计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(6):125−129 [doi: 10.15888/j.cnki.csa.006788]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于改进 Logistic 映射的图像加密算法①

胡春杰[1,2], 阮　聪[2], 牛智星[1]

[1](江苏南水科技有限公司, 南京 210012)
[2](水利部南京水利水文自动化研究所, 南京 210012)
通讯作者: 胡春杰, E-mail: 448396246@qq.com

摘　要: 为了有效地提高图像加密效果及安全性, 设计一种改进 logistic 映射图像加密算法. 首先在 cubic 映射和 logistic 映射基础上, 提出了一种新的二维离散映射, 克服了混沌区间窄和参数少的问题, 并利用改进的 logistic 映射对图像进行置乱, 然后将置乱图像进行相邻像素间按位异或运算、交叉换位操作得到最终密文图像. 仿真结果表明, 该算法简单易执行, 安全性好, 抗攻击能力较强, 效率高等特点.

关键词: cubic 映射; 改进 logistic 映射; 交叉换位; 图像加密

引用格式: 胡春杰,阮聪,牛智星.基于改进 Logistic 映射的图像加密算法.计算机系统应用,2019,28(6):125–129. http://www.c-s-a.org.cn/1003-3254/6788.html

Image Encryption Algorithm Based on Improved Logistic Mapping

HU Chun-Jie[1,2], RUAN Cong[2], NIU Zhi-Xing[1]

[1](Jiangsu Nanshui Technology Co. Ltd., Nanjing 210012, China)
[2](Nanjing Automation Institute of Water Conservancy, Ministry of Water Resources, Nanjing 210012, China)

Abstract: In order to effectively improve the image encryption effect and security, an improved logistic mapping image encryption algorithm is designed. Firstly, on the basis of cubic mapping and logistic mapping, a new two-dimensional discrete mapping is proposed to overcome the problem of narrow chaotic interval and fewer parameters. The image is scrambled by improved logistic mapping. Then the scrambled image is processed by bitwise exclusive or operation between adjacent pixels, and the final cipher-text image is obtained by crossover operation. The simulation results show that the algorithm is simple and easy to execute, has good security, strong anti-attack ability and high efficiency.

Key words: cubic mapping; improved logistic mapping; bit exchanged across; image encryption

引言

随着数字技术、通信技术的飞速发展与普及, 图像信息成为多媒体和网络中最重要的信息之一. 然而, 由于互联网的不确定性与开放性, 在图像数据传输过程中, 其信息数据安全性问题越来越受到重视. 所以, 如何保证数字图像的安全性显得特别重要, 图像加密是最直接有效的途径之一. 传统的加密方法加密效率低、时间较长, 不再适用于图像加密[1,2]. 由于混沌系统具有伪随机性、初值敏感性等特性, 因此将混沌系统应用到图像加密中非常契合. 随着研究的不断深入, 混沌图像加密算法和技术有了相当大发展[3–6].

文献[7]提出基于 logistic 映射图像加密算法. 简单易实现, 效果良好, 但是单一的映射加密安全性较差. 文献[8]提出一种基于图像分区的置乱算法. 该算法首先对原始图像进行分块置乱,再对相邻像素值进行异或运算置乱图像. 谢国波[9]提出了结合 logistic 映射和 Arnold 映射对图像进行加密, 提高了置乱和扩散两者之间的关联性, 增加了图像的安全性. 文献[10]提出了

① 收稿时间: 2018-08-29; 修改时间: 2018-09-26; 采用时间: 2018-09-29; csa 在线出版时间: 2019-05-25

加强型超混沌加密算法, 相比低维系统密钥空间大, 非线性行为复杂化, 虽提高了图像的安全性, 但是效率不高[11−13].

本文在 cubic 映射和 logistic 映射基础上, 提出了一种改进 logistic 映射的图像加密算法. 首先改进 logistic 映射对图像进行置乱, 然后将置乱图像进行相邻像素间按位异或运算、交叉换位操作, 实现了对数字图像的加密. 实验结果表明, 本文算法不仅达到了较好的加密效果, 而且安全性好, 抵抗统计攻击和差分攻击强等特点.

