

基于 Lorenz-Duffing 复合混沌系统的彩色图像加密

张 帆

(河北外国语学院, 河北 秦皇岛 066311)

摘 要: 由于 Lorenz, Duffing 等一些混沌算法结构过于简单并且参数数量较少, 应用在信息加密中容易被破译. 将 Lorenz 与 Duffing 混沌算法相融合, 产生一种新的多参数、结构复杂的六维混沌算法. 将该混沌算法结合 Arnold 映射应用于彩色图像加密领域, 仿真结果表明该混沌算法加密效果良好.

关键词: Lorenz 混沌系统; Duffing 混沌系统; 数字彩色图像; Arnold 变换; 加密算法

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2013)10-0062-04

A New Six-Dimensional Chaotic Algorithms and Its Application in Image Encryption

ZHANG Fan

(Hebei Vocational College of Foreign Languages, Qinhuangdao 066311, China)

Abstract: Some of the chaotic algorithms as of the Lorenz, Duffing and so on are too simple in structure and have inadequate parameters, so applied to information encryption is easy to be decrypted. By mixing the Lorenz chaotic algorithm with the Duffing chaotic algorithm, a new multi-parameter six-dimensional chaotic algorithm with a more complex structure is proposed in this paper. Combined with Arnold mapping applied in color image encryption area, the simulation results show that the new algorithm thus created is very effective.

Key words: Lorenz chaotic system; Duffing chaotic system; digital color image; Arnold transform encryption algorithm

1 引言

当前混沌算法研究热点正在由数学和物理的基础理论研究逐步过渡到实际的工程应用研究, 并得到了较大的发展. 现今已经发现了许多混沌算法, 如 Lorenz、Chen、Chai、Lu、Ricker、Rossler、Chebyshev 和 duffing 等. 由于混沌算法对初始值和参数的变化非常敏感, 并具有遍历性和类随机性, 因此它正被越来越多的研究人员应用于图像加密领域^[1].

目前已经发现的 Lorenz 等多数混沌算法的一个共同特点是结构简单, 在物理上容易实现, 但是上述混沌算法应用于密码学领域的效果不是很好, 其主要原因是算法中的可变参数和变量较少, 算法的动力学结构比较简单, 使得混沌输出序列的变化规律容易被破译, 这种情况在低维混沌算法中表现的

尤为突出^[2-5]. 基于混沌系统的可加性理论^[6-7], 本文提出一个新 Lorenz-Duffing 六维混沌算法. 该算法在其超混沌状态时可产生 3 个正的 Lyapunov 指数, 动力学结构复杂, 算法中拥有 13 个参数和变量可作为密钥使用, 密钥空间较大, 上述特点使该算法更加适合于在密码学领域的应用.

2 新六维混沌系统

Lorenz 方程具体形式为

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = cx - xz - y \\ \dot{z} = xy - bz \end{cases} \quad (1)$$

当 $a = 10, b = 8/3, c = 28$ 时, 该系统处于混沌状态.

Duffing 混沌算法具有丰富的非线性动力学特

征,适用于检测频率信号,是目前研究混沌的常用模型之一. Duffing 方程具体形式为

$$\ddot{x}(t) + d\dot{x}(t) + x^3(t) = e \cos \omega t \quad (2)$$

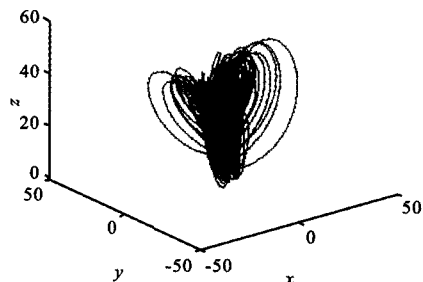
式中: d 为阻尼比, e 为周期策动幅值, ω 为角频率. 其等价算法为

$$\begin{cases} \dot{x} = y \\ \dot{y} = -dy - x^3 + e \cos \omega t \end{cases} \quad (3)$$

