

基于 Logistic 映射和超混沌的自适应图像加密算法

李 玲¹, 王伟男¹, 李津杰¹, 江 进²

(1 重庆邮电大学 数理学院, 重庆 400065; 2 重庆邮电大学通 信与信息工程学院, 重庆 400065)

摘 要: 为了实现对图像信息的有效保护,提出了一种基于 Logistic 映射和超混沌系统的图像加密算法. 该算法主要思想是利用 Logistic 映射产生的混沌序列对明文进行像素置乱并结合超混沌以及图像自身的像素分布特征,对不同的像素点进行不同方式的像素灰度变换. 仿真实验和安全性分析表明,该算法具有较高的安全性,拥有较大的密钥空间且对密钥具有相对较高的敏感性,同时实现了“一次一密”的加密目标,可以有效地抵御穷举攻击、统计攻击以及选择明文攻击等.

关键词: Logistic 混沌映射;超混沌系统;统计攻击;选择明文攻击

中图分类号: TP391

文献标识码: A

文章编号: 1000-7180(2012)01-0042-05

Self-Adaptive Image Encryption Algorithm Based on Logistic Map and Hyper-Chaos

LI Ling¹, WANG Wei-nan¹, LI Jin-jie¹, JIANG Jin²

(1 College of Mathematics and Physics, Chongqing University Posts and Telecommunications,
Chongqing 400065, China; 2 College of Communication and Information Engineering,
Chongqing University Posts and Telecommunications, Chongqing 400065, China)

Abstract: In order to protect the information of images effectively, a novel image encryption scheme based on Logistic map and hyper-chaos system is proposed in this paper. The encryption system employs the chaotic sequence of Logistic map combining hyper-chaos to scramble the pixel matrix and make gray-level transformation. Simulation experiment and security analysis show that the suggested algorithm is of high security, a large key space, and relatively high sensitivity to secret keys. At the same time, it achieves the aim of ‘one time one key’ and can defend exhaustive attack, statistical attack and chosen-plaintext attack.

Key words: logistic map; hyper-chaos system; statistical attack; chosen-plaintext attack

1 引言

目前,随着多媒体产业和数字通信技术的快速发展,越来越多的人开始关注信息在网络传递过程中的安全性问题,因此,现在面临的的主要挑战是要有效地保证数据在网络中的机密性. 然而,传统的加密算法如 AES,SDES 等有着诸如密钥空间小、加密速度慢等明显缺陷. 因此,基于混沌系统的加密方法应运而生. 自从 1989 年 Matthews 首次提出可以利用混沌系统进行加密以来,研究人员开始越来越多

地关注基于混沌的加密算法. 对于图像加密方法来说,混沌系统是 SDES 等传统算法的有效替代选择. 混沌系统作为一种非线性动力系统,具有诸如伪随机性、无周期性、对系统初值有高度的敏感性以及遍历性等特点^[1]. 很多的图像加密算法^[2-6]通过利用混沌系统产生一个伪随机序列并据此对明文进行加密,如:文献[7]提出了一种基于一维 Logistic 映射的像素置乱方法;Fridrich^[8]提出一种利用 Baker 映射的像素置乱方法. 然而,这些单纯基于低维混沌系统的算法,具有较为简单的形式和密钥空间,难以有

收稿日期: 2011-06-03; 修回日期: 2011-07-01

基金项目: 重庆市教委科研基金(KJ100505); 重庆邮电大学自然科学基金(A2009-31)

效地抵御穷举攻击等。

超混沌系统是一种结构复杂的四维混沌系统,主要优点表现为:与低维混沌系统相比,其系统产生的序列随机性更高,系统参数更多,共有四个初值可以作为密钥,密钥空间更大。通过利用超混沌系统的优点,本文提出了一种基于一维 Logistic 混沌映射和超混沌的复合混沌图像加密新算法。该算法根据图像的自身特征通过“一次一密”的方法对明文进行像素置乱和像素灰度置换,从而增加了密文的随机性以及密码分析人员的破解难度。仿真实验分析表明,该算法具有较高的安全性,可以有效地抵御穷举攻击、统计攻击以及选择明文攻击等。

