

一种基于延迟反馈 Logistic 映射的彩色图像加密算法

谭冬文, 李彩虹, 李守亮, 李 廉
(兰州大学 信息学院, 甘肃 兰州 730000)

摘 要: 为克服 Logistic 映射存在的缺陷, 基于延迟反馈设计了一种改进的 Logistic 混沌映射. 基于该混沌映射, 提出了一种新的密钥与明文相关的图像加密算法. 仿真结果表明, 提出的图像加密算法只需进行一轮置乱扩散操作即可获得较好的加密效果, 可有效抵御统计分析攻击、差分攻击和选择明文攻击, 同时展现出较强的鲁棒性.

关键词: 图像加密; Logistic 映射; 时间延迟; 置换扩散; 抗攻击

中图分类号: TP309.7

文献标识码: A

文章编号: 1000—7180(2017)10—0047—06

A Color Image Encryption Algorithm Based on Delayed Feedback Logistic Mapping

TAN Dong-wen, LI Cai-hong, LI Shou-liang, LI Lian

(College of Information, Lanzhou University, Lanzhou 730000, China)

Abstract: To overcome the shortcomings of Logistic map, an improved Logistic chaotic map is designed via delayed feedback. Based on the proposed chaotic map, a new image encryption algorithm relative to plain text is proposed. The simulation results show that the encryption algorithm proposed in this paper only needs a round of permutation and diffusion operation to achieve satisfactory encryption effect, and can effectively resist statistical analysis attack, differential attack and selective plain text attack, and exhibits strong robustness.

Key words: image encryption; logistic map; time delay; permutation and diffusion; anti attack

1 引言

图像加密技术作为保障图像信息在互联网上安全传输的手段之一, 正受到广泛关注^[1]. 图像自身的特点如信息量大和相关性强等决定了传统的文本加密方法已不完全适用图像加密领域. 考虑到混沌的典型特征如初值敏感性、遍历性和伪随机性等^[2]与加密系统的要求相符, 英国数学家 Matthews^[3]首次将混沌理论引入到图像加密中. 随后, Fridrich^[4]提出了置乱扩散混沌加密结构. 自此, 混沌图像加密领域成为科研工作人员的研究热点, 涌现了大量的相关研究成果^[5-8]. Ruishan Du 和 Yang Li^[9]利用超混沌系统产生混沌序列, 使用异或操作对信息进行加密, 获得了较好的加密效果, 但是由于超混沌系统的

计算复杂度高, 该方案存在实时性不高的缺点^[10]. 文献[11]提出了级联映射模型, 可以使用 Logistic 映射、帐篷映射、正弦映射等混沌映射组合成一个新的混沌映射模型, 利用该混沌模型产生混沌序列对图像进行加密, 可是并没有考虑到时间延迟因素. 文献[12], 使用 chen 混沌系统对转换为二维灰度图像的彩色图像进行行与列的置换, 加密效果较好, 但使用三维 chen 系统产生混沌序列时出现计算量较大的问题.

本文中, 提出了一个将 Logistic 混沌映射模型和延迟反馈结合在一起的新模型-延迟反馈 Logistic 映射. 本文提出的延迟反馈 Logistic 混沌映射较传统的 Logistic 映射具有更大的混沌区间, 具有较快的加密速度; 同时该加密算法能够有效抵抗统计分

析攻击、差分攻击和选择明文攻击,并在抗裁剪攻击和对抗噪声攻击方面也显示了较强的鲁棒性.

2 延迟反馈 Logistic 混沌映射

Logistic 映射是一个非常经典且应用广泛的一维离散非线性动力系统,因其具有较好的混沌特性,较低的计算量,能够产生混沌序列,被广泛应用于信息加密中. 数学上,Logistic 映射被定义为^[13]:

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

式中,控制参数 $\mu \in [0, 4]$.

图 1 为 Logistic 映射的分岔图. 从图中可以看出,Logistic 映射展现混沌的参数区间偏窄,并在混沌区间内存在多个周期窗口现象.

