列设计一个混沌密码发生器,产生与明文图像大小相同的 4 个随机矩阵,记作 X、Y、R 和 W,运用 X 矩阵对明文做前向扩散,得到矩阵 A,再运用 R 和 W 矩阵设计一种与明文关联的置乱方法对矩阵 A 进行置乱得到矩阵 B,在置乱的过程中还进行了循环移位操作使加密效果更好;最后运用 Y 矩阵对矩阵 B 做后向扩散,得到呈现噪声样式和不再具有可视信息的最终密文图像。通过实验仿真证明,该加密算法密钥空间大,密钥敏感性强,信息熵接近理论值 8,抗差分攻击和统计攻击能力强,得到的密文图像相邻像素相关性低,安全性高。

关键词:混沌映射;明文关联;双向扩散;图像加密;循环移位
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2021)12-0092-06
doi:10.3969/j.issn.1673-629X.2021.12.016

Image Encryption Algorithm Based on Chaotic System and Bidirectional Diffusion

FEI Min, LI Guo-dong
(School of Statistics and Data Science, Xinjiang University of Finance and Economics, Urumqi 830012, China)

Abstract: Aiming at the problems of some image encryption algorithms which are independent of plaintext, poor security and low encryption efficiency, an image encryption algorithm based on piecewise linear chaotic map and associated with plaintext is designed. Firstly, the initial values and parameters are used as keys to iterate piecewise linear chaotic maps to generate chaotic sequences. Secondly, a chaotic cipher generator is designed by using the generated chaotic sequences to generate four random matrices with the same size as the plaintext image, which are denoted as X, Y, R and W. Then, X is used to do forward diffusion of plaintext to obtain A, and then R and W are used to design a scrambling method associated with plaintext to scramble the A and get the B. In the scrambling process, the cyclic shift operation is also carried out to make the encryption effect better. Finally, Y is used to do backward diffusion of B to obtain the final ciphertext image which presents noise pattern and no longer has visual information. The experimental simulation shows that the proposed encryption algorithm has large key space, strong key sensitivity, information entropy close to the theoretical value of 8, strong ability to resist differential attacks and statistical attacks, and the adjacent pixels of the ciphertext image have low correlation and high security.

Key words: chaotic mapping; plaintext correlation; bidirectional diffusion; image encryption; cyclic shift

0 引 言

目前,混沌研究逐渐取得一些成果,研究人员开始把混沌的研究成果应用到图像研究与应用领域,利用混沌解决一些问题,例如信息安全与图像识别方面,应用比较多的是图像加密领域[1-9]。文献[10]提出的加密方案为后来的很多学者设计加密方案提供了思路,所给出的加密方案解决了部分加密方案所使用到的混沌系统结构单一等问题,并且加密方案依据明文图像信息决定所筛选的像素点个数,利用进行预处理后的伪随机序列对筛选出的明文像素点做运算,从而生成第二级密钥,将其代入分段线性混沌映射按照给出的具体加密方案完成图像加密,通过仿真实验证明加密方案各项安全性指标均非常接近理想值,并且加密效果优良[10]。文献[11]为了提升加密效率,对文献[10]给出的加密方案进行改进,具体改进方法是对彩色图像进行加密,首先将彩色图像转化为 R、G、B 灰度图像,借助 Henon 映射和二维 Logistic 映射生成伪随机序列,并且对得到的伪随机序列进行预处理,利用预

收稿日期:2020-11-17 **修回日期**:2021-03-18
基金项目:国家自然科学基金(11461063);新疆维吾尔自治区自然科学基金项目(2017D01A24);新疆财经大学基金(2019XTD002)
作者简介:费 敏(1995-),女,硕士,研究方向为图像加密;通信作者:李国东(1976-),男,博士,教授,研究方向为混沌保密通讯。

