

基于混沌的位级图像加密算法研究

吴新华

(南通纺织职业技术学院 现教中心, 江苏 南通 226007)

摘 要: 提出了一种新的位级图像混沌加密算法. 首先将明文图像划分为 8 幅位级图像并将其作为一个整体, 利用 Chen's 混沌系统生成混沌序列, 进行位级图像置乱, 然后利用 Logistic 混沌序列进行图像像素扩散, 最后进行测试仿真和性能分析, 并与其他图像加密算法进行比较, 测试结果表明所提算法具有较强的安全性和有效性.

关键词: 混沌; 图像加密; 位级图像; 置乱; 扩散

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2013)12-0069-04

Research on the Bit-Level Image Encryption Algorithm Based on Chaos

WU Xin-hua

(Modern Education Technology Center, Nantong Textile Vocational Technology College, Nantong 226007, China)

Abstract: A new bit-level image encryption algorithm based on chaos is presented with the properties of chaotic sequences and inherent characters of bit-level images. At first, the plain image is divided into 8 bit-level images which are treated as a group. And the bit-level images' group is permuted using chaotic sequences generated by Chen's chaotic map. Then the image pixel-level diffusion is carried on using Logistic chaotic sequences. Finally, experiments have been carried out to compare its performance with that of other schemes, and the results justify the superior security of our proposed algorithm.

Key words: chaos; image encryption; bit-level image; permutation; diffusion

1 引言

图像加密是信息安全保护的核心技术,然而传统的加密算法(如 DES, AES, IDEA 和 RSA 等)很难适用于图像加密的实际需求,近年来兴起的混沌加密方式已成为网络信息安全的研究热点.

混沌系统具有对初始条件和混沌参数非常敏感以及生成的混沌序列具有非周期性和伪随机性的特性,非常适用于图像加密. 自从英国数学家 Matthews 提出混沌数据加密的思想以来^[1],人们提出了多种基于混沌的图像加密算法,主要有图像位置置乱^[2]、图像灰度值替代^[3],以及位置置乱与灰度值替代相结合的加密^[4-5]三大类图像加密算法,但是现有的图像加密算法基本上是基于像素值的研究,而基于位级图像的加密研究甚少,即使有些文献涉及

位级图像混沌加密,但是存在诸如混沌系统维数较低而造成的安全性不高^[6]、Arnold 变换中图像矩阵行列大小一致的限制^[7]、难以抵抗已知/选择明文攻击^[8]等局限性,加密算法有待进一步改进与完善.

本文利用混沌信号的优良特性,结合位级图像的内在特点,采用位级图像置乱—图像像素扩散的加密方案,研究提出了一种新的位级图像混沌加密算法,测试结果表明所提算法在直方图、密钥空间、密钥敏感性、相关性和密文图像信息熵等方面具有一定的有效性和较强的保密性能.

2 位级图像与陈氏混沌系统

2.1 位级图像

对于灰度图像而言,其亮度通常量化为 0~255 的数量级. 任何像素值都可以表示为 8 bits 的形式,

收稿日期: 2013-01-19; 修回日期: 2013-03-22

基金项目: 国家自然科学基金项目(61004027, 61174066);江苏省自然科学基金项目(BK2010275);南通市应用研究计划项目(K2010017, BK2012032);江苏省高校自然科学研究项目(10KJB120002)

假设某点像素值为 $G(x, y)$, 可表示如下:

$$G(x, y) = b(8)b(7)b(6)\cdots b(1) \quad (1)$$

按照像素中 bit 的位置, 每幅灰度图像都可以划分为 8 幅位级图像. 一幅大小为 256×256 、灰度级 256 的 cameraman 图像, 可以划分为 8 幅位级图像 (PiC8 - PiC1). 从图中可以看出: bit 位数越高的位级图像与原始图像越相似, 因为像素中不同 bit 含有的信息量不同, 例如某像素点中最高位的 '1' 表示 $128(2^7)$, 而最低位的 '1' 只表示 $1(2^0)$; 另外原始图像的相邻位级图像之间具有很强的相关性, 例如 PiC8 与 PiC7 位级图像对应位置的值相反, 其差异率达到 73.75%, 因此需将原始图像的 8 幅位级图像作为一个整体进行处理.

2.2 Chen's 系统

Chen's 系统由香港城市大学的陈关荣教授首次于 1999 年提出^[5], 其形式表示如下:

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy \\ \dot{z} = xy - bz \end{cases} \quad (2)$$

式中, a, b 和 c 是系统参数, 当 $a = 35, b = 3$ 和 $c \in [20, 28.4]$ 时, 系统具有混沌特性, 其混沌吸引子见图 1. 众所周知, 初值 (x_0, y_0, z_0) 和参数 (c) 可选作为混沌系统的密钥.

