

基于超混沌系统的彩色图像加密新算法

陈秋琼, 张振娟, 魏 旭

(南通大学 电子信息学院, 江苏 南通 226019)

摘 要: 为了研究数字图像在通信中的安全传输问题, 提出了一种改进的基于超混沌系统的彩色图像加密算法. 利用改进的 Logistic 映射对彩色图像的 R、G、B 三层像素灰度值进行位置置乱, 对置乱后的各层像素灰度值采用陈氏超混沌系统异或加密, 得到彩色密文图像. 使用 MATLAB7.0 进行仿真. 密文图像杂乱无章, 毫无规律, 完全不同于原始图像. 仿真结果表明, 该算法密钥空间大, 效率高, 安全性能好, 适用于彩色图像的安全传输.

关键词: 陈氏超混沌; 图像加密; Logistic 映射; 密钥

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2012)04-0041-04

A Novel Algorithm for Color Image Encryption Based on Hyper-chaos

CHEN Qiu-qiong, ZHANG Zhen-juan, WEI Xu

(School of Electronics and Information, Nantong University, Nantong 226019, China)

Abstract: In order to study the digital image transmission in communication security issues, a modified color image encryption algorithm based on hyper-chaos system was put forwarded in this letter. It firstly made use of the improvement of the Logistic map to scramble the pixel value of the R, G, B of colored image, then used a hyper-chaotic system to confuse the relationship between the plain-image and the cipher-image. MATLAB7.0 is used for simulation. There is no rule among the cipher-text and completely different from the original image. Simulation results indicate that, the suggested encryption algorithm of image has the advantages of large key space and high efficiency and security, and moreover, is suitable for data transmission of color image.

Key words: Chen's hyper-chaos; Image cipher; Logistic system; Keys

1 引言

随着多媒体信息相关技术的迅猛发展, 可以采用视频、图像等多媒体方法对信息进行表达. 数字图像是静态的视频, 是形成某段视频的基础, 在多媒体信息表达中占据十分重要的位置. 近年来, 数字图像处理技术及网络技术的迅猛发展, 数字化多媒体数据信息传输日益广泛, 确保信息的安全传播和使用成为目前国内外学者研究的热点. 众所周知, 利用混沌系统对图像加密是一种比较安全可靠的方法^[1]. 近几年提出了许多基于混沌系统的数字图像加密算法^[2-3]. 这些方案的提出都取得了良好的效果, 具有

较大的密钥空间, 能抵抗不同的攻击, 加密安全性能良好. 但混沌系统也存在着一些缺陷, 如密钥相对简单、确定序列的参数少、系统安全性能不高. 而超混沌系统是一种特殊的混沌系统, 拥有一个以上的 Lyapunov 指数, 使得其动力学行为比一般的混沌系统更复杂, 具有更大密钥空间, 加密系统的抗破译能力更高. 基于超混沌系统的这些特征, 将其运用于通信方案加密的新型研究日益兴起^[4-5]. 文中提出了一种新的基于陈氏超混沌系统的彩色图像加密算法, 结合改进的 Logistic 映射, 对图像的像素灰度值进行加密. 该算法适用于彩色图像加密, 与传统的加密算法及一般的混沌图像加密方法相比, 密钥空间更大, 加密更为安全可靠.

收稿日期: 2011-07-02; **修回日期:** 2011-09-09

基金项目: 江苏省自然科学基金项目(BK2010275); 南通市科技局项目(K2009053)

2 混沌映射

2.1 改进的 Logistic 映射

Logistic 映射是一维区间映射,可以产生复杂的混沌行为,其动力学方程如式(1):

$$x_{n+1} = \mu \times x_n \times (1 - x_n); \mu \in (0, 4), x_n \in [0, 1], n = 0, 1, \dots \quad (1)$$

当 μ 在 $(0, 3.6)$ 之间变化且不断增加时,经过多次迭代该映射总是呈现倍周期分叉现象,因此不能用于图像加密;当 $\mu \in [3.6, 4)$ 时,系统达到混沌状态,可以实现加密.但该混沌系统的密钥空间很小,且安全性较低.为了克服这种局限性,文献[5]中提出了一种新的非线性混沌系统,对 Logistic 映射进行改进,用幂函数和正切函数代替线性函数,形成一个新的混沌系统,其动力学方程为

$$x_{n+1} = (1 - b^{-4}) \times \cot(a/(1+b) \times (1+1/b)^b \times \tan(a \times x_n) \times (1 - x_n)^b \quad (2)$$

大量实验数据验证了当 $x_n \in (0, 1), a \in (0, 1.4], b \in [5, 43]$ 或 $x_n \in (0, 1), a \in (1.4, 1.5], b \in [9, 38]$ 或 $x_n \in (0, 1), a \in (1.5, 1.57], b \in [3, 15]$ 时,该方程能产生复杂的混沌现象,并且满足非周期性、随机性、发散性等要求^[6].验证结果表明,改进的 Logistic 映射,控制参数变化范围较大,提供了较强的密钥空间,因此比原映射具有更高的安全性.