处理后的伪随机序列从明文图像中筛选出一部分像素点,通过分析文献[10]中筛选出的像素点与混沌映射产生的伪随机序列之间的计算规则发现,原有的依次做加法运算再做取模运算的计算规则的计算时间非常长导致整个加密方案加密效率不高,因此对原有计算规则进行改进,运用改进后的筛选出的像素点与混沌映射产生的伪随机序列之间的运算规则得到伪随机序列,将其作为第二级密钥,代入超 Lorenz 混沌系统产生混沌序列,按照"正向扩散-置乱-后向扩散"的顺序完成对彩色图像的加密。通过实验仿真发现运用改进后的方法能够大大节约加密的时间,一定程度上能够提升加密效率,并且加密方案与明文紧密相关联,解决了部分加密方案无法抵御明文攻击的问题[11]。文献[12]采用随机分块、块内块间同步置乱扩散及环形扩散等操作,通过实验仿真发现所设计的加密方案能够大大提高图像加密效率[12]。基于上述加密方案,设计一种"扩散-置乱-扩散"结构的图像加密算法。

1　分段线性混沌映射

分段线性混沌映射表达式为:

$$x_i = f(x_{i-1},p) = \begin{cases} \dfrac{x_{i-1}}{p}, 0 < x_{i-1} < p \\ \dfrac{x_{i-1}-p}{0.5-p}, p \leqslant x_{i-1} < 0.5 \\ f(1-x_{i-1},p), 0.5 \leqslant x_{i-1} < 1 \end{cases} \tag{1}$$

其中,p 表示分段线性混沌映射的参数,$0 < p < 0.5$;x 表示分段线性混沌映射的状态变量,$0 < x < 1$。加密方案迭代两次分段线性混沌映射,其中一个的初始值和参数记为 x_0 和 p,另一个的初始值和参数记为 y_0 和 q,$\{x_0,p,y_0,q\}$ 属于密钥的一部分。

2　算法设计

设 P 表示明文图像,大小为 $M \times N$。密钥用 K 表示,具体为 $K=\{x_0,p,y_0,q,r_1,r_2,r_3,r_4\}$,其中 x_0 与 p 和 y_0 与 q 表示两个分段线性混沌映射的初始值与参数,r_1,r_2,r_3 和 r_4 表示 4 个 8 位的随机整数,取值区间为[0,255]。具体加密流程如图 1 所示。

2.1　混沌密码发生器

给出的式(2)~式(5)称为混沌密码发生器,借助分段线性混沌映射所生成的伪随机序列,并且利用式(2)~式(5)给出的具体运算规则进行运算能够得到四个跟明文图像大小完全一致即无任何差异的随机矩阵,将这四个随机矩阵记为 $\boldsymbol{X},\boldsymbol{Y},\boldsymbol{R},\boldsymbol{W}$,四个矩阵大小全部是 $M \times N$,具体的运算规则由式(2)~式(5)展示[13]。

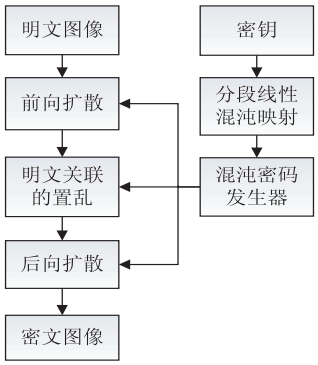


图 1　加密算法流程

Step1:将 x_0 和 p,y_0 和 q 分别作为分段线性混沌系统也就是表达式(1)的初始值以及参数,为了避免暂态效应,舍去迭代分段线性混沌映射 r_1+r_2 次,再继续迭代分段线性混沌映射 $M \times N$ 次,生成长度为 $M \times N$ 的状态变量序列,记为 $\{x_i\}, i=1,2,\cdots,MN$,$\{y_i\}, i=1,2,\cdots,MN$。