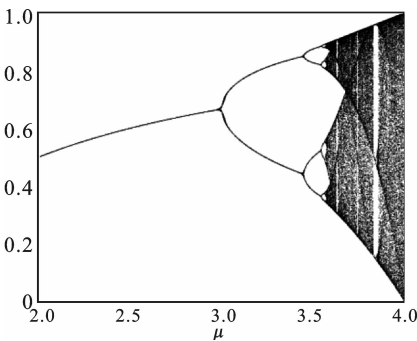


图 1 Logistic 映射的分岔图

为克服传统 Logistic 映射的缺陷,提高加密系统的安全性,本文设计了一种基于延迟反馈的 Logistic 混沌映射,图 2 为延迟反馈模型的结构图. 延迟反馈 Logistic 映射可被定义为:

$$x_{n+1} = \text{mod}(F(x_n + \epsilon x_{n-\tau}), 1) \tag{2}$$

式中, ϵ 为反馈增益, 范围为 $[-1, 1]$, $F(\cdot)$ 为一维 Logistic 映射, $\text{mod}(x, y)$ 为取余运算, 在本文中时间延迟因子 $\tau = 1$.

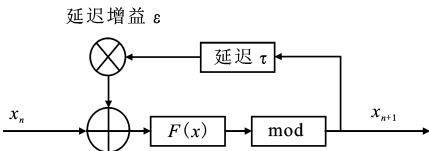


图 2 延迟反馈 Logistic 映射结构

图 3 展示了延迟反馈 Logistic 混沌映射随反馈增益 ϵ 变化的分岔图.

从图 3 可以看出,当反馈增益 $\epsilon=0$ 时,延迟反馈 Logistic 混沌映射分岔图跟 Logistic 混沌映射是一样的. 随着反馈增益 ϵ 的增大,其产生混沌序列参数区间范围增大,周期窗口消失,从而形成一个较大的混沌区间. 随着 μ 参数的增大,动力学行为更加复

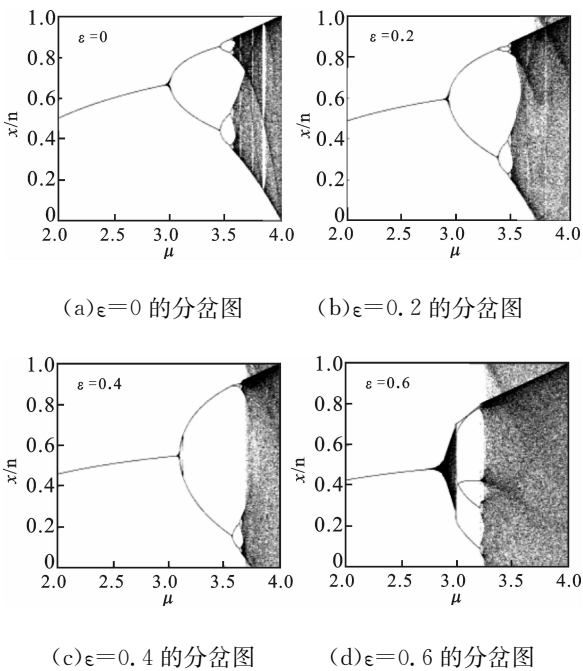


图 3 延迟反馈 Logistic 映射的分岔图

杂,非线性效果更好. 相比传统的 Logistic 混沌映射,其具有更好的混沌映射行为,更宽的混沌参数范围.

3 图像加密方案

本文加密算法采用经典的置乱扩散结构,图像置乱即打乱图像中每个像素的位置,扩散是改变每个像素的值. 本文提出的加密算法流程图如图 4 所示.

基于时延反馈 Logistic 映射的彩色图像加密方案详细步骤如下:

- (1) 输入原始彩色图像 P ;
- (2) 图像预处理,将彩色图像 P 进行 R, G, B 分离得到 $R_{M \times N}, G_{M \times N}, B_{M \times N}$, 依据式(3) 将其合并得到一幅新图像 $P'_{M \times 3N}$. 表达式定义如下:

$$\begin{cases} P'(:, j) = R'(:, j) & \text{if } \text{mod}(j, 3) = 1 \\ P'(:, j) = G'(:, j) & \text{if } \text{mod}(j, 3) = 2 \\ P'(:, j) = B'(:, j) & \text{if } \text{mod}(j, 3) = 0 \end{cases} \tag{3}$$