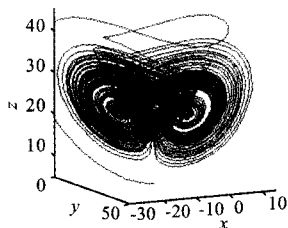


图 1 陈氏系统的混沌吸引子

3 位级图像混沌加密算法

3.1 算法概述

算法采用先置乱再扩散的结构: 首先将明文图像划分为 8 幅位级图像并将其作为一个整体, 利用 Chen's 系统产生混沌序列, 分别进行行、列置乱, 该置乱操作可执行 m 轮; 然后将置乱图像的像素值进行加密运算以满足扩散性能, 整个置乱—扩散操作执行 n 轮.

3.2 位级图像置乱

为了不失普遍性, 我们假设明文灰度图像 I 的大小为 $M \times N$, 其位级图像的置乱算法如下:

(1) 将明文图像 I 划分为 8 幅位级图像 (PiC8 - PiC1, 大小均为 $M \times N$), 然后将 8 幅位级图像组合

为一个整体, 并将其转换为大小为 $2M \times 4N$ 的矩阵 (PI), 其形式表示为

$$PI = \begin{bmatrix} \text{PiC7} & \text{PiC5} & \text{PiC3} & \text{PiC1} \\ \text{PiC8} & \text{PiC6} & \text{PiC4} & \text{PiC2} \end{bmatrix}_{2M \times 4N}$$

(2) 将 Chen's 混沌系统 (见式 (2)) 迭代 N_0 次, 其中系统初值 (x_0, y_0, z_0) 的取值与矩阵 (PI) 有关; 继续迭代陈氏混沌系统, 得到混沌序列 $X = \{x_1, x_2, x_3, \dots, x_{2M-1}, x_{2M}\}$ 和 $Y = \{y_1, y_2, y_3, \dots, y_{2N-1}, y_{2N}\}$; 然后将混沌序列 (X, Y) 进行升序排列, 得到新的混沌序列 $(\bar{X}, \bar{Y})$ 以及对应的排序序列 (T_X, T_Y) .

(3) 按照排序序列 T_X 对矩阵 PI 进行行置乱, 即将矩阵 PI 的第 T_{X1} 行移至第一行, 将第 T_{X2} 行移至第二行, $\dots$, 将第 T_{X2M} 行移至最后一行; 然后将行置乱后的矩阵按照排序序列 T_Y 进行列置乱.

(4) 将系统初值 (x_0, y_0, z_0) 赋值为 $(x_{2M+1}, y_{4N+1}, z_0)$, 重复 $m-1$ 轮行、列置乱 (步骤 2 和 3).

(5) 根据位级图像所在置乱矩阵中的位置, 得到置乱后的灰度图像, 其中某点像素值为 $G'(x, y)$, 可表示为

$$G'(x, y) = b'(8)b'(7)b'(6)\cdots b'(1) \quad (3)$$

3.3 图像像素扩散

位级图像置乱的作用不仅能改变像素的位置, 而且能修改像素值, 但是其抵抗差分攻击性能有待改进. 在所提图像像素扩散方案中, 将置乱图像进行 Z 字扫描形成一维序列 $P = \{P_1, P_2, P_3, \dots, P_{M \times N-1}, P_{M \times N}\}$. 任一像素按序进行如下操作:

$$C_i = (P_i + C_{i-1} + XX_i) \bmod 256 \quad (4)$$

式中, P_i 和 C_i 分别为置乱后图像、扩散后图像的像素值, XX_i 为由 Logistic 混沌系统产生的混沌序列进行适当处理而得, 描述如下:

$$\begin{cases} xx_{i+1} = \mu \cdot xx_i \cdot (1 - xx_i) \\ XX_i = \lfloor (xx_i \times 10^6) \bmod 256 \rfloor \end{cases} \quad (5)$$

同时, C_0 设置为 $\lfloor xx_0 \cdot 10^4 \rfloor \bmod 256$. 从式 (3) 中可看出, 图像像素扩散 C_i 不仅与 P_i 和 XX_i 有关, 而且与前一个扩散值 C_{i-1} 有关, 因此即使是 1 bit 的小小改变, 也会使接下来的扩散值发生变化.

