

文章编号: 1007- 2985(2008) 05- 0064- 04

基于混沌映射的图像置乱加密算法^{*}

汪 超, 黄 峰
(湖南工程学院, 湖南 湘潭 411101)

摘 要: 提出了一种基于混沌映射的图像置乱加密算法, 映射置乱了像素的位置, 过程是可逆的, 可用于加密图像. 设计了密钥产生的方法, 分析了图像加密算法的安全性问题. 结果表明, 该映射可加密压缩文件甚至任意长度的数据集.

关键词: 图像加密; 混沌; 置乱

中图分类号: TP309. 7

文献标识码: A

随着网络的发展, 人们对图像安全问题越来越重视. 一些常见的数据加密算法, 如 DES 算法^[1]、AES 算法等被应用到图像加密领域^[1]. 但在加密大尺寸图像, 如卫星图像时, 这些算法遇到了加密速度低、安全性不能保证、需要同时解决压缩和加密等问题. 图像相对文本具有信息量大, 相邻像素间具有相关性等特点. 针对其特点, 近年来涌现出以混沌加密为代表的新的图像加密技术^[2]. 这些算法可大致分 2 类, 一类构造伪随机信号流, 改变像素值, 一类利用图像的几何特点, 随机置乱图像像素位置, 减少像素间的相关性. 安全性能分析表明, 由于图像是二维的, 具有一定的几何特点, 因此一个安全的图像加密算法应同时包括这 2 个子过程: 混淆(Confusion) 和扩散(Diffusion). 研究图像置乱加密方法很有意义^[3].

利用构造的思想, 提出了一种新的混沌映射^[4-5], 可加密任意形状的图像. 笔者推导了计算公式, 提出了图像加密算法, 设计了密钥, 并对加密算法进行了仿真.

1 混沌映射原理和算法

映射利用了图像的一个重要性质: 像素能够插入到其他像素之间. 设图像为矩形, 大小为 $M \times N (M \neq N)$. 首先将原图像构造为一个等腰三角形, 等腰三角形每行的像素数目依次为 1, 2, 3, ..., 然后利用三角形行之间的像素数目差, 依次将奇数行的像素插入到偶数行像素之间, 于是三角形被拉伸为一个长为 MN 的直线, 最后按照原图像特征将直线折叠成为一个和原图像大小一样 MN 的图像, 如图 1 所示.

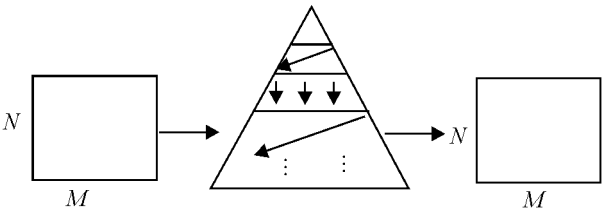


图 1 映射示意图

由原理可得到该映射的算法, 设图像大小为 $M \times N$, $A(i, j)$ 为图像中的任意一点, 且 $i = 0, 1, 2, \dots, N - 1, j = 0, 1, 2, \dots, M - 1$; $L(i)$ 为将三角形拉伸后的行向量, 其中 $i = 0, 1, \dots, MN - 1$. 由下式计算点 $A(i, j)$ 在三角形中的行数:

$$\frac{k(k-1)}{2} < i \times N + j \leq \frac{k(k+1)}{2}. \tag{1}$$

(1) 左映射算法

^{*} 收稿日期: 2008- 07- 13

作者简介: 汪 超(1970-), 男, 湖南醴陵人, 湖南工程学院讲师, 硕士, 主要从事计算机控制和数字图像处理研究.

(i) 当 k 为奇数时,

$$L[2(i \times N + j) + 1 - \frac{k(k-1)}{2}] = A(i, j). \tag{2}$$

(ii) 当 k 为偶数时,

$$L[2(i \times N + j) - \frac{(k+2)(k-1)}{2}] = A(i, j). \tag{3}$$

需要注意, 原图很难构造一个完整的三角形, 因此三角形最后 1 行可能并不完整, 该文将其保留.