(3) 依据图像 $P'_{M \times 3N}$ 信息获取初始值,产生用于置换的混沌序列. 将图像 $P'_{M \times 3N}$ 像素值进行相加取平均值并依据确定的变换公式将其映射到 $(0, 1)$ 范围内得到第一个初始值,将图像 $P'_{M \times 3N}$ 的像素值与其所有像素的平均值相减,计算其方差后再依据确定的变换公式将该方差映射到 $(0, 1)$ 范围内得到第二个初始值. 其函数表达式如下:

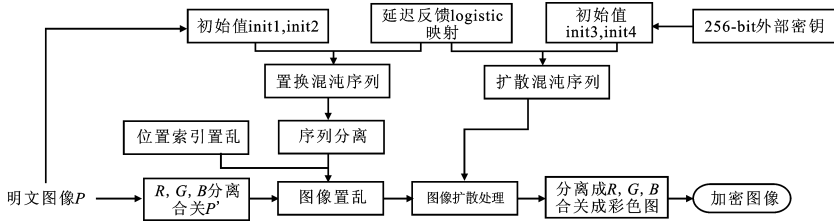


图4 加密算法流程框架图

$$\begin{cases} \text{init1} = \frac{\sum_{i=1}^M \sum_{j=1}^N P'(i, j)}{M * N} \bmod 1 \\ \text{init2} = \frac{\sum_{i=1}^M \sum_{j=1}^N (P'(i, j) - \bar{x})^2}{M * N} \bmod 1 \end{cases} \quad (4)$$

在式(4)中, M 表示输入图像的行数, N 表示输入图像的列数, $\bar{x}$ 为所有像素的平均值. 将式(4)得到的初始值代入式(2)进行迭代运算产生长度 $L = M + 3N$ 的序列 S ;

(4) 给定一个 256 位外部二进制密钥 K , 以 8 位为一个单元对其进行块划分即可得到

$$K = k_1, k_2, k_3, k_4, \dots, k_{32}$$

依据式(5)产生混沌序列的两个初始值, 代入式(2)中迭代生成用于扩散的序列 S' ;

$$\begin{cases} \text{init3} = (k_1 \oplus k_2 \oplus k_3 \oplus \dots \oplus k_{16}) / 255 \\ \text{init4} = (k_{17} \oplus k_{18} \oplus k_{19} \oplus \dots \oplus k_{32}) / 255 \end{cases} \quad (5)$$

(5) 将序列 S 用于置乱操作. 首先, 将该序列依据式(6)分为两个子序列 S_1, S_2 , 然后使用 S_1, S_2 分别用于置换图像 P' 的行与列,

$$\begin{cases} S_1(i) = S(j) & \text{if } j \leq M \\ S_2(i) = S(j) & \text{if } M < j \leq 3N \end{cases} \quad (6)$$

将式(6)得到的两个子序列 S_1, S_2 从小到大分别排序, 依据排序后的 S_1 子序列的下标数组 ind_1 对图像 P' 进行行置换, 然后依据排序后的 S_2 下标数组 ind_2 再进行列置换得到新图像 $P''_{M \times 3N}$;

(6) 将用式(5)产生的初值得到的序列 S' 变换成 $S'_{M \times 3N}$, 依据式(7)对置换后的新图像 $P''_{M \times 3N}$ 进行扩散处理.

在式(7)中, $\text{floor}(x)$ 表示不大于 x 的最大整数, $\oplus$ 表示两数按其二进制值进行比特位异或运算, P'' 为扩散处理后的加密图像;

(7) 将图像 P'' 使用与步骤(2)相同的规则进行分离得到三幅灰度图像 $R'_{M \times N}, G'_{M \times N}, B'_{M \times N}$, 然后将这三幅灰度图像进行合并得到一幅加密后的彩色

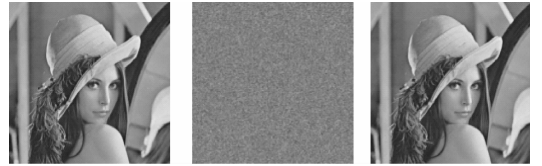
图像 $\overline{P_{M \times N}}$.

