Computer Science and Application 计算机科学与应用, 2016, 6(9), 565-572
Published Online September 2016 in Hans. http://www.hanspub.org/journal/csa
http://dx.doi.org/10.12677/csa.2016.69070

Hans汉斯

Bit-Level Color Digital Image Encryption Algorithm Based on Lorenz Chaotic System

Jingjing Huang, Qinghua Wang, Zhenhua Li

Nanjing University of Science and Technology, Nanjing Jiangsu
Email: 823223165@qq.com

Received: Sep. 8th, 2016; accepted: Sep. 23rd, 2016; published: Sep. 29th, 2016

Abstract

In this paper, we present a bit-level color digital image encryption algorithm based on Lorenz chaotic system. Firstly the red, green and blue components of each pixel are encrypted by the x, y, z three dimensional chaotic sequences generated by the Lorenz Chaotic System, respectively, and then they are merged into the whole. In the process of encryption, each decimal pixel value is treated as an eight bit binary number and is permuted by the ascending order position index chaotic sequence so as to achieve the purpose of pixel fusion and image encryption. The experimental results and security analysis show that the algorithm is a good encryption with better effects and can ensure adequate safety of the color image.

Keywords

Chaos, Bit-Level, Image Encryption Algorithm

一种基于Lorenz混沌系统的比特级彩色图像加密算法

黄晶晶，王清华，李振华

南京理工大学，江苏 南京
Email: 823223165@qq.com

收稿日期：2016年9月8日；录用日期：2016年9月23日；发布日期：2016年9月29日

文章引用: 黄晶晶, 王清华, 李振华. 一种基于 Lorenz 混沌系统的比特级彩色图像加密算法[J]. 计算机科学与应用, 2016, 6(9): 565-572. http://dx.doi.org/10.12677/csa.2016.69070

摘　要

定本文提出了一种基于Lorenz混沌系统的比特级彩色数字图像加密算法，针对彩色数字图像的三个分量R、B、G，用Lorenz混沌系统产生的x、y、z三个维度的混沌序列分别进行加密，最后再合而为一。加密时，把每一个十进制的像素值看成是八位二进制数，利用混沌序列的升序排列位置索引进行置乱，达到像素融合的目的，实现图像的加密。加解密数值实验和算法的有效性安全性分析，说明该算法安全有效，具有较高的抗攻击能力。

关键词

混沌，比特级，加密算法

1. 引言

数字图像信息作为一种最直观的信息形式，在互联网的传播中发挥着非常重要的作用，数字图像的安全传递引起了越来越多的人关注[1]。

传统的加密技术在只能针对文本信息等数据量不大的情况，而数字图像数据呈二维分布，冗余量大，数据量复杂，传统的加密方式针对数字图像信息加解密效率一直不理想。近半个世纪以来，混沌系统的研究是非线性领域一个重要的课题[2]，鉴于混沌系统的特征和加密算法要求的特征有诸多的共性[3]，学者们开始将混沌运用到加密算法中。本文选用了较高维度的 Lorenz 系统，提出了一种基于 Lorenz 混沌系统的比特级加密方式。

2. Lorenz 混沌系统

Lorenz 混沌系统是一个经典的三维混沌系统，相对于其他低维系统而言，Lorenz 混沌系统具有显著优势[4]。其动力学方程为：

$$\begin{cases} \dfrac{\mathrm{d}x}{\mathrm{d}t} = \sigma(y - x) \\ \dfrac{\mathrm{d}y}{\mathrm{d}t} = rx - zx - y \\ \dfrac{\mathrm{d}z}{\mathrm{d}t} = xy - bz \end{cases} \tag{1}$$

其中，σ, r, b 为系统参数，x, y, z 为状态变量，一般取 $\sigma = 10, b = 8/3$，r 作为系统控制参数，在保持 σ, b 不变时 $r > 24.47$ 时 Lorenz 系统进入混沌状态[5]。