Step2:由向量 $\{x_i\}$ 和 $\{y_i\}$,按式(2)~式(5)得到矩阵 $\boldsymbol{X},\boldsymbol{Y},\boldsymbol{R}$ 和 $\boldsymbol{W}$。

$$X(u,v) = \mathrm{mod}\left(\mathrm{floor}\left(\left(\frac{r_1+1}{r_1+r_3+2}x_{(u-1)\times N+v} + \frac{r_3+1}{r_1+r_3+2}y_{(u-1)\times N+v}\right)\times 10^{14}\right),256\right) \tag{2}$$

$$Y(u,v) = \mathrm{mod}\left(\mathrm{floor}\left(\left(\frac{r_2+1}{r_2+r_4+2}x_{(u-1)\times N+v} + \frac{r_4+1}{r_2+r_4+2}y_{(u-1)\times N+v}\right)\times 10^{13}\right),256\right) \tag{3}$$

$$R(u,v) = \mathrm{mod}\left(\mathrm{floor}\left(\left(\frac{r_1+1}{r_1+r_4+2}x_{(u-1)\times N+v} + \frac{r_4+1}{r_1+r_4+2}y_{(u-1)\times N+v}\right)\times 10^{12}\right),M\right) \tag{4}$$

$$W(u,v) = \mathrm{mod}\left(\mathrm{floor}\left(\left(\frac{r_2+1}{r_2+r_3+2}x_{(u-1)\times N+v} + \frac{r_3+1}{r_2+r_3+2}y_{(u-1)\times N+v}\right)\times 10^{11}\right),N\right) \tag{5}$$

其中,$\mathrm{floor}(t)$ 表示返回小于或者等于数 t 的最大整数,$u=1,2,\cdots,M$,$v=1,2,\cdots,N$。利用生成的 $\boldsymbol{X}$ 矩阵完成前向扩散操作,$\boldsymbol{Y}$ 矩阵完成后向扩散操作,$\boldsymbol{R}$ 和 $\boldsymbol{W}$ 矩阵完成置乱操作。

2.2　前向扩散算法

Step1:借助混沌密码发生器得到的 $\boldsymbol{X}$ 矩阵以及 r_3,r_4,根据式(6)和式(7)给出的具体计算规则对明文图像第一行的所有像素值进行变换,即将 $P(1,j)$ 转化为 $A(1,j)$。

$$A(1,1) = \mathrm{mod}(P(1,1) + X(1,1) + r_3 + r_4, 256) \tag{6}$$

$$A(1,j) = \mathrm{mod}(P(1,j) + X(1,j) + A(1,j-1), 256), j = 2,3,\cdots,N \tag{7}$$

Step2:借助混沌密码发生器得到的 $\boldsymbol{X}$ 矩阵,根据式(8)给出的具体计算规则将明文图像第一列的像素值进行变换,即将 $P(i,1)$ 转化为 $A(i,1)$。

$$A(i,1) = \mathrm{mod}(P(i,1) + X(i,1) + A(i-1,1), 256), i = 2,3,\cdots,M \tag{8}$$

Step3:借助混沌密码发生器得到的 $\boldsymbol{X}$ 矩阵,根据式(9)给出的具体运算规则对明文图像除了第一行以及第一列剩余的所有像素值进行变换,即将 $P(i,j)$ 转化为 $A(i,j)$。

$$A(i,j) = \mathrm{mod}(P(i,j) + A(i-1,j) + A(i,j-1) + X(i,j), 256), i = 2,3,\cdots,M, j = 2,3,\cdots,N \tag{9}$$