$$\begin{cases} P''(i, j) = \\ P''(i, j) \oplus \text{floor}(S'(i, j) * 256) & \text{if } i = 1, j = 1 \\ P''(i, j) = P''(i, j) \oplus P''(i, j-1) \oplus \\ \text{floor}(S'(i, j) * 256) & \text{if } i = 1, 1 < j \leq 3 * N \\ P''(i, j) = P''(i, j) \oplus P''(i-1, j) \\ \oplus \text{floor}(S'(i, j) * 256) & \text{if } i = M, j = 1 \\ P''(i, j) = P''(i, j) \oplus P''(i-1, j) \oplus P''(i, j-1) \\ \oplus \text{floor}(S'(i, j) * 256) & \text{if } 1 < i \leq M, 1 < j \leq 3 * N \end{cases} \quad (7)$$

解密过程是上述图像加密的逆过程.

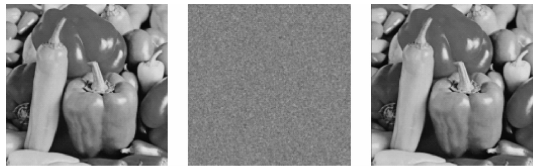
4 实验结果仿真与性能分析

本文选取 USC-SIP 库中 $512 * 512$ 的彩色图像对提出的图像加密算法进行仿真测试. 设置式(1)的系统参数 $\mu = 3.57, \epsilon = 0.6$. 对原始图像进行 1 轮的加密, 图 5, 图 6 分别是 Lena 和 Pepper 加密前后以及解密后的效果图.



(a)原始图像 Lena (b)加密图像 (c)解密后的图像

图5 Lena 加密前后及解密后效果图



(a)原始图像 Pepper (b)加密图像 (c)解密后图像

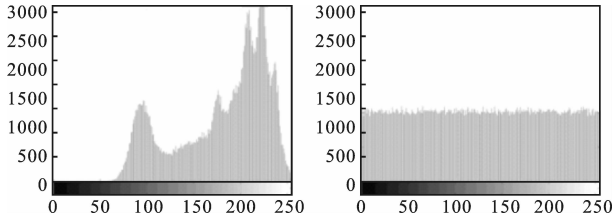
图6 Peper 加密前后及解密后效果图

(1) 密钥空间分析表明, 一个好的加密系统应该具备足够大的密钥空间以有效抵抗强力攻击. 本加密系统的密钥空间包括反馈增益 ϵ , Logistic 映射的参数 μ , 以及用于产生扩散序列的两个初始值 $\text{init3}, \text{init4}$. 假设计算精度为 $10 \sim 16$, 则该加密算法的密钥空间可达 $1.749 * 1048$. 由此可见, 本文的密钥空

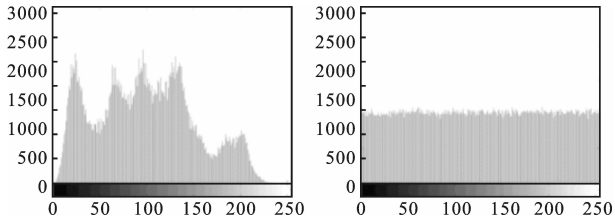
间是足以抵抗暴力攻击。

(2)统计特性分析,图像的统计分析手段包括直方图^[14]、相邻像素间的相关性和信息熵等。

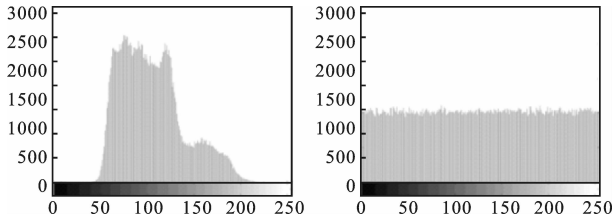
①图 7 给出了 Lena 图像加密前后的图像直方图,可以看出加密图像直方图与原始图像直方图存在明显差异,原图直方图中出现一系列的尖峰或波谷,会给攻击者提供可利用的信息;而加密后的图像像素接近均匀分布,因而从加密图像中几乎得不到有用的信息。