对 Lorenz 系统进行数值求解时，典型算法有两种[6]，一种是一阶欧拉法，另一种是四阶－五阶龙格库克(Ruuge-Kutta)法。四阶－五阶龙格库克(Ruuge-Kutta)法的计算精度远高于一阶欧拉法，但是计算时间也就相对来说比较长，而本算法对求解结果的精确值并没有太高的要求，所以我们采用了耗时较短的一阶欧拉法。

3. 加密解密算法

加密过程一般包括像素融合和像素置乱，两者紧密结合才能使加密效果更加完善[7]。本文采用比特级的加密方式，对比特级数值进行位置索引置乱，效果上可以达到像素融合的目的。算法如下：

Step 1，将原始彩色图像，分成三个关于 R,G,B 的灰度图，然后对每一个灰度图做如下处理：将图像的像素值二维矩阵由 L 行 R 列转换成 $L\times R$ 行一列的形式，每一行有一个十进制数，表示一个像素值。

Step 2，把三个灰度图的每一位像素值由十进制化成二进制形式，像素值在区间(0,255)上，所以每个十进制像素值由八位二进制数表示，不足八位的高位由 0 补齐。具体换算公式为：

$$\begin{cases} x_i = y_i \bmod 2 \\ y_{i+1} = \left[y_i / 2 \right] \end{cases} \tag{2}$$

其中 $i = 1,2,\cdots,8$，x_i 表示二进制数的第 i 位(第一位为最低位)，y_i 是原始像素值，$\left[y_i / 2 \right]$表示除以 2 再取整。

我们把每一位二进制数看成是一个数，换算过后由十进制数表示的 $L\times R$ 行一列的矩阵就变成了 $L\times R$ 行八列的形式。

Step 3，将 $L\times R$ 行八列的矩阵继续整形成 $L\times R\times 8$ 行一列的形式。

Step 4，代入初始值，用一阶欧拉法解 Lorenz 方程生成混沌序列，在做下式变化[8]：

$$x_k(i) = 100x_k(i) - round\left(100x_k(i)\right) \tag{3}$$

即序列每一个数乘以 100，再取小数部分，舍弃前面一部分结果，避免初值造成的影响，最终得到的序列记作 $\{A_i, i = 1,2,\cdots, L\times R\times 8\}$，其中 $L \times R$ 是需要加密的图像的大小，三个灰度图对应的序列分别如上记为 A_i, B_i, C_i。

Step 5，对混沌序列 A_i, B_i, C_i 分别进行排序，得到位置索引，根据位置索引对上述三个 $L\times R\times 8$ 行一列形式的矩阵进行置乱。

Step 6，对置乱后的三个 $L\times R\times 8$ 行一列形式的矩阵做第一步到第三步的逆操作。即先由 $L\times R\times 8$ 行一列形式整形成 $L\times R$ 行八列的形式；再把 $L\times R$ 行八列矩阵每一行的八个数看成是二进制的每一位合并成一个二进制数，将这个二进制数换算成一个十进制数，$L\times R$ 行八列的矩阵变成 $L\times R$ 行一列；然后将 $L\times R$ 行一列的矩阵还原成 L 行 R 列的形式，最后将三幅图合成一副彩色图，即为最终的加密图像。

解密过程是加密过程的逆运算。

4. 数值模拟

选取彩色图像 lena 作为测试图像，在 MATLAB2012 环境下编程实现算法。密钥选择 $x_0 = 0.11$，$y_0 = 1.02$，$z_0 = 0.1$，$r = 28$，步长 $h = 0.01$，lorenz 方程迭代次数 $n = 8\times L\times R + 1000$ 次，舍弃前 1000 次迭代结果，避免初值产生的影响，得到如图 1 所示，其中图(a)表示原图像，(b)表示加密图像，(c)表示解密图像。从图像中我们可以看出，加密图像完全掩盖了原图像的信息，加密效果良好，解密图像与原图像基本一致，解密不失真。