1 Logistic 映射及改进

1.1 Logistic 映射

Logistic 映射是一个典型的非线性迭代方程. 其方程如下:

$$x_{k+1}=\mu x_k(1-x_k) \tag{1}$$

其中, 当 3.5699<μ≤4 时, Logistic 映射系统处于混沌状态, 对给定初始值x_0, 在式 (1) 作用下生成的序列是非周期性、非收敛以及对初始条件敏感的, 如图 1 所示.

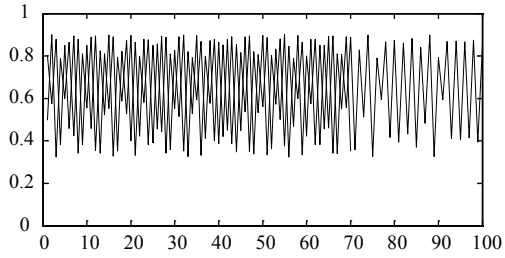


图 1 Logistic 映射序列分布

1.2 改进的 Logistic 映射

目前一维离散混沌映射有 logistic 映射和 cubic 映射以及它们的衍生映射, 其共同点都是系统参数少, 混沌区间窄, 混沌的复杂性较低, 函数形式简单. 为了克服以上不足, 本文将 logistic 映射和 cubic 映射进行结合改进, 其方程表达式如下所示:

$$\begin{cases} x_{k+1}=\mu y_k-cx_ky_k \\ y_{k+1}=ax_k^2-bx_k \end{cases} \tag{2}$$

式中, $\mu\in[0,4]$, $a\in[0,4]$, $b\in[0,3]$, $c\in[0,4]$ 当参数 μ=1.8, a=0.5, b=1, c=1 时, 系统具有两个正的 Laypunov 指数, 说明该系统是一个超混沌系统.

为了检验改进 logistic 映射系统伪随机性的好坏, 分别对 logistic 映射改进前后进行了 NIST 测试, 测试结果如表 1 所示, 从表 1 可以看出, logistic 序列有 5 项密钥通过, 改进 logistic 映射全部通过, 表明改进后映射的伪随机性高于经典的 logistic 映射.

表 1 NIST 测试结果

测试项目	Logistic 映射	改进 logistic 映射
频率	0.000	0.017
块内频率	0.000	0.095
累积和	0.000	0.054
游程	0.394	0.253
最长游程	0.068	0.935
二进制矩阵阶	0.693	0.065
FFT	0.001	0.554
非重叠块匹配	0.259	0.856
重叠块匹配	0.142	0.406
通用统计	0.246	0.234
近似熵	0.000	0.987
随机偏离	0.546	0.649
随机偏离变量	0.859	0.486
串行	0.000	0.133
线性复杂度	0.159	0.756

2 改进的加密算法设计

2.1 位置置乱

本文应用改进的 logistic 映射置乱明文图像, 其主要步骤如下:

(1) 将原始明文图像转换成二维矩阵, 分别将其行数和列数放在数组 $C1$ 和 $C2$ 中;

(2) 计算原始明文图像所有像素值之和为 sum, 通过式 (3), 得到辅助密钥 k;

$$k=\mathrm{mod}(sum,256)/255 \tag{3}$$

(3) 设改进 logistic 映射的初始值为x_0和y_0经过$x_0'=\sqrt{(x_0^2+k^2)/2}$和$y_0'=\sqrt{(x_0^2+k^2)/2}$得到混沌系统新的初始值$x_0'$和$y_0'$;

(4) 设置初始条件x_0=0.3,y_0=0.4 经过式 (2) 迭代生成两个实数序列$\{x_k,y_k|k=1,2,\cdots,m\times n\}$

(5) 对序列x_k和y_k分别依次进行升序操作, 并相应地记录各元素在原始序列的下标, 得到两个序列的索引 $Index1$ 和 $Index2$, 将索引 $Index1$ 和 $Index2$ 与原始图像的行 $C1$ 和列 $C2$ 交换, 从而达到置乱的效果, 得到置乱图像 C.