2 理论分析

2.1 Logistic 混沌映射

一维 Logistic 混沌映射可以定义如下:

$$x_{n+1} = \mu x_n (1 - x_n)$$

其中,当 $x_n \in (0, 1)$, 当 $\mu \in [3.5699456, 4]$ 时,系统处于混沌状态。且对于 Logistic 混沌映射有如下命题:

命题 1 该混沌序列的概率密度函数:

$$\rho = \begin{cases} \frac{1}{\pi \sqrt{x(1-x)}}, & 0 < x < 1 \\ 0, & \text{others} \end{cases} \quad (1)$$

命题 2 混沌序列中轨迹点的平均值:

$$\bar{x} = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{k=0}^{N-1} x_k = \int_0^1 x p(x) dx = 0.5 \quad (2)$$

命题 3 混沌序列的自相关性:

$$T(\tau) = \lim_{N \rightarrow \infty} \sum_{k=0}^{N-1} (x_k - \bar{x})(x_{k+\tau} - \bar{x}) = \int_0^1 x f^\tau(x) p(x) dx = 0 \quad (3)$$

命题 4 两个混沌序列的自相关性:

$$C(\tau) = \lim_{N \rightarrow \infty} \sum_{k=0}^{N-1} (x_k - \bar{x})(y_{k+\tau} - \bar{y}) = 0 \quad (4)$$

其中, x_0, y_0 为两个混沌序列的初值。

上述命题说明 Logistic 混沌映射具有确定性,其统计特性近似白噪声。利用系统对初值的敏感性可以获得相应的混沌序列,从而可以有效地对音频、图像等进行加密。

2.2 超混沌系统

超混沌系统的动力学方程可以描述如下:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) \\ \dot{x}_2 = -x_1 x_3 + d x_1 + c x_2 - x_4 \\ \dot{x}_3 = x_1 x_2 - b x_3 \\ \dot{x}_4 = x_1 + k \end{cases} \quad (5)$$

其中, a, b, c, d, k 作为系统参数,当 $a=36, b=3, c=28, d=-16$ 且 $-0.7 \leq k \leq 0.7$ 时,式(5)存在混沌吸引子, $k=0.2$ 时超混沌的吸引子如图 1 所示。由于超混沌系统相比低维混沌系统来说具有更多的 Lyapunov 指数和更复杂的系统结构,因此产生的超混沌序列的伪随机性也更好。

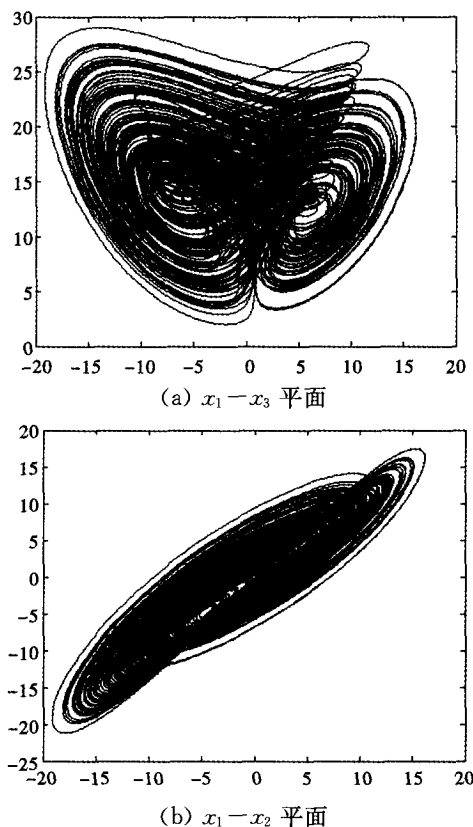


图 1 $k=0.2$ 时的超混沌吸引子

3 算法描述

3.1 算法思想

图像的像素点之间有很强的相关性,通过对明文像素矩阵进行置乱和改变像素值可以有效地降低像素之间的高度相关性,从而完成图像加密。

首先,设明文图像大小为 $M \times N$,首先给定一个初值利用一维 Logistic 映射 $\theta_{n+1} = 4\theta_n(1-\theta_n)$ 进行迭代,由于 θ 的取值范围为 $(0, 1)$, 所以将区间 $(0, 1)$ 等分成 M 个小区间,然后从小到大依次标号为 1, 2, 3... M , 然后将每次迭代得到的值落入到所分成的小区间内,进而得到该值落入的区间的区间号,并且