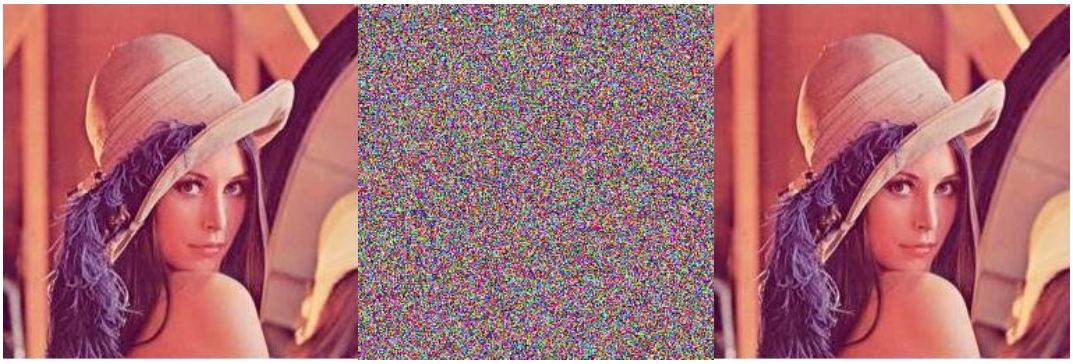
5. 算法的有效性和安全性分析

5.1. 灰度直方图分析

一个好的加密系统必须要具备抗统计攻击的能力，灰度直方图是衡量图像统计性能的一个重要指标[9]。如图 2 所示，加密后的图像直方图(b)趋于平坦，像素值分布比较均匀，完全掩盖了原图像素值的统计特征，可以一定程度上抵抗统计攻击。

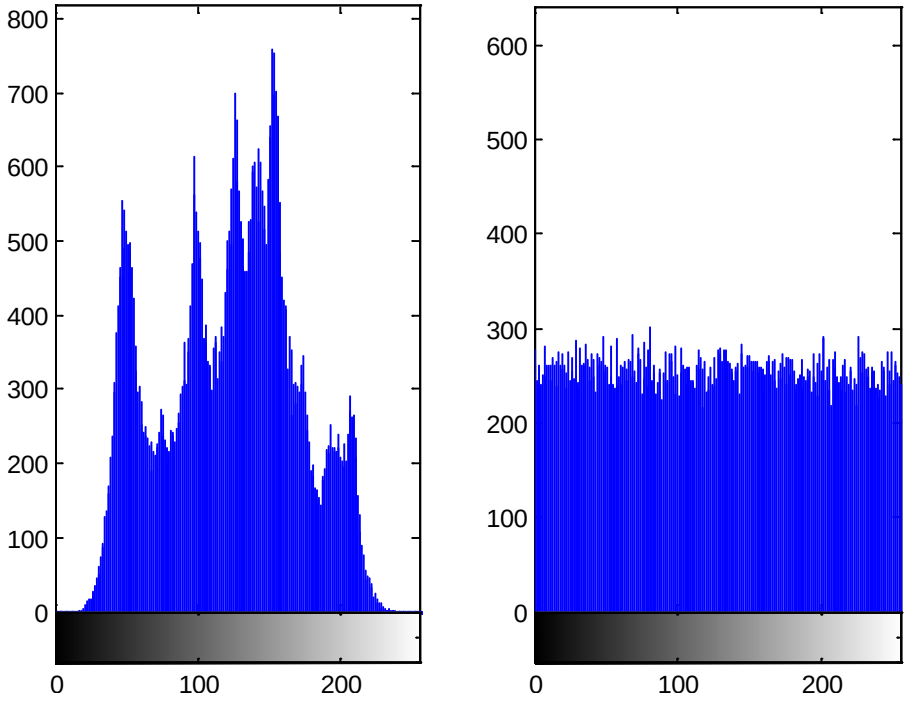
5.2. 相邻像素相关性分析

相邻像素相关性强是数字图像的重要统计特征之一，加密系统应该具有破坏相邻像素相关性强的能力。



(a) 原图像 (b) 加密图像 (c) 解密图像

Figure 1. Encryption decrypted image
图 1. 加密解密图像



(a) 加密前 (b) 加密后

Figure 2. The gray value histogram of the images encrypted before and after
图 2. 加密前后图像灰度值直方图

