文章编号: 1007- 2985(2008) 05- 0039- 03

基于 Lorenz 混沌系统的图像加密算法*

刘振华
(长沙航空职业技术学院, 湖南 长沙 410014)

摘 要: 提出了一种基于 Lorenz 混沌系统的图像加密算法, 实验表明该算法具有较强的抵御穷举攻击、统计攻击、已知明文攻击能力, 算法安全性高.

关键词: 混沌; Lorenz; 图像加密; 替代; 置乱
中图分类号: TP393.08 文献标识码: A

随着 Internet 技术与多媒体技术的飞速发展, 多媒体通信逐渐成为人们进行信息交流的重要手段, 因此信息的安全与保密通信显得越来越重要[1]. 混沌加密采用迭代的方式生成密钥序, 生成速度较快, 可以很好地满足图像加密的适时性要求.

1 Lorenz 混沌系统

Lorenz 系统是经典的三维混沌系统[2], 以 Lorenz 系统生成加密混沌序列有 3 大优点[3-4]: 一是系统结构较低维系统复杂, 系统变量的实数值序列更不可预测; 二是对系统输出的实数值混沌序列进行处理, 可产生单变量或多变量组合的加密混沌序列, 使得加密序列的设计非常灵活; 三是系统的 3 个初始值和 3 个参数都可以作为生成加密混沌序列的种子密钥, 若设计过程中再加入部分控制变量, 加密算法的密钥空间将大大高于低维混沌系统. Lorenz 系统的动力学方程为:

$$\begin{cases} \mathrm{d}x/\mathrm{d}y = \sigma(y - x), \\ \mathrm{d}y/\mathrm{d}t = rx - zx - y, \\ \mathrm{d}z/\mathrm{d}t = xy - bz. \end{cases} \quad (1)$$

2 算法设计

2.1 图像像素值替代加密算法设计

设 $I_{M\times N}$ 表示大小为 $M \times N$ 的图像, $I(x, y)(x \in [0, M-1], y \in [0, N-1])$ 表示图像 I 在点 (x, y) 处的灰度值, $I'(x, y)(x \in [0, M-1], y \in [0, N-1])$ 表示 (x, y) 经过加密后所对应的灰度值. 图像的像素值替代加密算法设计如下.

(ⅰ) 在图像 I 中随机选择 12 个像素点, 将其以 2 个为一组进按比特位异或操作, 得到 3 个 32 位数字 k_1, k_2, k_3 作为辅助密钥.

(ⅱ) 选择精度为 32 位的初值 x_0', y_0', z_0', 与辅助密钥 k_1, k_2, k_3 分别进行异或操作得到 $x_0 = x_0' \oplus$

* 收稿日期: 2008- 04- 23
基金项目: 湖南省自然科学基金资助项目(06JJ50098)
作者简介: 刘振华(1982-), 男, 湖南沅江人, 长沙航空职业技术学院助理实验师, 主要从事网络网络安全研究.

$k_1, y_0 = y'_0 \oplus k_2, z_0 = z'_0 \oplus k_3$, 作为(1)式的初始值, 生成长度都为 $L(L = M \times N, M \times N$ 为图像的大小)的混沌序列 x', y', z'.

(iii) 将 x', y', z' 这 3 个混沌序列以 0.5 为阈值二值化为 0, 1 序列 x, y, x.

(iv) 将 x, y, z 这 3 个序列进行异或生成一个序列 M, 即密钥序列.

(v) 将原始图像中各像素点的灰度值 $I(x, y)$ 与序列 M 产生的混沌密钥序列值进行异或操作, 得到加密后的像素灰度值 $I'(x, y)$.

(vi) 重复步骤(v), 将所有像素点加密, 即完成图像像素值的替代加密.

2.2 图像像素位置置乱加密算法设计

只经过像素值的替代加密, 很容易分析出加密算法而受到已知明文的攻击, 因此需要进一步对像素替代后的加密图进行置乱, 才能有效提高图像的保密性. 采用如下方法对图像进行像素位置的置乱.

(i) 选定初值 x_0, y_0, z_0 和参数 σ, r, b 及积分步长, 分别代入(1)式, 产生 3 个混沌序列 x', y', z'. 在这 3 个序列中随便选择 2 个序列, 分别为 x, y 序列.

(ii) 按(2)式的方式将经过替代加密后的图像中位置为 (i, j) 的像素点置换到位置 (i', j'), 若值相同则舍去, 重新生成新值:

$$i' = (i + x_{(i\times j+j)}) \times z \bmod M, j' = (j + y_{(i\times j+j)}) \times z \bmod N. \quad (2)$$

(iii) 循环步骤(ii), 直到所有的点都被置换, 完成图像的像素位置置乱.

3 实验结果与讨论

利用 Matlab7.0 平台, 取 256×256 Lena 彩色图像进行实验($N = 256$). Lorenz 混沌系统的系统参数和初值分别为: $\sigma = 10, r = 28, b = 8/3$; $x_0 = 0.11, y_0 = 1.02, z_0 = 0.1$. 系统演化时间区间为[0, 850]. 采用变步长的四阶五级 Runge-Kutta-Felhberg 算法解微分方程(1), 用于图像像素的替代加密. 取以下值用于图像像素置乱加密: $\sigma = 10, r = 28, b = 8/3$; $x_0 = 0.12, y_0 = 1.03, z_0 = 0.2$.