不停地迭代直至得到 M 个完全不同的值, 将这些数据记录为 $\{s_i, i=1, 2, 3 \cdots M\}$, 并且当 $i \neq j$ 时, $s_i \neq s_j$. 然后根据 $\{s_i, i=1, 2, 3 \cdots M\}$ 对明文进行行移动: 将第一行移动到第 s_1 行, 第二行移动到第 s_2 , $\cdots$ 直至完成整个明文的行移动得到置乱矩阵 A^r . 然后, 按照步骤 1 的方法继续迭代 $\theta_{n+1}=4\theta_n(1-\theta_n)$, 直至得到 N 个完全不同的数, 标记为 $\{t_i, i=1, 2, 3 \cdots M\}$, 并据此对矩阵 A^r 的第一行进行移动: 将第一列移动到第 t_1 列, 第二列移动到第 t_2 列, 依次进行进而完成对 A^r 的第一行移动, 然后再根据 $\theta_{n+1}=4\theta_n(1-\theta_n)$ 迭代完成对 A^r 的第二行移动, 直至完成对 A^r 的最后一行的移动, 得到置乱矩阵 A^{rc} , 至此完成了全文的像素置乱.

第二, 在对明文置乱后利用超混沌产生的混沌序列对置乱后的密文进行异或加密, 再令 $x_1=w, x_2=x, x_3=y, x_4=z$, 取四个初值 x_0, y_0, z_0, w_0 , 迭代 T_0 次, 得到 x'_0, y'_0, z'_0, w'_0 , T_0 作为密钥保存; 然后用超系统产生四组混沌序列 $\{x_k, y_k, z_k, w_k\}, (1 \leq k \leq L), L=M \times N$, 然后再根据公式进行 L 次迭代:

$$\begin{aligned} w_i &= \text{mod}((\text{abs}(w_i) - \text{floor}(\text{abs}(w_i))) \times 10^{14}, 256) \\ x_i &= \text{mod}((\text{abs}(x_i) - \text{floor}(\text{abs}(x_i))) \times 10^{14}, 256) \\ y_i &= \text{mod}((\text{abs}(y_i) - \text{floor}(\text{abs}(y_i))) \times 10^{14}, 256) \\ z_i &= \text{mod}((\text{abs}(z_i) - \text{floor}(\text{abs}(z_i))) \times 10^{14}, 256) \\ (i &= 1, 2, 3, \cdots L) \end{aligned} \quad (6)$$

初值选取为 $w_0 = -11.0431, x_0 = -7.9989, y_0 = 26.8729, z_0 = 0.1$, 得到 L 组值, 利用式(6)得到修正随机数列 M , 然后计算全图的图像像素的异或之和 s . 设 m_1, m_2, m_3 为明文的第一行前三个像素的对应的像素值, 利用公式 $w_{n+1}=4w_n(1-w_n)$ 分别迭代 M_0, N_0, P_0 次, 其中 M_0, N_0, P_0 均作为密钥保存, 带入 $w_k = \text{mod}(w_k \times 10^{14}, 256 \times 256)$, 得到三个值所对应的像素点, 设其相应像素值为 p_1, p_2, p_3 , 令 $p'_1 = \frac{p_1}{256}, p'_2 = \frac{p_2}{256}, p'_3 = \frac{p_3}{256}$, 然后将这三个值代入 $w_{n+1}=4w_n(1-w_n)$, 令

$$\begin{cases} p''_1 = \text{mod}(p'_1 \times 10^{14} + M_0, 256) \\ p''_2 = \text{mod}(p'_2 \times 10^{14} + N_0, 256) \\ p''_3 = \text{mod}(p'_3 \times 10^{14} + P_0, 256) \end{cases} \quad (7)$$

再令 $t = \text{mod}[\theta_{p_1+p_2+p_3}, 4]$.