(a)原始图像 Red 通道直方图 (b)加密图像 Red 通道直方图



(c)原始图像 Green 通道直方图 (d)加密图像 Green 通道直方图



(e)原始图像 Blue 通道直方图 (f)加密图像 Blue 通道直方图

图 7 Lena 的 R,G,B 加密前后的图像直方图

②相邻像素之间的相关性分析

从图像中分别选取水平、垂直和对角方向 2 000 组相邻像素,然后使用式(8)计算其相关系数:

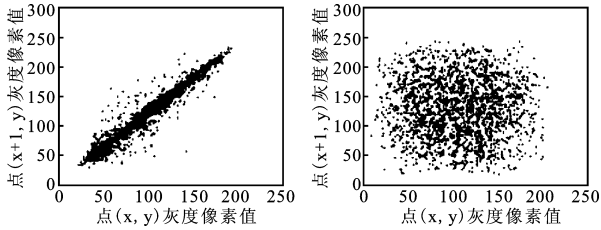
$$r = \frac{\sum_{i=1}^N (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{(\sum_{i=1}^N (x_i - \bar{x})^2)(\sum_{i=1}^N (y_i - \bar{y})^2)}} \quad (8)$$

式(8)中, N 表示选取的相邻像素对组数; $\bar{x}$ 、 $\bar{y}$ 分别是像素值 x_i 、 y_i 的平均值; x_i 和 y_i 分别是图像第 i 组相邻像素的像素值; r 为相邻像素的相关系数。

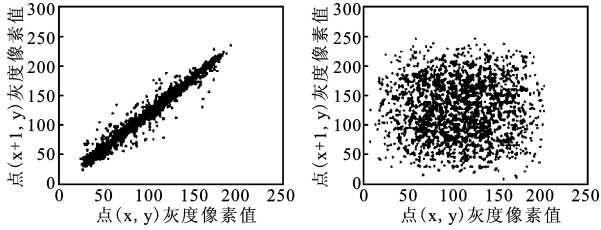
图 8 是原始的 Lena 图像与其加密后的图像在

水平、垂直和对角线方向相邻像素相关性的测试结果。

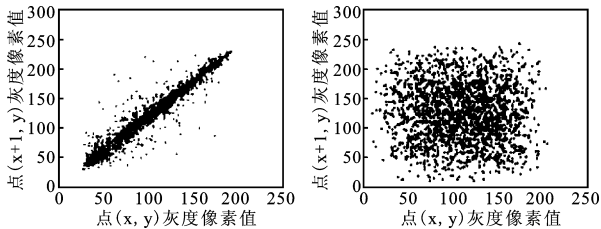
可以看出,在图 8(a)、图 8(c)和图 8(e)中测试结果图像分布接近为一个对角线,这表明其相关性非常强,分别达到了 0.971 926、0.985 029 和 0.959 329,而通过本文提出的加密算法进行加密之后,其像素值均均匀地分布在整个灰度空间中,水平、垂直和对角线三个方向的相邻像素相关性大幅度减少,其测量值分别达到了 -0.000 122、-0.001 465 和 0.001 376。



(a)原始图像水平像素相关性 (b)加密图像水平像素相关性



(c)原始图像垂直像素相关性 (d)加密图像垂直像素相关性



(e)原始图像对角线像素相关性 (f)加密图像对角线像素相关性

图 8 Lena 图像加密前后的像素相关性

图像的三个方向的相关度都趋向于零。

③信息熵分析

信息熵是用来衡量信息的不确定性的,设 m 为信息源,则 m 的信息熵计算公式可以定义为:

$$H(m) = - \sum_{i=0}^{2^n-1} p(m_i) \log_2 \frac{1}{p(m_i)} \quad (9)$$

式(9)中, $p(m_i)$ 表示符号出现的概率,对于 256 级灰度图像来说,理想期望值是 8. 加密后的图像的信息熵越接近 8,就表明该密文图像像素越接近随机分布. 使用式(9)计算加密后的图像的三个通道的信息熵,结果如表 2 所示。

表 2 彩色图像的信息熵

彩色图像	Lena		
	Red	Green	Blue
4. 2. 04. tiff	7. 999 250	7. 999 177	7. 999 418

从表 2 可以看出,加密后的三个通道的信息熵都非常接近于 8. 因此,使用本文提出的加密算法加密后的密文图像具有非常好的随机性.