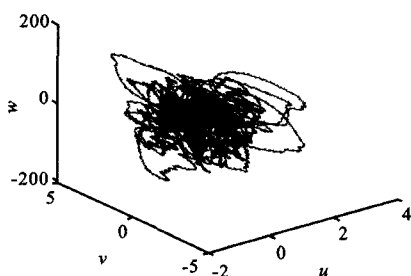
将 Duffing 系统方程的外部激励部分改为自治系统并在 Lorenz 系统第一项引入反馈控制器 $dxu - w$, 然后以反馈控制器和原 Duffing 混沌算法外部激励部分为桥梁, 将 Lorenz 系统和 Duffing 系统融合为一种结构复杂的含有 7 个可变参数的新六维混沌算法. 其具体形式为

$$\begin{cases} \dot{x} = a(y - x) + dxu - w \\ \dot{y} = cx - xz - y \\ \dot{z} = xy - bz \\ \dot{u} = v \\ \dot{v} = -ev - u^3 + f \cos(w) \\ \dot{w} = gx \end{cases} \quad (4)$$

取系统(4)的系数值与初值分别为 $a = 10, b = 8/3, c = 28, d = -2.5, e = 0.6, f = -8, g = 9.7, x = y = z = u = v = w = 1$, 新系统在 $x-y-z$ 平面的混沌吸引子如图 1 所示.



(a) $x-y-z$ 相平面的吸引子



(b) $u-v-w$ 相平面的吸引子

图 1 吸引子图

用上面给出的系统值与初值, 由 Matlab 软件求

得系统的六个 lyapunov 指数为

$$LE1 = 1.136\ 49, LE2 = 0.444\ 371,$$

$$LE3 = 0.002\ 243\ 3, LE4 = -0.269\ 909,$$

$$LE5 = -1.769\ 69, LE6 = -13.810\ 2, \text{系统为}$$

超混沌系统.

3 加密算法

3.1 基于 Arnold 图像的像素位置置乱

设像素的坐标为 x, y , Arnold 变换为

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N} \quad (5)$$

记变换中的矩阵为 A , 反复进行这以变换, 则有迭代公式:

$$Q_{ij}^{n+1} = A Q_{ij}^n \pmod{N}, n = 0, 1, 2, \dots \quad (6)$$

式中, $Q_{ij}^{n+1} \in S, Q_{ij}^n = (i, j)^T$ 为迭代的第 n 步时的点的位置.

3.2 基于混沌系统的像素值变换

通过改变图像中的像素值, 使其呈现为视觉上杂乱的图像. 因彩色图像由三基色矩阵 R, G, B 分量构成, 在对彩色图像加密时, 把由系统系数值和初值组成的密钥代入混沌系统. 系统输出 6 个混沌序列. 6 个混沌序列经过取整分段处理, 然后排列变换形成 6 个矩阵 $F_1, F_2, F_3, F_4, F_5, F_6$ 对彩色图像的三基色矩阵 R, G, B 进行两轮逐位异或加密, 加密的具体形式如式(7):

$$\begin{aligned} R_1 &= R \oplus F_1 \oplus F_4 \\ G_1 &= G \oplus F_2 \oplus F_5 \\ B_1 &= B \oplus F_3 \oplus F_6 \end{aligned} \quad (7)$$

4 加密设计

取分辨率为 256×256 的 lena 彩色图像, 对图像进行加密, 具体算法步骤如下:

(1) 输入原始图像 I , 采用 Arnold 映射对图像进行像素位置置换. 得到像素位置后的图像 $I1$.

(2) 代入由 7 位系统系数值与 6 位初值构成的密钥, 计算出 Lorenz-Duffing 复合混沌系统输出序列 $x\{x_k; k = 1, 2, \dots, 65\ 536\}, y\{y_k; k = 1, 2, \dots, 65\ 536\}, z\{z_k; k = 1, 2, \dots, 65\ 536\}, u\{u_k; k = 1, 2, \dots, 65\ 536\}, v\{v_k; k = 1, 2, \dots, 65\ 536\}, w\{w_k; k = 1, 2, \dots, 65\ 536\}$ 因混沌系统输出的序列 x, y, z, u, v, w 的值多不为整数, 需进一步变换为最大元素值为 255 的无符号整数值. 取各序列值的小数后三位扩大 1 000 倍, 与 256 求余, 得到处理后的 6 个整数序列 $x_1, y_1, z_1, u_1, v_1, w_1$. 由 $x_1, y_1, z_1, u_1, v_1, w_1$ 经

矩阵变换产生加密矩阵 $F_1, F_2, F_3, F_4, F_5, F_6$.