经过上述前向扩散操作后,得到初始密文图像,将其记为矩阵 $\boldsymbol{A}$。

2.3 明文关联的置乱算法

Step1:计算 $A(i,j)$ 所在行和列的全部元素(不含 $A(i,j)$)的和,记为 row_i,col_i。

$$\mathrm{row}_i = \mathrm{sum}(A(i,1 \text{ to } N)) - A(i,j) \tag{10}$$

$$\mathrm{col}_i = \mathrm{sum}(A(1 \text{ to } M,j)) - A(i,j) \tag{11}$$

Step2:利用式(12)和式(13)计算坐标 (m,n) 的值,即:

$$m = \mathrm{row}_i + R(i,j) \bmod M \tag{12}$$

$$n = \mathrm{col}_i + W(i,j) \bmod N \tag{13}$$

Step3:如果 $m = i$ 或 $n = j$,则 $A(i,j)$ 与 $A(m,n)$ 的位置保持不变,否则 $A(i,j)$ 与 $A(m,n)$ 互换位置,同时根据 $A(m,n)$ 的低 3 位的值,将 $A(i,j)$ 进行循环移位,即:

$$A(i,j) = A(i,j) <<< (A(m,n) \& 0 \times 7) \tag{14}$$

其中,"$x <<< y$"表示 x 循环左移 y 位。

Step4:按 Step1 ~ Step3 的方法,先置乱矩阵 $\boldsymbol{A}$ 的第 M 行,然后再置乱矩阵 $\boldsymbol{A}$ 的第 N 列,接着按从左向右再从上而下的扫描顺序依次置乱矩阵 $\boldsymbol{A}$ 的元素 $A(1 \text{ to } M-1, 1 \text{ to } N-1)$,最后置乱矩阵 $\boldsymbol{A}$ 的元素 $A(M,N)$。

完成以上具体置乱步骤后,得到置乱后的中间密文图像,将其记为矩阵 $\boldsymbol{B}$。

2.4 后向扩散算法

Step1:借助混沌密码发生器生成的 $\boldsymbol{Y}$ 矩阵,运用式(15)以及式(16)给出的具体运算规则对置乱得到的中间密文图像的第 M 行的所有像素值进行变换,即将 $B(M,j)$ 转化为 $C(M,j)$。

$$C(M,N) = \mathrm{mod}((B(M,N) + Y(M,N) + r_1 + r_2), 256) \tag{15}$$

$$C(M,j) = \mathrm{mod}((B(M,j) + Y(M,j) + C(M,j+1)), 256), j = N-1, N-2, \cdots, 1 \tag{16}$$

Step2:借助混沌密码发生器生成的 $\boldsymbol{Y}$ 矩阵,运用式(17)给出的具体运算规则对置乱得到的中间密文图像的第 N 列的所有像素值进行变换,即将 $B(i,N)$ 转化为 $C(i,N)$。

$$C(i,N) = \mathrm{mod}((B(i,N) + Y(i,N) + C(i+1,N)), 256), i = M-1, M-2, \cdots, 1 \tag{17}$$

Step3:借助混沌密码发生器生成的 $\boldsymbol{Y}$ 矩阵,运用式(18)给出的具体运算规则对置乱得到的中间密文图像除去第 M 行以及第 N 列的剩余像素值进行变换,即将 $B(i,j)$ 转化为 $C(i,j)$。

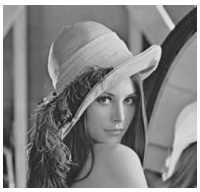
$$C(i,j) = \mathrm{mod}((B(i,j) + C(i+1,j) + C(i,j+1) + Y(i,j)), 256), i = M-1, \cdots, 1, j = N-1, \cdots, 1 \tag{18}$$

经过上述后向扩散操作后得到矩阵 $\boldsymbol{C}$,将其记为最终密文图像。

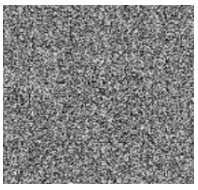
Step4:倘若要对密文图像进行解密得到明文图像,就需要完成上述加密过程的逆过程[14]。

3 实验仿真

实验仿真在 Matlab R2018a 的环境下进行,选择大小为 256 × 256 的 Lena 图像进行加密仿真实验,其中密钥的具体初始值为 $\{x_0 = 0.7896, p = 0.5487, y_0 = 0.3535, q = 0.6677, r_1 = 69, r_2 = 138, r_3 = 91, r_4 = 105\}$。解密还原得到的明文图像及密文图像如图 2 所示。