在测试图像中，随机选取 1000 对相邻的像素点对，记为(x_i, y_i),其中 x_i, y_i 分别代表第i对像素的两个像素值。按如下定义的相关系数，计算这 1000 对像素灰度值之间的线性相关系数。

$$Cov(x,y) = E\left[\left(x - E(x)\right)\left(y - E(y)\right)\right] \tag{3}$$

$$r_{xy} = \frac{\left|Cov(x,y)\right|}{\sqrt{D(x)}\sqrt{D(y)}} \tag{4}$$

式中，x，y 表示两个相邻的像素灰度值。在实际测试中用如下离散化的计算公式[10]：

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{5}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)^2 \tag{6}$$

$$Cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)\left(y_i-E(y)\right) \tag{7}$$

以相邻两像素灰度值为 x,y 坐标，得到加密前后相邻两点的相关性分析结果如图 3 (水平方向)、图 4 (垂直方向)、图 5 (对角方向)所示。可以看出，加密前的图像像素之间具有较强的相关性，经过加密过后，这种相关性已经基本被破坏了。

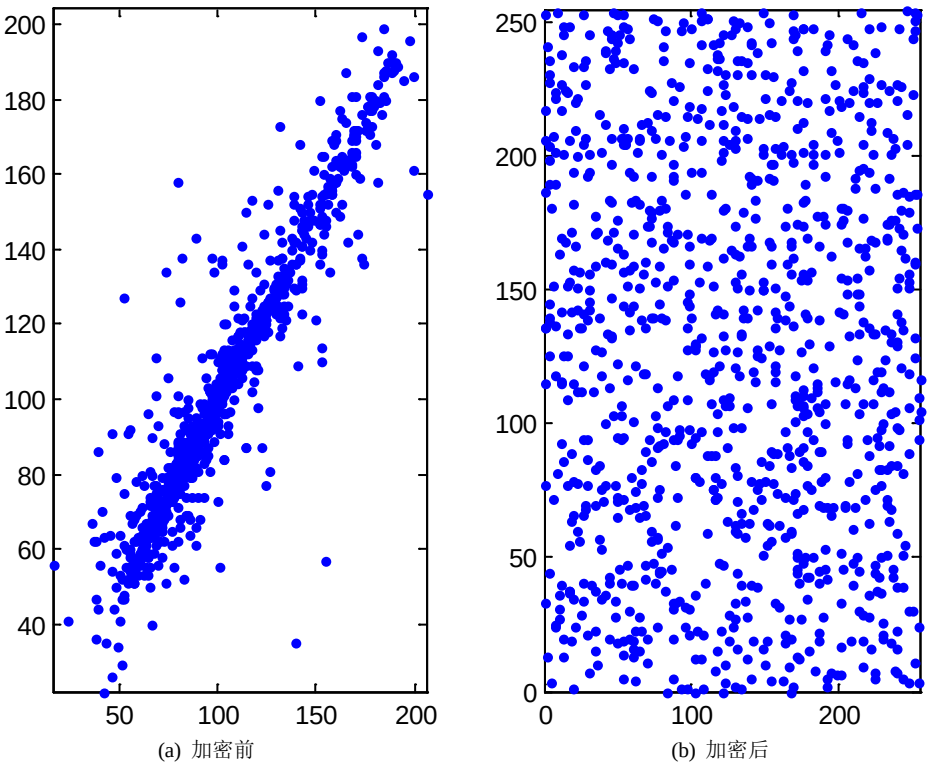
5.3. 密钥空间分析

密钥主要是由 Lorenz 混沌系统三个分量的初始值 x_0、y_0、z_0 和计算步长 h 组成。由 Lorenz 映射的特点可知，σ,b 保持不变，$r>24.47$ 时，系统进入混沌状态。密钥的四个参量均按照浮点数的最高精度 10^{-16} 计算，忽略参数的整数部分区分度，密钥的取值种类可达$(10^{15})^4$，相当于二进制密钥的 60 位，可见密钥空间相当大，足以抵抗穷举攻击[11]。