(2) 右映射算法.

(i) 当 k 为奇数时,

$$L[2(i \times N + j) + 1 - \frac{k(k-1)}{2}] = A(i, M - 1 - j). \tag{4}$$

(ii) 当 k 为偶数时,

$$L[2(i \times N + j) - \frac{(k+2)(k-1)}{2}] = A(i, M - 1 - j). \tag{5}$$

2 图像加密和解密算法

由于映射可分为左映射和右映射, 将左映射和右映射的映射次数设计为密钥 key . 如 $\text{key} = 1234$, 表示图像依次左映射 1 次, 右映射 2 次, 然后用左映射 3 次, 最后用右映射 4 次. 为了保证加密效果, 每一个部分密钥值都小于 10^{31} . 加密算法如图 2 所示, 其中 K_1 及 K_2 分别是密钥 key 的一部分, 可以相同或可互相推导得到, 函数 $F(K)$ 为密钥的函数, 输出为扩散函数的参数.

图像加密算法可采用的扩散函数

$$v_k' = v_k + G(v_{k-1}') \bmod L. \tag{7}$$

其中: v_k 是指每一个像素的值; v_k' 为扩散后的像素值; G 是像素值的函数. 如可以设 $G(v_{k-1}') = 5 v_{k-1}'$, 8 位灰度图 $L = 256$. 图像加密算法分为 3 步: (i) 根据安全要求, 设置密钥 key , 得到 K_1 及 K_2 . 利用 K_1 及算法(1), (3) 至(5), 将图像 $A(i, j)$ 拉伸成一条直线 $L(i), i = 0, 1, \dots, MN - 1$; (ii) 利用算法(6), 将直线折叠, 得到置乱图像 $B(i, j)$; (iii) 利用密钥 K_2 及扩散函数, 对置乱函数进行处理得到密图.

图像解密算法与加密算法相反, 如图 3 所示, 解密密钥与加密密钥相同, 因此该算法为对称加密算法.

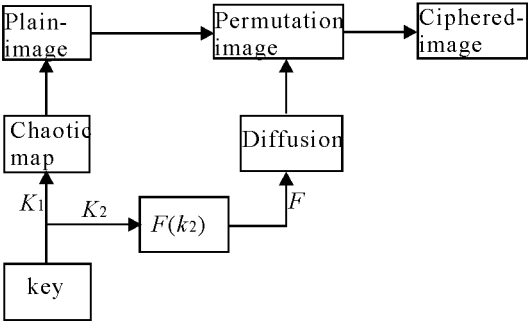


图 2 图像加密算法

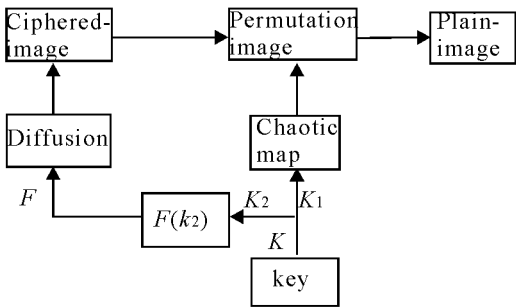


图 3 图像解密算法

3 加密实例

对 8 位 lena 灰度图进行仿真测试, 图像为 256×240 的矩形图像, 如图 4- a 所示. 为了研究新映射的性能, 笔者令 $K_2 = 0$, 即不使用扩散函数, 此时, 加密系统仅仅置乱图像, 没有改变图像的像素值. 当 $\text{key} = 1$ 时, 图像已没有原图特征, 如图 4- b 所示; 当 $\text{key} = 0123456789$ 时, 密图像素平均分布, 加密效果良好, 如图 4- c, 加密图像的直方图如图 4- d.