(a)还原后的 Lena 图像



(b)Lena 密文图像

图 2 加密与解密实验结果

4 安全性分析

4.1 密钥空间

好的加密算法应该具备密钥空间大的特性[15],加密算法的初始密钥有 8 个,分别是:$x_0, p, y_0, q, r_1, r_2, r_3, r_4$。其中,$x_0, y_0 \in (0,1)$ 是浮点数,精度达到了 10^{-14},$p, q \in (0,0.5)$,也是浮点数,其精度也达到了 10^{-14},$r_1 \sim r_4$ 为[0,255]中的整数,步进为 1,因此,通过计算能够得到密钥空间的具体数值约等于 $1.0737 \times$

10^{65},说明设计的加密方案具备抵御穷举攻击的能力。

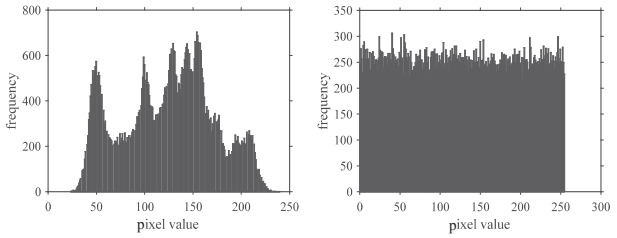
4.2　直方图分析

衡量一个加密方案是否具备抵御基于统计特性的攻击的能力必须要考虑明文图像以及经过加密方案加密得到的密文图像的直方图[16]。直方图能够刻画出某个图像里各灰度值的分布状态。以大小为 256 × 256 像素的 Lena 、girl 、全黑、全白图像为例,密文图像的直方图χ^2 检验结果见表 1。

表 1　χ^2 检验结果

项目	Lena	girl	全黑	全白
明文	4.114 7e4	5.298 1e4	1.671 1e7	1.671 1e7
密文	240.046 9	250.695 3	292.742 2	268.718 8

根据表 1 中的数据可知,密文图像的χ^2 统计量的计算值小于$\chi^2_{0.05}(255)$,故可认为密文图像近似均匀分布。由图 3 可知,明文图像的直方图均具有明显的波伏特性,但是密文图像直方图趋近于均匀分布。