3.4 图像解密

图像解密是“位级图像置乱—图像像素扩散”这一图像加密的逆过程, 即首先进行像素扩散 (见式 (6)), 再进行位级图像置乱, 同时在置乱中先列再行重新排序. 图像加、解密过程中的密钥必须一致, 否则解密恢复图像为无用信息.

$$P'_i = (C'_i - C'_{i-1} - XX'_i) \bmod 256 \quad (6)$$

4 性能分析

本节对所提的位级图像混沌加密算法进行测试仿真和性能分析,同时与其余图像加密算法进行比较,包括:像素级置乱—扩散加密算法(Pixel-Level Permutation and Diffusion, PLPD)、二维循环移位加密算法(Two-Dimension Circulation Encryption Algorithm, TDCEA)和位级图像置乱算法(Bit-Level only Permutation BLP).在算法仿真中,设 Logistic 混沌系统初值 $xx_0=0.123\ 45$, Chen's 混沌系统初值 $z_0=1.123\ 456$, x_0 和 y_0 与位级图像的 bit 分布有关:

$$\begin{cases} x_0 = 0.3 + \sum_{i,j}^{2M,4N} \left[\frac{PI(i,j)}{(80 \times M \times N)} \right] \\ y_0 = -0.4 + \sum_{i,j}^{2M,4N} \left[\frac{(8 \times M \times N - PI(i,j))}{(80 \times M \times N)} \right] \end{cases} \quad (7)$$

同时设定混沌系统参数 $c=26$, 迭代初始次数 $N_0=50$, 轮数 $m=1, n=1$.

4.1 直方图分析

图像直方图显示了像素值的分布情况,理想的直方图是均匀分布的,以抵抗攻击者从中获取相关的图像信息.图 2(a)和(b)为原始 Cameraman 图像及其直方图,图 2(c)和(d)为经过位级图像混沌加密后的密文图像及其直方图,从中可以看出:加密后的密文图像杂乱无章,同时其直方图分布均匀,攻击者无法从中获得任何有用信息.进一步测试发现,PLPD 密文直方图也比较理想,而 TDCEA 和 BLP 密文直方图如图 2(e)和(f)所示分布不均匀,有待进一步提高.

4.2 密钥空间及密钥敏感性分析

所提算法的密钥主要包括 Chen's 混沌系统的初值(x_0, y_0, z_0)、参数(c)以及 Logistic 混沌系统的初值(xx_0).其中混沌系统的任一初值敏感度均达到 10^{-16} ,那么密钥空间至少达到 10^{-64} ,这足以抵抗穷恶意举攻击.仍以 Cameraman 图像为例,当仅改变加密密钥 z_0 ,将其修改为 $z_0=1.123\ 456\ 000\ 000\ 000\ 1$,进行位级图像混沌加密得到密文图像(见图 3a),将此图与图 3(c)对比,得到差异图像为图 3(b),可见算法对加密密钥的敏感性很高;解密时,当加、解密密钥一致时会恢复出原始图像,如图 3(c)所示,当加、解密密钥不一致的时候,即使是细微的差别,如仅仅改变解密密钥 $z_0=$

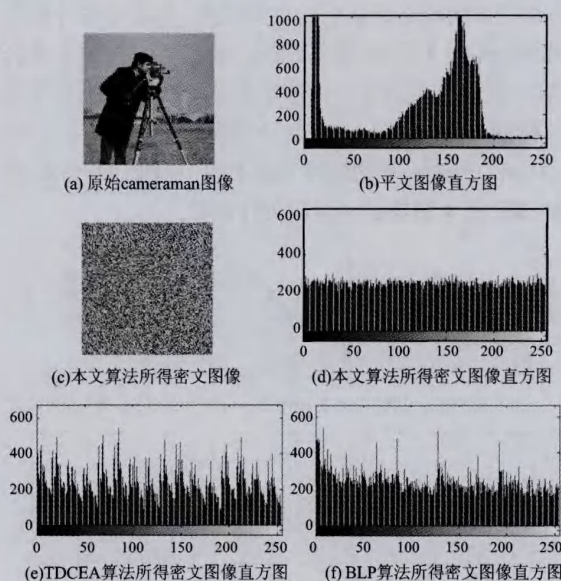


图 2 明文图像、密文图像的直方图

1.123 456 000 000 000 1(对应的加密密钥为 $z_0=1.123\ 456$),解密图像如图 4(d)所示,为毫无价值的无用信息.

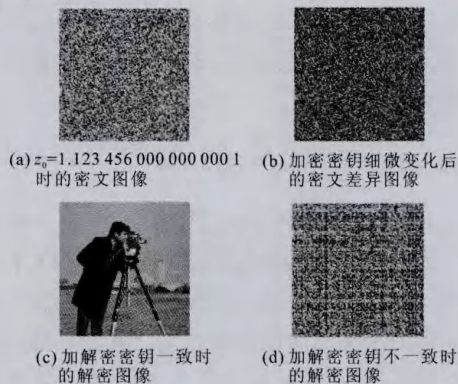


图 3 密钥敏感性分析图

4.3 相关性分析

通过下式计算水平、垂直和对角线方向相邻像素的相关性:

$$\text{cov}(x, y) = E((x - E(x))(y - E(y))) \quad (8)$$

$$R_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)} \cdot \sqrt{D(y)}} \quad (9)$$