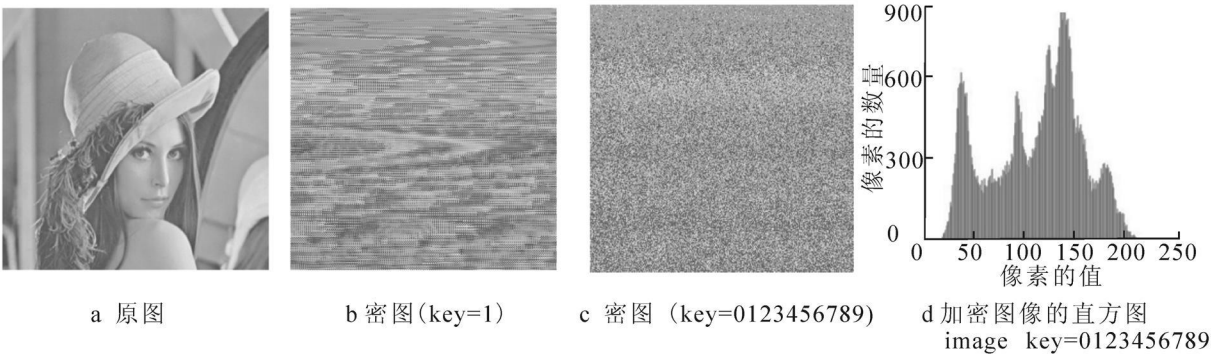


图 4 图像加密实例

4 安全性能分析

4.1 密钥空间分析

由于最基本、最流行的破解方法是对密钥进行穷尽搜索, 密钥空间大是加密算法安全的前提, 加密算法的密钥空间(无扩散函数)如表 1 所示. 研究表明, 密钥空间大小只和密钥长度有关, 在理想情况下(计算速度允许), 可认为密钥能无限增加.

表 1 密钥长度和密钥空间

密钥长度/bit	64	128	512
密钥空间	1.84×10^{19}	3.4×10^{38}	1.34×10^{154}

4.2 密钥敏感度

当加密密钥 key= 0123456789 加密时, 用解密密钥 key₁= 0123456788 和 key₂= 0123456780 分别解密, 如图 5 所示. 即使加密密钥和解密密钥仅 1 位有最差异, 也无法解密图像, 说明对密钥差异非常敏感.

4.3 统计分析

由于图像相邻像素之间具有很强的相关性, 如果密图相邻像素之间相关性变小, 说明密图安全性变强. 图 6 为原图和密图的(x, y)和(x, y+ 1)关系, 原图的相关系数为 0. 940 4, 加密之后的相关系数为 0. 005 4, 证明密图相邻像素之间相关度接近于 0. 其他相邻点的相关系数如表 2 所示, 说明密图相邻像素之间相关性很小.

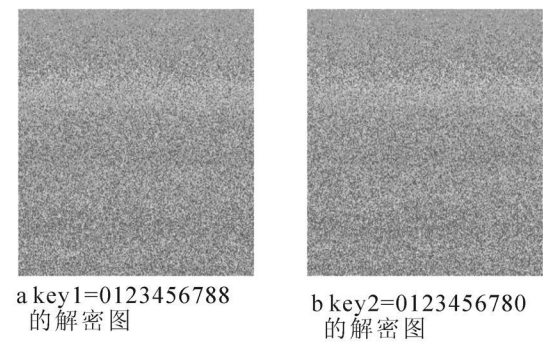


图 5 密钥敏感度测试

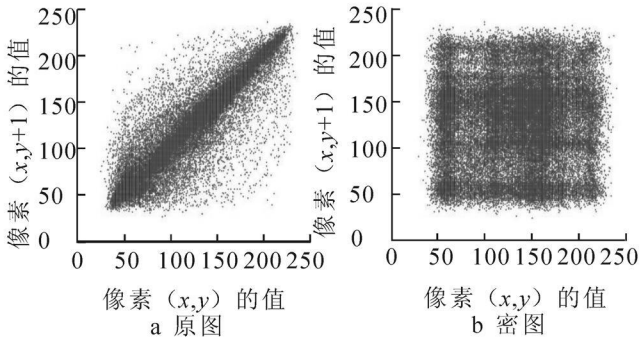


图 6 相邻点分析

表 2 加密前后相邻点之间的相关系数

项目	原图	密图
水平方向	0.968 3	0.036 7
竖直方向	0.940 4	0.029 8
对角线方向	0.913 0	0.034 2

4.4 $r-m$ 自相关度

该参数越能准确刻画出图像中像素的关联程度, 设图像 $A = (i, j)_{M \times N}$ 及集合 $A_{i,j}^{r,m}$. 如上所述, 则图像 A 的 $r-m$ 相关性定义为