(3) 6 个加密矩阵分别对 Arnold 置乱后的图像 I1 的三基色矩阵 R_1, G_1, B_1 进行 2 轮像素值变换加密得到 R_2, G_2, B_2 .

(4) 由加密得到的三基色矩阵 R_2, G_2, B_2 构成加密完成的彩色图像 I2 图像的解密过程就是加密过程的逆过程.

5 实验结果及算法安全性分析

5.1 密钥敏感性测试

对 256×256 的 lena 彩色图像 2(a) 进行加密处理, 经六次 Arnold 置乱处理后得到图像如图 2(b) 所示, 再经 Lorenz-Dudding 混沌系统像素置换后得到加密完成的图 2(c), 图 2(d) 是代入正确密钥解密成功的图像, 将初始值 $y=1$ 改为 $y=1.000\ 001$ 后解密得到错误解密的图 2(e).

混沌加密算法对参数和初始值敏感性越强, 它的安全性就越高. 由图 2(c) 可以看出由加密后图像很难找出与原图像相关的信息. 图 2(e) 显示密钥值微小的变化使得对图像解密的失败.

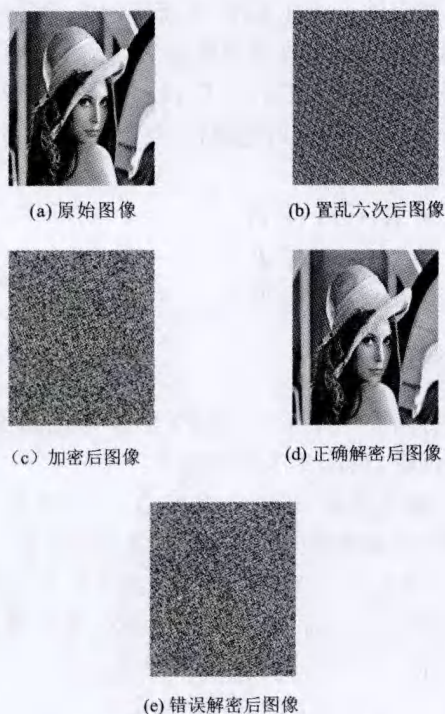


图 2 处理的图像

5.2 直方图分析

图 3 中显示加密前彩色图像三基色矩阵 R, G, B 的直方图分布不均匀, 波峰波谷值相差很大, 加密后彩色图像三基色矩阵 R_1, G_1, B_1 的直方图分布均匀, 很好地掩盖了原图像的分布规律. 能够很好的抵

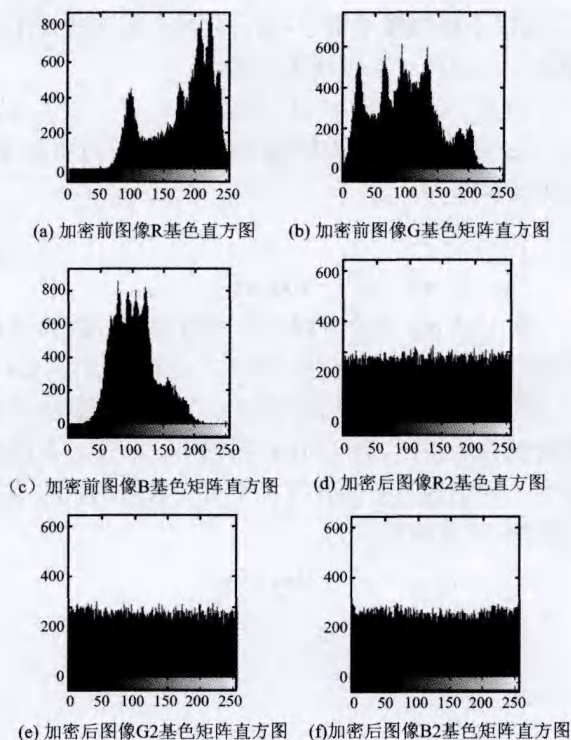


图 3 图像加密前后的直方图

抗统计分析的攻击.