2.2 图像像素值的改变

首先对置乱图像 C 中每个像素和它前面相邻的像素进行按位异或运算, 再对其异或运算的结果进行像素值的交叉换位, 得出最终加密图像. 其主要步骤如下:

(1) 设置乱图像 C 的第一个像素的灰度值为 $C(1)$ 与 255 进行异或, 得到$C'(1)$,再对$C'(1)$进行交叉换位, 得到 $Q(1)$. 具体的换位操作如下图 2 所示 (图 2 中的 bit1, bit2, …, bit8 分别表示像素点二进制灰度值的第 1, 2, …, 8 位);

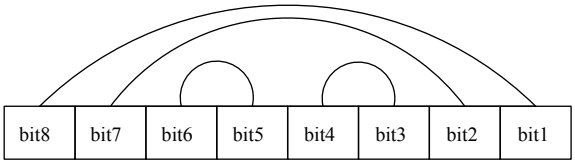


图 2 交叉换位示意图

(2) 置乱图像 C 的第二个像素的灰度值 $C(2)$ 与 $Q(1)$ 进行异或操作, 得到$C'(2)$,再对$C'(1)$进行交叉换位, 得到 $Q(2)$;

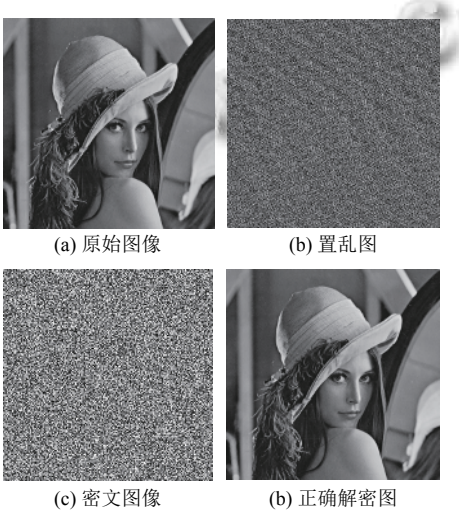
(3) 依次将图像的每个灰度值 $C(i)$ 与 $Q(i\text{-}1)$ 进行异或, 得到$C'(i)$; 依据交叉换位规则得到 $Q(i)$. 最后将一维 $Q(i)$ 换成图像 D, 即得到最终加密图像 D.

2.3 解密算法

解密过程为加密过程的相反过程, 只要在正确的密钥条件下, 按照加密过程的相反操作处理就可以恢复得到原始图像.

3 仿真结果

本文采用经典的 Lena 作为原始图像, 大小为 256×256, 在 Matlab7.0 平台上仿真实验, 运行得到加密图像. 图 3(b) 为置乱图像, 图 3(c) 为密文图像, 图 3(d) 为正确解密图像.



(a) 原始图像 (b) 置乱图

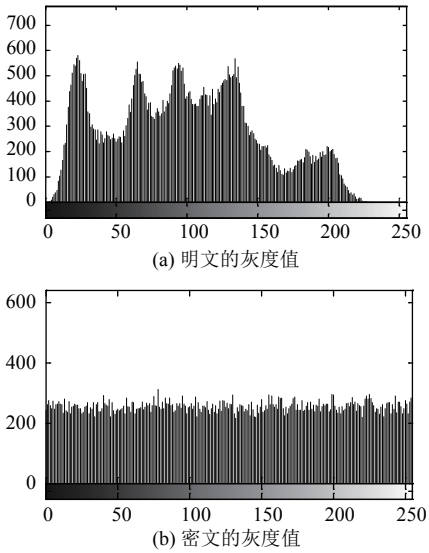
(c) 密文图像 (b) 正确解密图

图 3 图像加密与解密

4 算法分析

4.1 直方图分析

图 4(a) 为明文图像的灰度直方图, 图 4(b) 为密文图像的灰度直方图. 从图 4 可以看出, 明文图像的像素点分布不均匀, 密文图像的像素点分布相对均匀, 很好地隐藏了明文图像的统计特性, 达到了预期的要求.



(a) 明文的灰度值

(b) 密文的灰度值

图 4 加密前后的灰度值

4.2 密钥空间分析

本文加密算法中改进的 logistic 映射有 4 个系统参数和 2 个初始值共 6 个密钥值. 假如计算机精度可以达到10^{-16},那么密钥空间为10^{96},以及在置乱-扩散过程中有一个外层循环, 可见密钥空间非常大. 想要通过穷举攻击解密图像, 成功的几率是及其渺小的, 也就是说可以满足抵御暴力破译的要求.