加密方式选择如表 1 所示.

如若 $t=3$, 则选用与其相对应的加密组 (x_k, y_k, z_k) 进行加密. 然后, 再对超混沌产生的混沌序列进行修正:

$$\begin{cases} x_i = x_i \oplus \text{mod}((s + p''_1), 256) \\ y_i = y_i \oplus \text{mod}((s + p''_2), 256) \\ z_i = z_i \oplus \text{mod}((s + p''_3), 256) \end{cases} \quad (8)$$

最后, 利用修正后的密钥流对置乱后的图像进行像素灰度变换: 对置乱后的密文 A 与修正后的序列根据下面定义的公式进行异或:

$$\begin{cases} C_{3(i-1)+1} = \text{bitxor}(A_{3(i-1)+1}, B_{x_i}) \\ C_{3(i-1)+2} = \text{bitxor}(A_{3(i-1)+2}, B_{y_i}) \\ C_{3(i-1)+3} = \text{bitxor}(A_{3(i-1)+3}, B_{z_i}) \end{cases} \quad (9)$$

至此, 完成全文的加密.

表 1 加密方式选择

t 值	加密组选择
0	(w_k, x_k, y_k)
1	(x_k, y_k, z_k)
2	(y_k, z_k, w_k)
3	(z_k, x_k, w_k)

3.2 加密解密步骤

步骤 1 根据一维 Logistic 产生的迭代值所落入的区间来对明文进行行列置乱;

步骤 2 利用超混沌系统并根据明文的自身特征得到修正后的随机序列;

步骤 3 计算全文的像素异或和并利用一维 Logistic 映射产生一组随机序列, 得到超混沌修正序列;

步骤 4 利用修正后的超混沌密钥流与置乱后的密文进行异或处理, 直到完成加密整个图像.

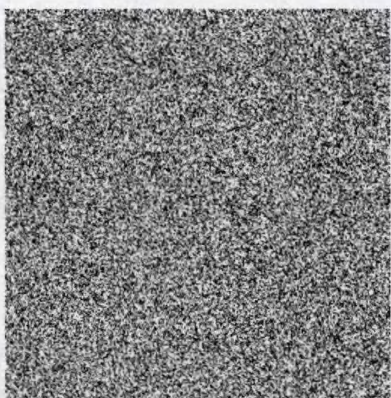
解密算法即为加密的逆过程, 利用超混沌产生的序列从点 (M, N) 可以依次还原为置乱后的密文, 然后根据 Logistic 产生的混沌序列, 将其还原为原始明文.

4 实验结果及安全性分析

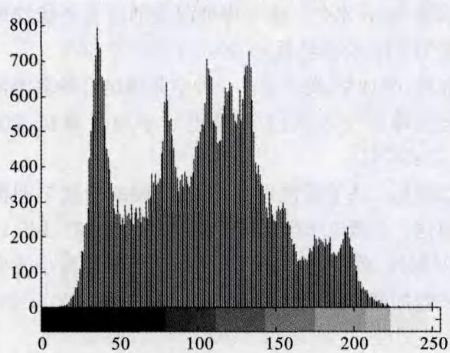
一个好的加密算法应该具有较高的安全性, 可以抵御各种攻击, 如穷举攻击, 选择明文攻击等等. 本文采用大小 256×256 的 Lena 灰度图像作为明文, 以 MATLAB7.0 为平台, 通过实验仿真来对密钥空间, 密钥的敏感性以及像素之间的相关性进行分析. 以下为对本文算法所作的实验分析. 原始图为图 2(a), 加密后的图为图 2(b), 图 2(c) 为原明文图的直方图分布, 图 2(d) 为加密后的直方图分布, 通过对比两图, 可以清晰地发现加密后的直方图非常均匀, 而且与原始图有着巨大的差别, 统计特性良好, 有着很好的扰乱性和扩散性, 可以有效抵抗统计攻击.