式中, x, y 是图像中两相邻像素的像素值, $E(x)$ 是 x 的数学期望, $D(x)$ 是 x 的方差, $\text{cov}(x, y)$ 是 x, y 的协方差. 原始图像中相邻像素的相关性是很大的,为了抵抗统计攻击,必须是相邻两个像素的相关性降低,相关系数越小说明加密性能越好.仍以 Cameraman 图像为例,随机选择 2 500 个像素点进行相关性分析,图 4 所示分别为原始图像和加密图像水平、垂直、

对角线方向相邻像素点的相关性图. 为了定性分析原始图像和密文图像相邻像素点的相关性,按照上述公式进行计算,得到密文图像水平、垂直、对角线相邻像素点的相关性分别为-0.009 2,-0.015 6和-0.013 2,进一步测试发现其均小于 PLPD、TDCEA 和 BLP 密文图像的相应相关性系数.

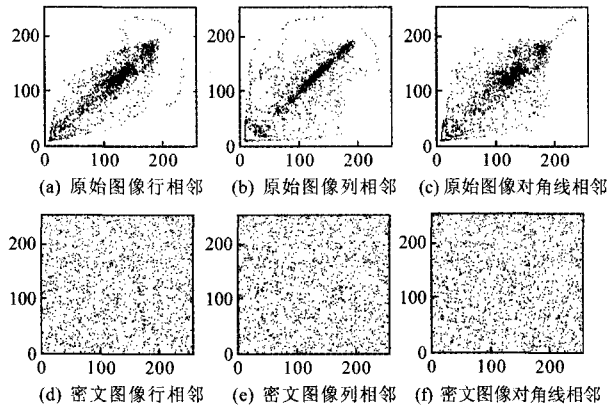


图 4 明文图像、密文图像相邻像素点的相关性图

4.4 信息熵分析

在对称加密系统中,信息熵是衡量加密效果的标准之一.信息源 m 的信息熵 $H(m)$ 可由式(9)计算,那么对于密文图像而言,8 bits 长度像素的信息熵理想值为 8.

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \log \frac{1}{p(m_i)} \tag{10}$$

以 Cameraman 和 Lena 图像为例,表 1 中分别给出了所提算法和对比算法 (PLPD、TDCEA 和 BLP)所得密文图像的信息熵,从中可以看出经所提算法加密的密文图像信息熵大于经其余算法加密的密文图像信息熵,且更接近于 8,由此可见该算法的加密效果明显优于其他对比算法.

表 1 密文图像的信息熵比较

Image	Proposed scheme	PLPD	TDCEA	BLP
Cameraman	7.997 1	7.996 8	7.756 6	7.949 9
Lena	7.997 4	7.996 9	7.911 1	7.966 5

5 结束语

本文利用混沌信号的优良特性,结合位级图像

的内在特点,采用位级图像置乱—图像像素扩散的加密方案,研究提出了一种新的位级图像混沌加密算法,然后对所提算法进行测试仿真和性能分析,同时与其他图像加密算法 (如 PLPD、TDCEA 和 BLP)进行比较,测试结果表明所提算法在直方图、密钥空间、密钥敏感性、相关性和密文图像信息熵等方面具有更好的加密性能,以此验证所提算法具有较强的保密性和有效性.

参考文献:

[1] Matthews R. On the derivation of a chaotic encryption algorithm[J]. Cryptologia, 1989(1):29-42.

[2] 高恩婷,刘家胜. 基于 M 序列的数字图像置乱方法[J]. 微电子学与计算机, 2009,26(6):171-174.

[3] 刘家胜,黄贤武,朱灿焰,等. 基于模运算与混沌映射的图像加密算法的研究[J]. 微电子学与计算机, 2006, 23(12):206-209.

[4] 盛苏英,吴新华. 一种混沌图像加密算法的研究与改进[J]. 微电子学与计算机, 2010, 27(10):61-65.

[5] Wang Y, Wong K W, Liao X F, et al. A chaos-based image encryption algorithm with variable control parameters[J]. Chaos Soliton Fractals, 2009, 41(4): 1773-1783.

[6] Zhang H, Cai R. Image encryption algorithm based on bit-plane scrambling and multiple chaotic systems combination[C]//2010 International Conference on Intelligent Computing and Integrated Systems (ICISS). Guilin, 2010:113-117.

[7] Zhang W, Wong K W, Yu H, et al. A symmetric color image encryption algorithm using the intrinsic features of bit distributions[J]. Communications in Non-linear Science and Numerical Simulation, 2013, 18(3): 584-600.

[8] Chen H C, Guo J I, Huang L C, et al. Design and realization of a new signal security system for multimedia data transmission[J]. EURASIP Journal on Applied Signal Processing, 2003(13):1291-1305.

作者简介:

吴新华 男,(1980—),硕士,教师.研究方向为混沌加密.