5.3 相关性分析

通过下式计算相邻像素的水平、垂直和对角线方向的相关性:

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

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

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

$$\gamma_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)} \sqrt{D(y)}} \quad (8)$$

式中, x, y 是图像中两相邻像素的像素值, 是 $E(x)$ 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, γ_{xy} 为两相邻像素的相关系数. 从原始图像和加密后图像中任取一行、一列以及对角线上的像素点进行相邻像素相关系数计算, 求得图像在水平, 垂直, 对角线相邻像素的相关系数如表 1 所示.

由实验结果可知, 此算法的加密信号具有较好的扩散和混淆, 原始图像的相邻像素的相关系数接近 1, 具有高度相关性. 而加密后的相关性系数接近 0, 相邻像素已基本不相关. 因此该算法对统计分析

具有更好的安全性.

表 1 相邻像素相关系数

方向	原始图像	加密后图像
水平	0.953 3	0.003 3
垂直	0.993 3	0.012 9
对角线	0.904 0	0.029 3

6 结束语

本文提出了一种新的六维混沌算法,其结构是由 Lorenz 混沌算法和 Duffing 混沌算法融合后形成的,由于两个混沌算法的相互作用,融合后的新六维混沌算法动力学结构复杂,算法中共有 13 个可变参数和变量可作为密钥来使用,密钥空间大,更难被破译.结合 Arnold 变换对彩色图像进行加密,理论分析和仿真实验证实了所设计的加密算法的性能和加密效果.

参考文献:

[1] 卢辉斌,张鹏,国宪鹏,等.一种新的基于双混沌系统的图像加密算法[J]. 计算机工程与应用,2012,48(2): 90-92.

[2] 王相生,甘骏人.一种基于混沌的序列密码生成方法[J]. 计算机学报,2002(4):16-21.

[3] 陈华,冯登国,范丽敏.一种关于分组密码的新的统计检测方法[J]. 计算机学报,2009(4):7-13.

[4] 刘金梅,丘水生.基于超混沌系统的图像加密算法的安全性分析[J]. 计算机应用研究,2010(3):1042-1044.

[5] 廖晓峰,肖迪,张勇,等.2009 混沌密码学原理及应用[M]. 北京:科学出版社,2009(7):135-179.

[6] 于津江,曹鹤飞,许海波,等.复合混沌系统的非线性动力行为学分析[J]. 物理学报,2006,55(1):29-34.

[7] 甘建超,肖先赐.混沌的可加性[J]. 物理学报,2003,52(5):1085-1090.

作者简介:

张帆 男,(1981-),硕士,讲师.研究方向为计算机技术.

(上接第 61 页)

参考文献:

[1] 吕良干.云计算环境下资源负载均衡调度算法研究[D]. 乌鲁木齐:新疆大学,2010:25-40.

[2] Costanzo A di, Assuncao M D de, Buyya R. Harnessing cloud technologies for a virtualized distributed computing infrastructure[J]. IEEE journal of Internet Computing,2009,13(5):24-33.

[3] Stage A, Setzer T, Bichler M. Automated capacity management and selection of infrastructure as a service providers[C]//IFIP/IEEE International Symposium on Intrgrated Network Management Workshops. New York,2009.

[4] Lawton G. Developing software online with plantform as a service technology[J]. IEEE. Journal of Computer,2008,41(6):13-15.

[5] Hou Z,Zhou X,Gu J,et al. ASAAS: application software as a service for high performance cloud computing

[C]// 12th IEEE International Conference on High Performance Computing and Communications. Melbourne,2010:156-163.

[6] Head M R,Sailer A,Shaikh H,et al. Towards self-assisted troubleshooting for the deployment of private clouds[C]// 5th IEEE International Conference on Cloud Computing. Miami,2010:156-163.

[7] Vouk M A. Cloud computing—issues, research and implementations[C]//30th International Conference on Information Technology Interfaces. USA:Northcarolina University,2008:31-40.

作者简介:

刘军华 男,(1979-),硕士,讲师.研究方向为软件工程、图像处理、信息安全与保密、人工神经网络.

雷超阳 男,(1971-),博士,教授.研究方向为图像处理、模式识别.