4.3 信息熵

信息熵是衡量信号源不确定性的重要参数, 图像越是混乱, 信息熵就越接近理想值, 其定义式为:

$$H(m)=\sum_{i=1}^{2N-1}P(m_i)\log_2\frac{1}{P(m_i)} \tag{4}$$

其中, $P(m_i)$是灰度值m_i出现的概率, N 为像素比特位数. 由式 (11) 计算可得原始图像的信息熵为 7.5683, 密文图像的信息熵为 7.9900, 非常接近于灰度级为 256 的图像最大值 8, 可以得出密文图像所有像素值分布十分均匀的, 加密系统能够有效地抵御恶意熵攻击.

4.4 相邻像素点的相关性

为了检验与分析加密前后图像的相关性, 分别从

明文和密文中随机性地选取 2000 对相邻的像素, 使用式 (12) 计算相关性:

$$\begin{cases} D(x)=1/n\sum_{i=1}^{n}[x_i-E(x)]^2 \\ \mathrm{cov}(x,y)=1/n\sum_{i=1}^{n}[x_i-E(x)][y_i-E(y)] \\ r=\mathrm{cov}(x,y)/(\sqrt{D(x)}\sqrt{D(y)}) \end{cases} \tag{5}$$

其中, $E(x)$、$E(y)$ 分别是 x, y 的期望; n 是像素点的个数; $\mathrm{cov}(x, y)$ 是 x, y 的协方差; r 相关系数,

图 5 至图 7 分别是明文图像和密文图像在垂直、水平、对角线方向相邻点分布情况. 从各图中可以看出, 明文图像中的点基本上都集中在对角线周围, 即图像相邻点相关性很强. 而密文图像中的像素点均匀集中在坐标上, 即密图相邻点相关性低.

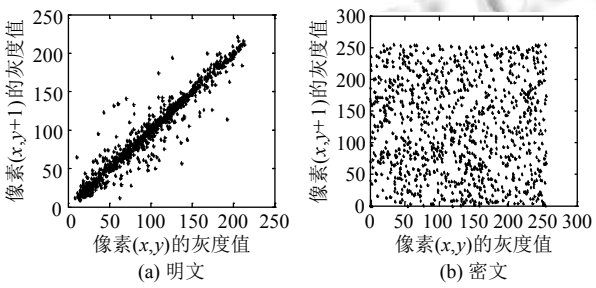


图 5 垂直方向的相关性

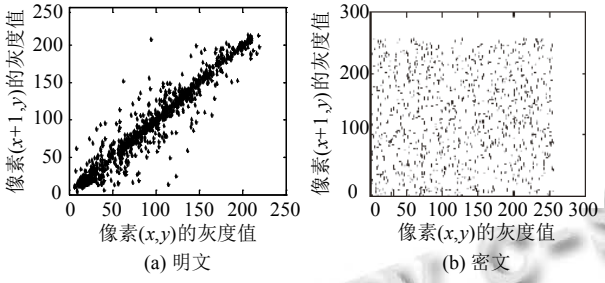


图 6 水平方向的相关性

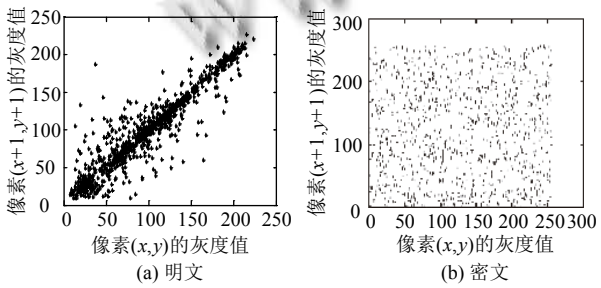


图 7 对角方向的相关性

由表 2 可得到, 明文图像的相邻像素点相关性系数趋近于 1, 而密文图像的相关性较小, 其相关系数靠近于 0, 可以得出密文图像的相邻间像素点基本不再相关. 相比较其他算法[4,9,14], 可见该算法的相关系数 r 更小一点, 说明本文加密算法具有良好的扩散性.