5.4. 密钥雪崩效应分析

密钥的雪崩效应是指加密算法对密钥变化的敏感性，即密钥的任意参数发生微小变化，都将导致解密错误。我们分布改变 x_0、y_0、z_0 和 h 的值，观察解密图像，考察算法对密钥的敏感度。

当参数 x_0、y_0、z_0、步长 h 分别改变 10^{-15} 的情况下，解密图像为图 6、图 7、图 8、图 9 所示，均不能正确解密，可见算法对密钥非常敏感。



(a) 加密前　　(b) 加密后

Figure 3. The correlation analysis between adjacent pixels of plaintext and ciphertext (The horizontal direction)

图 3. 明文图像和密文图像相邻两点的相关性分析结果(水平方向)

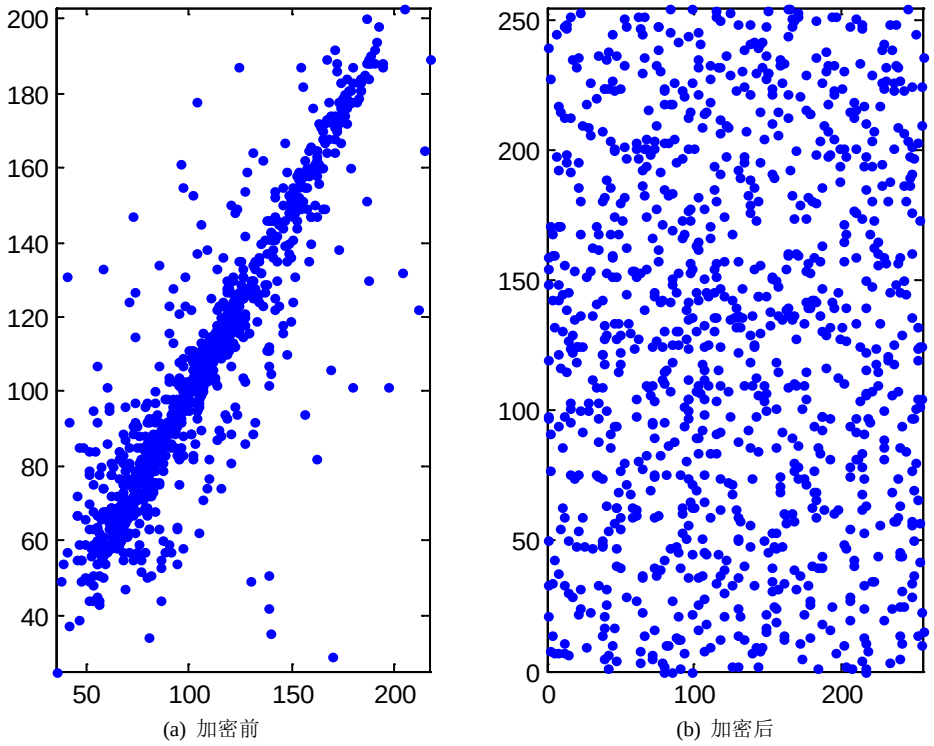


Figure 4. The correlation analysis between adjacent pixels of plaintext and ciphertext (The vertical direction)
图 4. 明文图像和密文图像相邻两点的相关性分析结果(垂直方向)