(a)Lena 明文　　(b)Lena 密文

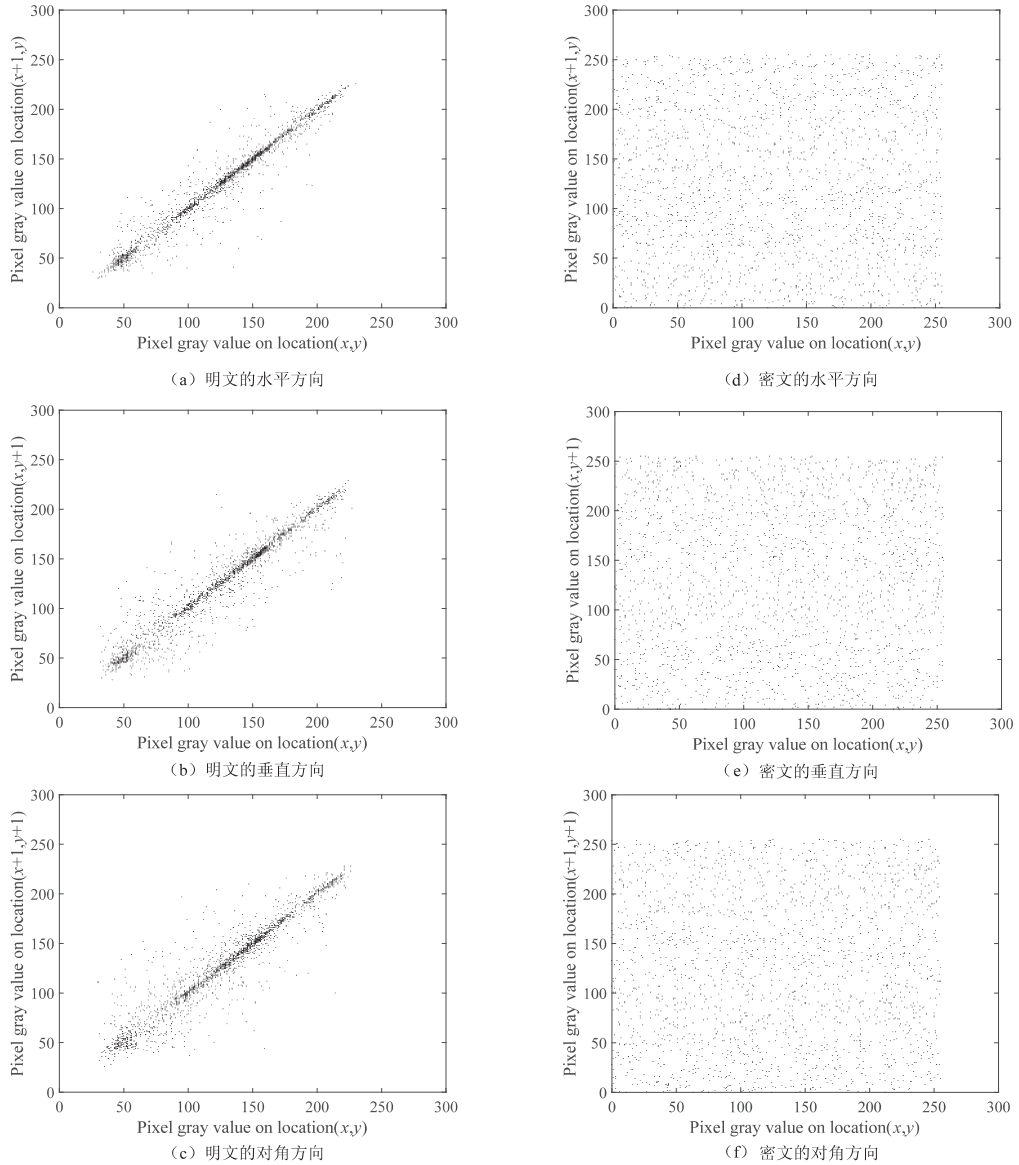
图 3　Lena 图像直方图及其密文图像直方图

4.3　相邻像素相关性分析

相关系数计算公式如下:

$$r_{xy}=\frac{\operatorname{cov}(u,v)}{\sqrt{D(u)}\ \sqrt{D(v)}} \tag{19}$$

从 Lena 明文以及密文图像中随机筛选出 2 000 对水平、垂直以及对角线方向上的相邻像素点,对筛选出的相邻像素点之间的相关系数进行计算,并且对筛选出的相邻像素点之间的关联情况图绘制出来,得到的具体结果由表 2 及图 4 展示。



(a) 明文的水平方向　　(d) 密文的水平方向

(b) 明文的垂直方向　　(e) 密文的垂直方向

(c) 明文的对角方向　　(f) 密文的对角方向

图 4　Lena 明文和密文图像在各方向的相邻像素分布

表 2 明/密文图像相邻像素相关性系数

图像	水平	垂直	正对角	反对角
明文	0.978 3	0.946 0	0.922 4	0.942 6
密文	0.002 4	0.014 6	0.022 6	0.003 6

根据表 2 中的具体数值,能够看出 Lena 明文图像在水平、垂直、正对角线以及反对角线这四个方向上相互邻近像素点的相关系数全部在 1 附近,但是经过所设计的加密方案加密得到的 Lena 密文图像在水平、垂直、正对角线以及反对角线这四个方向上相互邻近像素点的相关系数全部在 0 附近,也就是说经过所设计的加密方案加密得到的 Lena 密文图像相互邻近的像素点不存在明显的相关性。依据图 4 所展示的结果,能够看出明文图像在水平、垂直以及对角线方向上的相邻像素点对全部分布在直线 $y = x$ 周围,但是经过加密方案加密获得的 Lena 密文图像在这三个方向上的相邻像素点对全部呈现均匀分布的状态,因此,通过分析以上实验结果能够反映出所设计的加密方案具备有效隐藏 Lena 明文图像像素统计信息的能力。