表 2 相邻像素点的相关

方向	原始图像	加密图像	文献[4]	文献[9]	文献[14]
水平	0.9568	0.0098	–0.0029	0.0136	0.0216
垂直	0.9642	–0.0089	–0.0150	0.0062	0.0065
对角	0.9351	0.0014	0.0129	0.0175	0.0347

4.5 差分攻击分析

为了测试明文图像一个像素的变化对该算法整体加密结果的影响, 采用两种常见的措施[15]: 像素变化率 (*NPCR*) 和统一平均变化程度 (*UACI*). 若一个像素值的变化导致密文图像发生显著地改变, 就可以说明算法能抵御差分攻击.

$$NPCR=\frac{\sum_{i,j}D(i,j)}{m\times n}\times 100\% \tag{6}$$

$$UACI=\frac{1}{m\times n}\left[\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right]\times 100\% \tag{7}$$

其中, $D_{ij}=\begin{cases}1, c_1(i,j)\neq c_2(i,j)\\ 0, c_1(i,j)=c_2(i,j)\end{cases}$, m 和 n 分别是图像的行数和列数;

现从图像中随机选取 5 个像素点, 分别将像素值加 1, 再对改变像素值后图像进行加密, 应用式 (13) 和式 (14) 进行计算. 对得到的值取平均值 $NPCR$=99.61% 和 $UACI$=31.62%. 这就说明当改变原始图像 lena(256×256) 一个像素时, 会使密文图像接近 100% 的 *NPCR* 变化, *UACI* 也在 31% 以上. 说明本文加密算法抵抗差分攻击能力比较强.

5 结束语

本文提出了基于改进 logistic 映射的图像加密算法. 先利用改进的 logistic 映射对图像进行位置置乱, 再进行相邻像素间按位异或、交叉换位操作得到最终加密图像. 仿真实验分析表明, 该算法可以达到良好的加密效果、简单易实现、安全性较好, 在数字图像通信传输中, 具有良好的实用价值.

参考文献

1 François M, Grosges T, Barchiesi D, *et al*. A new image encryption scheme based on a chaotic function. Signal

Processing: Image Communication, 2012, 27(3): 249–259. [doi: 10.1016/j.image.2011.11.003]
2 胡春杰, 陈晓, 郭银. 基于多混沌映射的光学图像加密算法. 激光杂志, 2017, 38(1): 110–114.
3 张健, 房东鑫. 应用混沌映射索引和 DNA 编码的图像加密技术. 计算机工程与设计, 2015, 36(3): 613–618.
4 Kanso A, Ghebleh M. A novel image encryption algorithm based on a 3D chaotic map. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(7): 2943–2959. [doi: 10.1016/j.cnsns.2011.11.030]
5 Wang XY, Yang L. A novel chaotic image encryption algorithm based on water wave motion and water drop diffusion models. Optics Communications, 2012, 285(20): 4033–4042. [doi: 10.1016/j.optcom.2012.06.039]
6 Lin R, Liu QN, Zhang CL. A new fast algorithm for gyrator transform. Laser Technology, 2012, 36(1): 50–53.
7 刘刚, 王立香. 一种新的基于混沌的图像加密算法. 电视技术, 2008, 32(12): 22–24. [doi: 10.3969/j.issn.1002-8692.2008.12.007]
8 朱晓升, 廖晓峰. 基于图像分区的置乱算法. 计算机技术与发展, 2015, 25(12): 52–55, 59.
9 谢国波, 丁煜明. 基于 Logistic 映射的可变置乱参数的图像加密算法. 微电子学与计算机, 2015, 32(4): 111–115.
10 Zhu CX, Sun KH. Cryptanalysis and improvement of a class of hyperchaos based image encryption algorithms. Acta Physica Sinica, 2012, 61(12): 120503.
11 Wang XG, Zhan M, Lai CH, *et al*. Error function attack of chaos synchronization based encryption schemes. Chaos, 2004, 14(1): 128–137. [doi: 10.1063/1.1633492]
12 Pan TG, Li DY. A novel image encryption using Arnold cat. International Journal of Security and its Application, 2013, 7(5): 377–386. [doi: 10.14257/ijsia]
13 张海涛, 姚雪, 陈虹宇, 等. 基于分层 Arnold 变换的置乱算法. 计算机应用, 2013, 33(8): 2240–2243.
14 赵芳玲, 马文涛. 一种图像混合加密算法仿真研究. 计算机仿真, 2012, 29(5): 278–282, 290. [doi: 10.3969/j.issn.1006-9348.2012.05.068]
15 王静, 蒋国平. 一种超混沌图像加密算法的安全性分析及其改进. 物理学报, 2011, 60(6): 83–93.