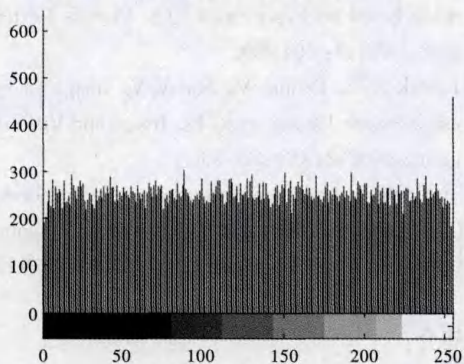
(a)原始的 Lena 图像



(b)加密的 Lena 图像



(c)原始图像的直方图



(d)加密图像的直方图

图2 加密效果及直方图

4.1 加密密钥空间分析

在本文的算法中,超混沌的一组初值 $\{w_0, x_0, y_0, z_0\}$ 和 Logistic 的初值 x_0 作为密钥,每个初值均有 16 位有效数字,则密钥空间为 $10^{16 \times 5} = 10^{80}$,此外,在对超混沌序列修正时所迭代一维 Logistic 映射的迭代次数 M_0, N_0, P_0 也作为密钥保存.因此,本算法拥有足够大密钥空间,可以有效的抵御穷举攻击.

4.2 密钥的敏感性分析

为了考查本文算法的密钥的敏感性,文中做以下几个实验:由选择初值可以确定相应的 t 的值,进而可以确定相应的加密数为 $\{w_k, x_k, y_k\}$,即用这组数来对置乱后的图像进行异或加密,对于密钥超混沌的三个初值分别进行 10^{-14} 的微小扰动:

$$w_0 = -11.043100000000001, x_0 = -7.9989,$$

$$y_0 = 26.8729, z_0 = 0.1;$$

$$w_0 = -11.0431, x_0 = -7.998900000000001,$$

$$y_0 = 26.8729, z_0 = 0.1;$$

$$w_0 = -11.0431, x_0 = -7.9989,$$

$$y_0 = 26.872900000000001, z_0 = 0.1$$

从图3和图2可以看出,3个密钥中的其中一个改变 10^{-14} ,解密出来的图像与原文有着巨大的不同,没有显示出明文图像的相关信息.因此,本文所提出的算法具有较高的密钥敏感性,可以抵御基于敏感性的攻击.

4.3 像素的相关性分析

为了考查两个像素之间的联系,下面从原图和密文随机选取 1000 对像素对来分别从水平方向、垂直方向和对角方向考察明文的扩散程度. x, y 是两个相邻像素点的像素值, $r_{xy}^h, r_{xy}^v, r_{xy}^d$ 分别表示图像水平、垂直、对角三个方向的相关系数:

$$r_{xy} = \frac{\text{Conv}(x, y)}{\sqrt{D(x)} \sqrt{D(y)}}$$

$$\text{Conv}(x, y) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)][y_i - E(y)]$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)]^2$$

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

对上述选择的 1000 对像素点进行相关系数计算,经过计算 $r_{xy}^h = 0.9724, r_{xy}^v = 0.9440, r_{xy}^d = 0.9276$,经过加密后的图像 $r_{xy}^h = -0.0025, r_{xy}^v = -0.0294, r_{xy}^d = -0.0118$.图4显示了明文与密文水平方向相关性.