4.4 信息熵

信息熵反映的是图像中灰度分布情况[17]。p_i 表示图像灰度 i 出现的概率,具体的计算公式为:

$$H(x) = -\sum_{i=1}^{n} p_i \log_2 p_i \tag{20}$$

表 3 信息熵、相对熵和冗余度

项目	明文	密文	全黑	全白
信息熵	7.431 8	7.997 4	7.999 0	7.999 0
相对熵	0.929 0	0.999 7	0.999 9	0.999 9
冗余度	0.071 0	0.000 3	0.000 1	0.000 1

由表 3 可知,明文图像的冗余度在 5% 以上,密文图像的冗余度小于 0.05%,密文的信息熵接近于理想值 8,说明所设计的加密方案可以对抗基于信息熵的分析。

4.5 密钥敏感性分析

当对密钥做极其不明显的改变时,分析运用所设计的加密方案加密完全一致的明文图像生成的两个密文图像间所存在的差异情况。对 Lena 图像运用所设计的加密以及解密方案进行加解密,对原始密钥 x_0 改变 10^{-16},借助改变前后的密钥以及所设计的加密方案加密相同的明文图像生成的两幅密文图像结果如图 5 所示。根据图 5 得到的两幅密文图像能够看出,对初始密钥的值做极其不明显的改变,对完全一致的明文图像加密生成的两个密文图像的差图像表现为噪声样式,也就是说所设计的加密方案具备强的密钥敏感性。并且通过得到的实验结果能够发现当密钥发生仅 10^{-16} 极其不明显的变化时,也不能够获得正确解密图像。所以,从这一点也能够说明所设计的加密方案具备强的密钥敏感性。

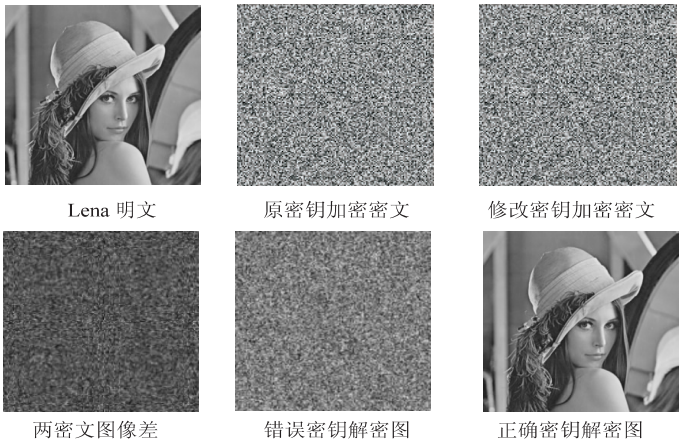


图 5 Lena 图像密钥敏感性实验结果

4.6 差分攻击分析

衡量抵御差分攻击的能力的重要指标是 NPCR(像素变化率)、UACI(归一化像素平均值)、BACI,计算方式如下:

$$\mathrm{NPCR} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} |\mathrm{Sign}(P_1(i,j) - P_2(i,j))| \times 100\% \tag{21}$$

$$\mathrm{UACI}(P_1,P_2)=\frac{1}{MN}\sum_{i}^{M}\sum_{j}^{N}\frac{|P_1(i,j)-P_2(i,j)|}{255-0}\times 100\% \quad (22)$$

$$\mathrm{BACI}(P_1,P_2)=\frac{1}{(M-1)(N-1)}\sum_{i=1}^{(M-1)(N-1)}\frac{m_i}{255} \quad (23)$$