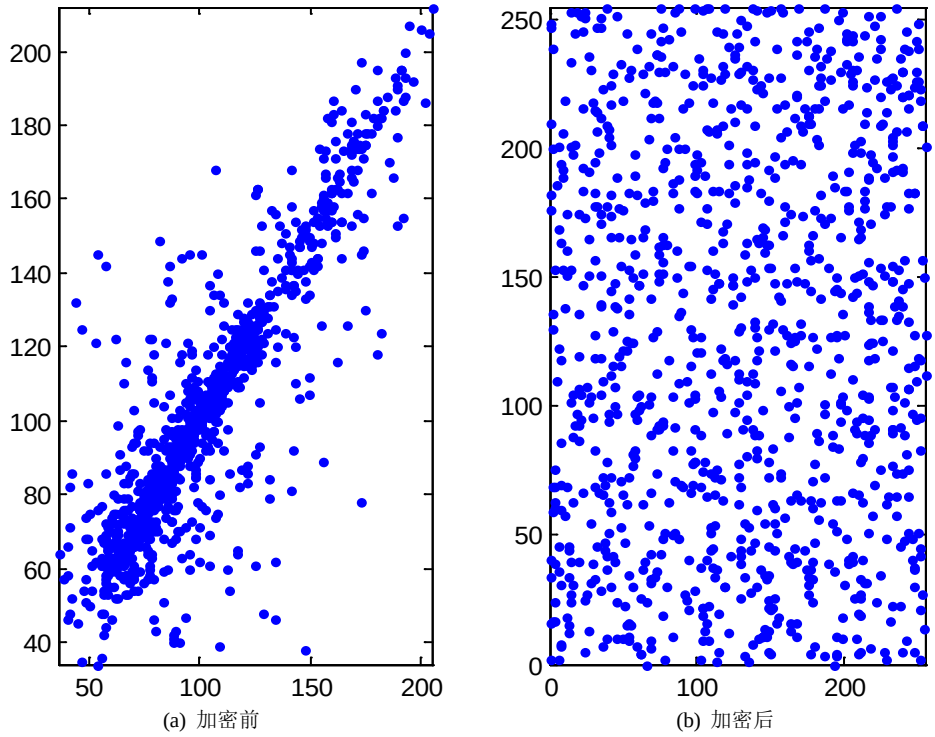


Figure 5. The correlation analysis between adjacent pixels of plaintext and ciphertext (The diagonal direction)
图 5. 明文图像和密文图像相邻两点的相关性分析结果(对角方向)