$$R^{r,m}(A) = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{|A_{i,j}^{r,m}|}{|A_{i,m}^{r,255}|}}{M \times N} \times 100\%, \tag{8}$$

其中 $A_{i,j}^{r,m}$ 表示 $A_{i,j}^{r,m}$ 集合中元素的个数. 当 r 与 m 发生变化时, 参数 R 的值也将随之发生变化. 计算表明, 当 $r = 1$ 时, $r-m$ 相关度随 m 变化情况如表 3 所示, 其中 key = 0123456789, 加密后密图的自相关度相对加密前的 lena 图的相关度明显减小.

表 3 加密前后 $r-m$ 自相关度

m	1	3	5	7	9	10
lena	0.380 4	0.433 8	0.515 8	0.576 0	0.621 3	0.640 1
key	0.148 2	0.151 0	0.165 1	0.178 5	0.191 3	0.197 5
m	11	13	15	17	19	20
lena	0.656 9	0.685 7	0.709 6	0.730 0	0.747 5	0.755 4
key	0.203 6	0.215 3	0.226 6	0.237 5	0.248 2	0.253 5

5 结语

利用构造的思想, 提出了一种新的混沌映射, 能够加密任意形状图像. 加密算法和其他算法比较具有明显优势: (1) 与 SCAN 语言比较, 密钥空间更大, 如 Baker map 最大为 2^{N-1} (N 为图像的宽), 而该映射密钥空间很大(表 1); 对密钥变化敏感, 只要密钥稍有变化, 密图就会截然不同; 应用前景更为广泛, 能够加密任意形状的图像或数据集, 突破了其他算法对图像形状的限制; 加密速度快, 能够实现实时加密. (2) 和混沌流密码比较, 加密前后没有信息损失、移植性高, 加密方法简单, 易于软、硬件实现. 由于具有很强的灵活性, 混沌映射能用于压缩后的图像加密, 以及数字水印等领域.

参考文献:

[1] BOURBAKIS N, ALEXOPOULOS C. Picture Data Encryption Using SCAN Patterns [J]. Pattern Recognition, 1992, 25(6): 567– 581.

[2] MANICCAM S S, BOURBKIS N G. Image and Video Encryption Using Scan Patterns [J]. Pattern Recognition, 2004, 37(4): 725– 737.

[3] FRIDRICH J. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps [J]. Int. J. Bifurc. Chaos, 1998, 8(6): 1 259– 1 284.

[4] CHEN Guan-rong, MAO Yao-bin, CHUI CHARLES K. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps [J]. Chaos, Solitons & Fractals, 2004, 21(3): 749– 761.

[5] LI Shu-jun, MOU Xuan-qin, BOLIYA L YANG, et al. Problems with a Probabilistic Encryption Scheme Based on Chaotic Systems [J]. Int. J. Bifurc. Chaos, 2003, 13(10): 3 063– 3 077.

Image Randomly Encryption Algorithm Based on Chaos Mapping

WANG Chao, HUANG Feng

(Hunan Institute of Engineering, Xiangtan 411104, Hunan China)

Abstract: A digital image encryption algorithm based on chaotic mapping is presented in this paper. The paper formulates the approach of the map, designs a method of key generation and analyses the security of the proposed image encryption. The simulation results show that the proposed encryption approach is valid. Analysis shows that the map can encrypt compressed images or arbitrary length of data sets.

Key words: image encryption; chaotic; set chaotically (责任编辑 陈炳权)