表 4　明文敏感性分析结果

指标	Lena	Girl	全黑	全白
NPCR	99.609 9	99.619 1	99.605 4	99.608 7
UACI	33.482 5	33.461 7	33.460 8	33.467 2
BACI	26.774 7	26.765 4	26.763 8	26.768 3

P_1 指密文图像，P_2 指明文图像中某一像素值产生极其不明显的变动时所对应的密文图像。随机筛选明文图像中的一点坐标,将其进行微小变动,重复 100 次实验计算两密文间的 NPCR、UACI 和 BACI 的平均值,结果列于表 4 中。由表 4 可知,计算结果极其接近于理论值,说明加密算法具有很强的抗差分攻击能力。

5　结束语

提出一种基于分段线性混沌系统的正向扩散以及逆向扩散相结合的图像加密方案,并且通过实验仿真分析所设计的加密算法各项安全性指标是否达到理想值即安全性能是否良好。采用“前向扩散-置乱-后向扩散”的结构来加密图像,对于所设计的加密算法而言,即使采用相同的密钥,不同的明文图像将对应不同的等价密钥和加密算法,从而得到完全不同的密文图像。依据实验仿真得到的各项安全性能指标的具体结果,能够看出所设计的加密算法具备足够大的密钥空间,拥有非常良好的密钥敏感性,并且抗统计和差分攻击能力强,是一种非常优秀的图像加密算法。

参考文献:

[1] MAY R M. Simple mathematical models with very complicated dynamics[J]. Nature,1976,261(5560):459-467.

[2] DEVANEY R L. An introduction to chaotic dynamical systems[M]. New York:West View Press,1989.

[3] ZHANG Yong. Plaintext related image encryption scheme using chaotic map[J]. Telkomnika Indonesian Journal of Electrical Engineering,2014,12(1):635-643.

[4] 张　勇. 混沌数字图像加密[M]. 北京:清华大学出版社,2016.

[5] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal,1949,28(4):656-715.

[6] 于万波. 混沌的计算分析与探索[M]. 北京:清华大学出版社,2016:2-5.

[7] 田军锋,彭静静,左宪禹,等. 基于循环移位和多混沌映射的图像加密算法[J]. 计算机科学,2020,47(10):327-331.

[8] 刘西林,严广乐. 基于明文相关的混沌映射与 SHA-256 算法数字图像的加密与监测[J]. 计算机应用研究,2019,36(11):3401-3403.

[9] 王　瑶,韩亚军. 基于双向相关扩散与非线性混沌 S 盒的图像加密算法[J]. 包装工程,2019,40(15):243-251.

[10] ZHANG Yong. Two-level secret key image encryption method based on piecewise linear map and logistic map[J]. Applied Mechanics & Materials,2013,241-244:2728-2731.

[11] 谢国波,高兆曦. 明文关联的多混沌彩色图像加密算法[J]. 计算机工程与设计,2019,40(4):920-930.

[12] 梁　颖,张绍武. 位级同步置乱扩散和像素级环形扩散图像加密算法[J]. 中国图象图形学报,2018,23(6):814-826.

[13] 魏　慧,李国东. 基于细胞神经网络超混沌特性的图像加密算法[J]. 微电子学与计算机,2020,37(5):43-48.

[14] 曾　珂,禹思敏,胡迎春,等. 基于 3D-LSCM 的图像混沌加密算法[J]. 电子技术应用,2020,46(1):86-91.

[15] 张修引,曾齐红,邵燕林,等. 二维超混沌系统的研究及在图像加密中的应用[J]. 计算机技术与发展,2020,30(5):103-108.

[16] 李珊珊,周怡彤,张红丽,等. 基于离散余弦变换的图像加密效果评估方法[J]. 计算机技术与发展,2020,30(5):99-102.

[17] 袁岁维,范九伦. 基于二维分段线性映射的图像加密方法[J]. 微电子学与计算机,2010,27(6):181-184.