(3)抗差分攻击分析

一个对明文敏感性越强的图像加密系统,抵抗差分攻击的能力就越好. 为了描述加密算法对明文的敏感性,我们使用像素改变率 NPCR(Number of Pixels Change Rate)和归一化像素值平均改变强度 UACI(Unified Average Changing Intensity)去度量. 两幅图像 $C_{R,G,B}$ 和 $C'_{R,G,B}$ 的 NPCR 与 UACI 的

表 3 NPCR 和 UACI

文件名	NPCR/%			UACI/%		
	R	G	B	R	G	B
4. 1. 01. tiff	99. 641 4	99. 630 7	99. 592 6	33. 422 3	33. 509 1	33. 340 0
4. 1. 02. tiff	99. 583 4	99. 588 0	99. 607 8	33. 523 5	33. 424 6	33. 511 3
4. 1. 03. tiff	99. 641 4	99. 627 7	99. 641 4	33. 563 0	33. 573 1	33. 554 8
4. 2. 04. tiff	99. 589 2	99. 609 0	99. 608 2	33. 475 2	33. 542 8	33. 509 4

表 3 列出了四幅彩色图像的 $NPCR_{R,G,B}$ 和 $UACI_{R,G,B}$ 的结果,从中我们可以看出 $NPCR_{R,G,B} > 99. 583\ 4\%$, $UACI_{R,G,B} > 33. 34\%$. 可见,本文提出的图像加密算法对明文十分敏感. 因此,该算法能很好地抵抗差分攻击.

(4)鲁棒性

①抗裁剪攻击能力分析

针对加密数字图像在存储与传输过程中受到裁剪攻击后解密图像信息容易丢失,本文通过选取大小为 $\beta * (M \times N)$ 的遮挡矩阵, β 取值分别为 1/4, 1/2 和 3/4, 将被该矩阵遮挡后像素值置为 0, 解密图像如图 9.

从图 9 可以看出,解密后的图像能够较好的恢复出原始图像信息,本文算法能很好地抵抗裁剪攻击.

②抗噪声性能分析

为验证本文提出的算法的抗噪声攻击性能,对加密图像加入不同强度的高斯噪声,强度分别为 10、15 和 20, 然后对其解密,结果如图 10.

从图 10 可以看出解密后的图像较好地恢复原始图像信息,表明本文算法具有一定的抗噪声攻击能力.

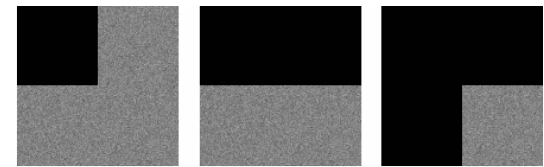
计算公式可以定义为^[15]:

$$NPCR_{R,G,B} = \sum_{i=1}^M \sum_{j=1}^N \frac{D(i,j)}{M \times N} \times 100\%$$
 (10)

$$UACI_{R,G,B} = \sum_{i=1}^M \sum_{j=1}^N \frac{|C_{R,G,B}(i,j) - C'_{R,G,B}(i,j)|}{M \times N \times 255} \times 100\%$$
 (11)

$$D(i,j) = \begin{cases} 0, & \text{if } C_{R,G,B}(i,j) = C'_{R,G,B}(i,j) \\ 1, & \text{if } C_{R,G,B}(i,j) \neq C'_{R,G,B}(i,j) \end{cases}$$
 (12)

$C_{R,G,B}$ 和 $C'_{R,G,B}$ 是由两幅仅存在一个像素比特位不同的明文图像加密得到的. 测试的彩色图像来源于 USC-SIPI 图像库. 对每一幅测试图像,随机选择一个像素值改变其最低的比特位,结果如表 3 所示.