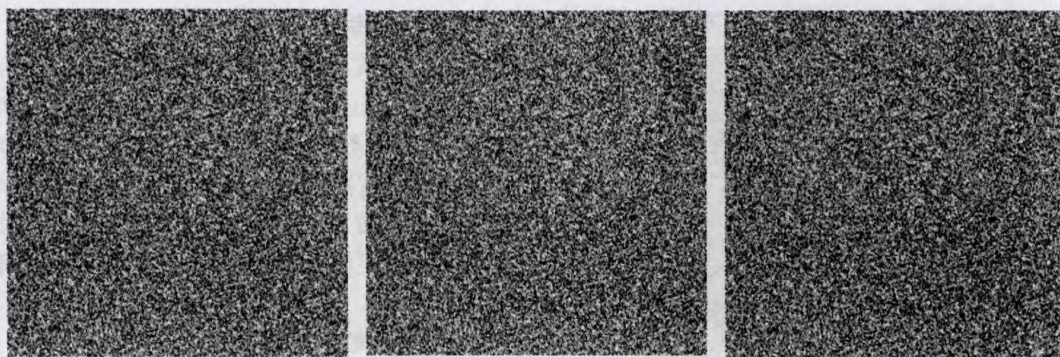
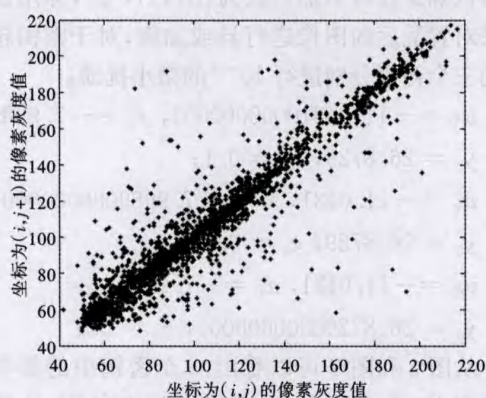
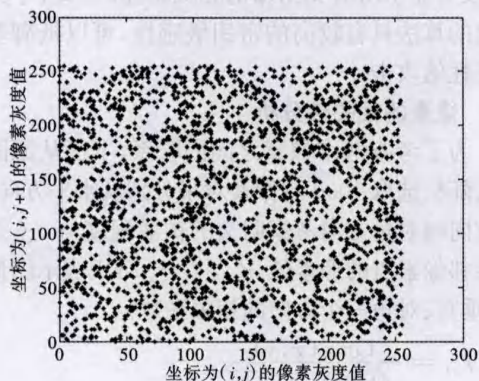
(a) w_0 微小扰动后的解密图(b) x_0 微小扰动后的解密图(c) y_0 微小扰动后的解密图

图3 密钥敏感性测试



(a) 明文的水平方向相关性



(b) 密文的水平方向相关性

图4 水平方向相关性比较

通过对比加密前后图像相关性系数以及图4(a)和图4(b), 显见加密后的图像像素之间的相关性已成随机对应关系, 同时密文的相关性系数均接近零, 这表明, 明文的信息已有效地扩散到密文中, 因此该加密算法具有良好的扩散性。

5 结束语

本文通过复合一维 Logistic 映射和超混沌提出

了一种新的自适应图像加密算法, 算法通过嵌入明文信息密钥从而大大增强了其安全性和随机性。仿真实验表明, 该算法具有较大的密钥空间, 对密钥初值具有极高的敏感性, 因此, 本文算法可以有效地抵御穷举统计和统计攻击等, 具有较高的安全性和实际应用价值。

参考文献:

- [1] 李小鹏, 周平. 一类二维离散混沌系统在不同系统参数下的自适应混沌同步 [J]. 重庆邮电学院学报: 自然科学版, 2005, 17(1): 102-104.
- [2] 晋建秀, 丘水生. 基于物理混沌的混合图像加密系统研究 [J]. 物理学报, 2010, 59(2): 792-800.
- [3] 张硕, 蔡如华, 陈光喜. 一种空频域结合的多维混沌系统图像加密方案 [J]. 微电子学与计算机, 2010, 27(7): 60-64.
- [4] 廖琪男. 基于混沌序列和 CBC 模式的数字图像加密算法 [J]. 微电子学与计算机, 2011, 28(3): 165-169.
- [5] 刘家胜, 黄贤武, 朱灿焰, 等. 基于混沌与小波变换的图像加密算法 [J]. 微电子学与计算机, 2007, 24(12): 113-116.
- [6] Gao T G, Chen Z Q. A new image encryption algorithm based on hyper-chaos [J]. Physics Letters A, 2008, 372(4): 394-400.
- [7] Pareek N K, Patidar V, Sud V V. Image encryption using chaotic logistic map [J]. Image and Vision Computing, 2006, 24 (9): 926-934.
- [8] Fridrich J. Image encryption based on chaotic maps [J]. Systems, Man, and Cybernetics, Computational Cybernetics and Simulation, 1997, 2(1): 1105-1110.

作者简介:

李玲女, (1964—), 讲师. 研究方向为数字图像处理及偏微分方程。