(1) 加密效果如图 1 所示.

a 原始图像 b 加密后图像

图 1 加密效果图

由实验结果可知, 加密后的图像无法辨认, 说明此方法加密效果良好.

(2) 统计分析. 从图 2 可以看出, 加密前后图像的直方图发生了较大的变化, 和原图像相比, 加密后图像的像素值在[0, 255]区间内分布比较均匀, 因此该系统能够较有效地抵御统计攻击.

(3) 相邻像素点的相关性分析. 从图 3 可以看出, 原始图像的点主要分布在对角线上, 相邻像素点具有高度相关性; 而密文图像相邻像素点的相关性接近 0, 可以有效抵御已知明文攻击.

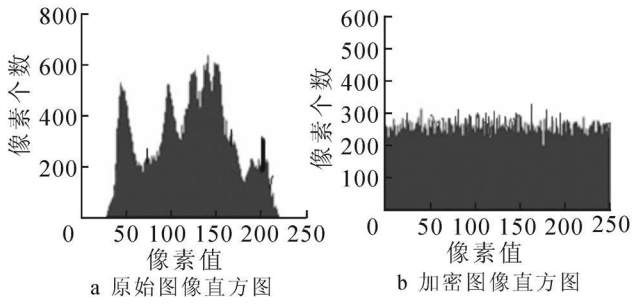

图 2 图像直方图

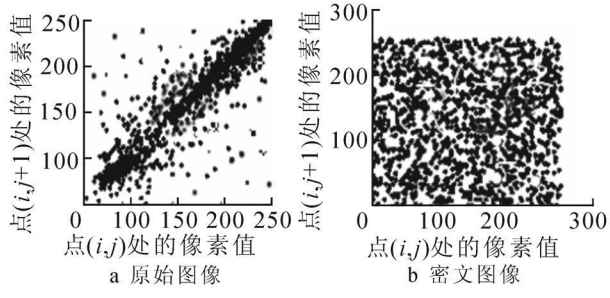

图 3 图像水平方向相邻像素点的相关性

4　结语

提出来了基于 Lorenz 系统的图像加密算法, 算法具有以下主要优点: (1) 替代和置乱均采用高维混沌系统, 克服了一维混沌系统不能抵御相空间重构攻击的缺点; (2) 以三维混沌系统实数初值为密钥, 密钥空间大, 引进 3 个辅助密钥, 大大拓展了密钥空间, 采用混沌系统产生的多个序列二值化后异或, 将各个混沌序列的初值作为密钥, 增加了密钥的长度, 增大了密钥空间, 使算法具有抵御穷举攻击的能力; (3) 混沌系统具有复杂的非线性混沌行为, 因此生成的密钥具有较高的复杂性, 且每次随机产生的密钥不同, 具有一次一密特性; (4) 密文具有在整个取值空间均匀分布的特性, 相邻像素具有近似于 0 的相关性.

参考文献:

[1] CHENG HOWARD, LI Xiao-bo. Partial Encryption of Compressed Images and Videos [J]. IEEE Transcations on Signal Processing, 2000, 48(8): 2 439- 2 551.

[2] 胡满峰, 徐振源. Lorenz 混沌系统的非线性反馈错位同步控制 [J]. 系统工程与电子技术, 2007, 29(8): 136- 138.

[3] 王　英, 郑德玲, 鞠　磊. 基于 Lorenz 混沌系统的数字图像加密算法 [J]. 北京科技大学学报, 2004, 26(6): 42- 43.

[4] 王东生, 曹　磊. 混沌、分形及其应用 [M]. 合肥: 中国科学技术大学出版社, 1995.

Image Encryption Algorithm Based on Lorenz Chaotic System

LIU Zhen-hua

(Changsha Aeronautical Vocational and Technical College, Changsha 410014, China)

Abstract: It proposed one kind of image encryption algorithm according to the Lorenz chaotic system. The experiment showed that the algorithm has stronger resistance for the exhaustion, count attack, the known-plaintext attack. The security of the algorithm is high.

Key words: chaotic; Lorenz; image encryption; confusion; diffusion

(责任编辑　向阳洁)

(上接第 38 页)

Framework of the Distributed Coordination Intrusion Detection System Based on the Ring Structure

JIANG Hua-bin

(Hunan Vocational College of Commerce, Changsha 410205, China)

Abstract: Through analyzing the characteristics and the cooperating mode of the present Distributed Intrusion Detection System (DIDS), this paper proposes a kind of architecture based on Ring Distributed Coordinated Intrusion Detection System (RDCIDS). Furthermore, it expatiates on the event-generator, and event-analyzer, event-responder of the DIDS; adopts the protocol analysis, the data analysis, command interpreter and cooperate processor. It provides more convenience for the RDCIDS and overcomes the defects such as complicated structure and load imbalance in each subsystem of the present distributed intrusion detection system.

Key words: ring; distributed intrusion detection; system; framework

(责任编辑　向阳洁)