(a)遮挡比例为 1/4 的加密图像 (b)遮挡比例为 1/2 的加密图像 (c)遮挡比例为 3/4 的加密图像



(e)遮挡比例为 1/4 的解密结果 (f)遮挡比例为 1/2 的解密结果 (g)遮挡比例为 3/4 的解密结果

图 9 抗裁剪攻击测试结果



(a)强度 10 (b)强度 15 (c)强度 20

图 10 加入不同强度高斯白噪声的 Lena 解密效果图

综上,就裁剪攻击和噪声攻击两方面来说,本算

法具有较强的鲁棒性.

5 结束语

本文提出了一种将时间延迟与 Logistic 映射相结合的新的混沌映射模型,该模型具有更宽的混沌参数区间,并且可克服传统 Logistic 映射在混沌参数区间内存在多个周期窗口的缺陷.本文提出的加密系统只需一轮的置换扩散加密操作便可获得良好的加密效果,而且置换操作的密钥与原始图像相关.性能分析和仿真结果表明,该加密算法具有较大的密钥空间,加密后的密文具有较好的伪随机性,能够有效抵抗统计分析攻击、差分攻击和选择明文攻击,并在抗裁剪攻击和抗噪声攻击方面显示了较强的鲁棒性.

参考文献:

- [1] 包林霞,刘伟,Bao Linxia,等.基于小波变换域混沌加密与循环移位的改进图像加密算法[J].计算机应用研究,2016,33(10):3074-3077.
- [2] Kanso A, Smaoui N. Logistic chaotic maps for binary numbers generations[J]. Chaos Solitons & Fractals, 2009, 40(5):2557-2568.
- [3] Matthews R. On the derivation of a "Chaotic" encryption algorithm[J]. Cryptologia, 1984, 8(1):29-41.
- [4] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International Journal of Bifurcation & Chaos, 2011, 21(6):1259-1284.
- [5] 卢辉斌,张鹏,国宪鹏,等.一种新的基于双混沌系统的图像加密方案[J].计算机工程与应用,2012,48(2):90-92.
- [6] 赵方舟,赵怀勋,李双,等.基于混沌映射的彩色图像加密算法设计实现[J].计算机与数字工程,2008,36(3):87-89.
- [7] Mohammad Seyedzadeh S, Mirzakuchaki S. A fast color image encryption algorithm based on coupled two-

dimensional piecewise chaotic map[J]. Signal Processing, 2012, 92(5):1202-1215.

- [8] 李玲,王伟男,李津杰,等.基于 Logistic 映射和超混沌的自适应图像加密算法[J].微电子学与计算机,2012,29(1):42-46.
- [9] Rui-Shan D U, Shang F H. Application of compound chaotic mapping in speech encryption algorithm[J]. International Journal of Computer Science & Network Security, 2014, 45(7):103-104.
- [10] Lian S, Sun J, Wang Z. A block cipher based on a suitable use of the chaotic standard map[J]. Chaos Solitons & Fractals, 2005, 26(1):117-129.
- [11] Zhou Y, Hua Z, Pun C M, et al. Cascade chaotic system with applications[J]. IEEE Transactions on Cybernetics, 2015, 45(9):2001-2012.
- [12] 刘云,郑永爱.基于混沌系统的彩色图像加密新方案[J].计算机工程与应用,2011,47(3):90-93.
- [13] May R M. Simple mathematical models with very complicated dynamics[J]. Nature, 1976, 261(5560):459-67.
- [14] 谢涛,何兴.一种新的基于混沌的彩色图像加密方案[J].计算机应用研究,2013,30(1):318-320.
- [15] 朱从旭,胡玉平,孙克辉.基于超混沌系统和密文交错扩散的图像加密新算法[J].电子与信息学报,2012,34(7):1735-1743.

作者简介:

谭冬文 男,(1992-),硕士研究生.研究方向为混沌加密、图像处理. E-mail: tandw14@lzu.edu.cn.

李彩虹 女,(1972-),博士,高级实验师.研究方向为混沌加密、信息安全、图像处理、语音识别.

李守亮 男,(1979-),博士,讲师.研究方向为混沌加密、图像处理、信息安全.

李廉 男,(1951-),博士,教授.研究方向为网格计算、无线传感器网络以及行为与情感分析、健康关怀等.