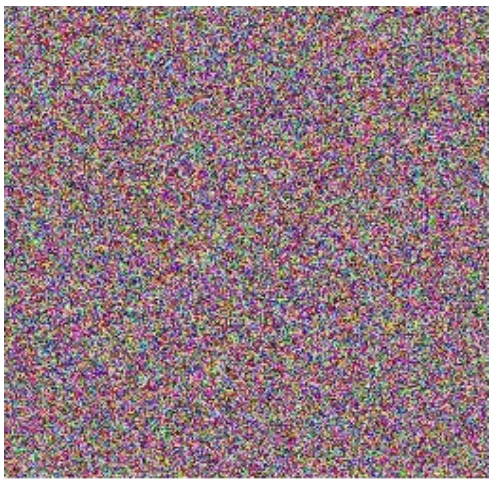


Figure 6. Ciphertext sensitivity to keyx
图 6. 密文对密钥 x_0 的敏感度

Figure 7. Ciphertext sensitivity to keyx
图 7. 密文对密钥 y_0 的敏感度

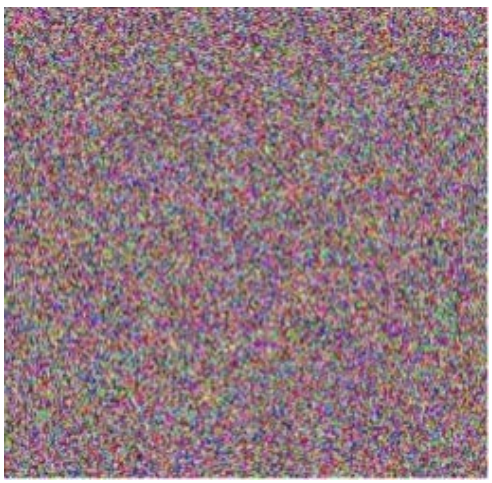


Figure 8. Ciphertext sensitivity to keyx
图 8. 密文对密钥 z_0 的敏感度

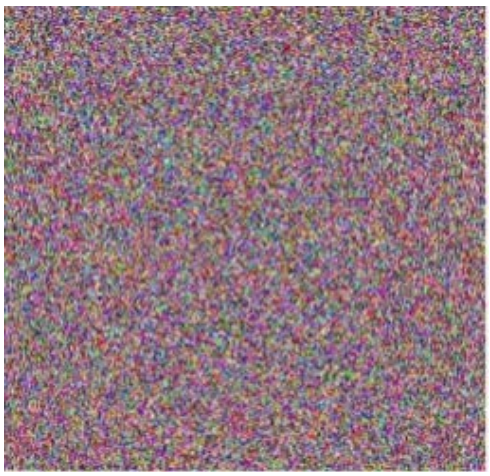


Figure 9. Ciphertext sensitivity to keyx
图 9. 密文对密钥 h 的敏感度

正确密钥 $K = (0.11,1.02,0.1,0.1)$

错误密钥 $K_1 = (0.11 + 10^{-15},1.02,0.1,0.01)$，如图 6 所示，考察算法对密钥 x_0 的敏感度

错误密钥 $K_2 = (0.11,1.02 + 10^{-15},0.1,0.01)$，如图 6 所示，考察算法对密钥 y_0 的敏感度

错误密钥 $K_3 = (0.11,1.02,0.1 + 10^{-15},0.01)$，如图 6 所示，考察算法对密钥 z_0 的敏感度

错误密钥 $K_4 = (0.11,1.02,0.1,0.01 + 10^{-15})$，如图 6 所示，考察算法对密钥 h 的敏感度

6. 总结

本文提出了一种基于 Lorenz 混沌系统的比特级彩色数字图像加密算法，对彩色数字图像的三个分量 R、G、B，分别用 Lorenz 混沌系统生产的三个状态分量 x、y、z 序列进行加密。将每一位十进制的像素值换算成八位二进制数，用混沌序列的升序排列位置索引对二进制数进行置乱，可以达到像素融合的效果。数值模拟结果表明该算法加密效果良好，不能从加密图像中提取任何原图像的有效信息，解密图像与原图像基本一致，无失真。算法的有效性和安全性分析表明，加密图像破坏了相邻像素的强相关性，均衡了原图像像素值的分布，有较强的抗统计攻击能力。密钥空间足够大，密钥对明文有明显的雪崩效应，微小的密钥差距也难以还原原图像，足以抵抗穷举攻击。

参考文献 (References)

[1] 蒋君莉, 张雪锋. 基于多混沌系统的彩色图像加密方法[J]. 计算机应用研究, 2014, 31(10): 3131-3136.

[2] 官国荣, 吴成茂, 贾倩. 一种改进 Lorenz 混沌系统构造及其加密应用[J]. 小型微型计算机系统, 2015, 36(4): 830-835.

[3] 陈关荣. 动力系统的混沌化[M]. 上海: 上海交通大学出版社, 2006.

[4] 孙志娟, 陈勇. 基于 Lorenz 三维超混沌系统的图像加密方法[J]. 微处理机, 2007, 28(3): 49-52.

[5] 林琳. 基于 Arnold 变换和 Lorenz 混沌系统的彩色图像加密算法[J]. 电子设计工程, 2014(18): 165-168.

[6] 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): 678-682.

[7] 祁燕, 刘丽萍. 标准映射和 Lorenz 混沌系统彩色图像加密算法[J]. 沈阳理工大学学报, 2014, 33(4): 40-47.

[8] 卢辉斌, 郑恒娜, 韩秀峰. 基于 Lorenz 三维混沌序列的彩色图像加密算法[J]. 电子测量技术, 2008, 31(11): 34-36.

[9] 邓金祥. 基于 Lorenz 混沌系统的图像加密算法研究[D]: [硕士学位论文]. 秦皇岛: 燕山大学, 2015.

[10] 陈关荣. 动力系统的混沌化[M]. 上海: 上海交通大学出版社, 2006.

[11] 朱薇. 基于混沌的虚拟光学图像加密关键技术研究[D]: [博士学位论文]. 南京: 南京邮电大学, 2014.