2.2 陈氏超混沌系统

陈氏混沌系统是 1999 年由陈关荣首先提出,它是一个三维常微分方程.陈吸引子的方程如下:

$$\begin{cases} \dot{y}_1 = m(y_2 - y_1) \\ \dot{y}_2 = (q - m)y_1 - y_1y_3 + qy_2 \\ \dot{y}_3 = y_1y_2 - ny_3 \end{cases} \quad (3)$$

式中, m, n, q 均为参数.文献[3]指出,陈吸引子方程与 Lorenz 系统方程的不同之处在于 y_2 前面的参数 q 的作用,使其比 Lorenz 系统具有更丰富的动态特性.因此,它的动态属性决定了具有比 Lorenz 系统更复杂的动力学行为.

陈氏超混沌系统由陈氏混沌系统产生.陈氏超混沌系统的动力学方程为

$$\begin{cases} \dot{x}_1 = \alpha(x_2 - x_1) \\ \dot{x}_2 = -x_1x_3 + \omega x_1 + \gamma x_2 - x_4 \\ \dot{x}_3 = x_1x_2 - \beta x_3 \\ \dot{x}_4 = x_1 + k \end{cases} \quad (4)$$

式中, $\alpha, \beta, \gamma, \omega, k$ 均为参数,且当 $\alpha = 36, \beta = 3, \gamma = 28, \omega = -16, k \in [-0.7, 0.7]$ 时,这个系统是超混

沌系统,它与混沌系统相比,具有两个或更多的正的 Lyapunov 指数,因而具有更为复杂的运动特性,大大增加了该系统的随机性和不确定性.当 $k = 0.2$ 时,该系统的 Lyapunov 指数分别为: $\lambda_1 = 1.552, \lambda_2 = 0.023, \lambda_3 = 0, \lambda_4 = -12.573$.由于其存在两个正的 Lyapunov 指数,在算法上比一般的混沌系统更加安全有效,所以该系统适用于信息及图像的安全加密.

3 新算法描述

本文给出一种新的彩色图像加密算法,其加密流程图如图 1 所示.

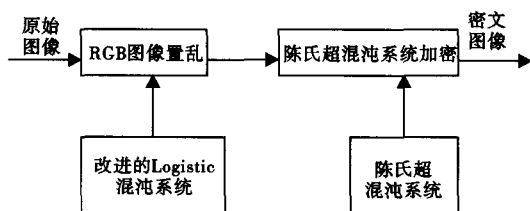


图 1 彩色图像加密流程图

如图 1 所示,对于大小为 $M \times N$ 的彩色图像 I ,分离图像的 RGB 三基色分量.根据改进的 Logistic 映射分别对这三层像素灰度值置乱,得到 RGB 置乱图像 I' ,然后利用陈氏超混沌系统对 I' 进行异或加密^[6].具体过程如下:

(1) 根据式(2)确定参数 a, b 的值及初值 x_0 (令参数 a, b 及初始值为加密密钥),读入彩色图像的 R 层像素灰度值;

(2) 由式(2)产生一个 $M+N$ 的混沌实值序列 $\{x_1, x_2, \dots, x_{M+N}\}$,按照从小到大的顺序排列该实值序列,从而形成一个有序序列 $\{z_1, z_2, \dots, z_{M+N}\}$,确定原混沌实值序列在该有序序列中的位置,形成一个置乱地址集合 $\{p_1, p_2, \dots, p_{M+N}\}$, $p_i \in [1, M+N]$.将 R 层像素灰度值按该地址集合进行置乱,将第 i 行像素灰度值置换至第 p_i 行,对列作相似变换.这样,得到置乱后的 R 层像素灰度值;

(3) 读入彩色图像的 G 层像素灰度值,确定与初值 x_0 不同的新的初值 x_0' (令参数 a, b 及初始值为加密密钥).按照步骤(2)对 G 层灰度值置乱;

(4) 同理,给定初值 x_0'' ,对 B 层像素灰度值按相同的方法置乱^[7];

(5) 确定参数 $\alpha, \beta, \gamma, \omega, k$,使方程组(3)为陈氏超混沌系统.令 $x_1 = y, x_2 = z, x_3 = w, x_4 = v$ 给定初值 y_0, z_0, w_0, v_0 (令四个初始值为加密密钥),利用

四阶龙格库塔算法求解该超混沌系统,产生四个混沌实值序列 $\{y_k, z_k, w_k, v_k\}$,其中 $k=M \times N$.将它们进行离散化处理,即式(5)~(8)的处理,得到四个位于 $[0, 255]$ 之间的整数序列:

$$y_i = \text{uint8}(\text{mod}(1\,000 \times (1\,000 \times y_i - \text{round}(1\,000 \times y_i)), 256)) \quad (5)$$

$$z_i = \text{uint8}(\text{mod}(1\,000 \times (1\,000 \times z_i - \text{round}(1\,000 \times z_i)), 256)) \quad (6)$$

$$w_i = \text{uint8}(\text{mod}(1\,000 \times (1\,000 \times w_i - \text{round}(1\,000 \times w_i)), 256)) \quad (7)$$

$$v_i = \text{uint8}(\text{mod}(1\,000 \times (1\,000 \times v_i - \text{round}(1\,000 \times v_i)), 256)); \quad (i = 1, 2, \dots, k) \quad (8)$$

(6) 将置乱后的 R, G, B 三层像素灰度值分别与 x_k, y_k, z_k 异或,得到加密后的三层 R', G', B' ;

(7) 合成三基色,输出加密后的彩色图像^[8];

解密算法与加密算法类似,即进行加密逆过程:确定与加密算法相同的密钥,先对加密后的图像运

用陈氏超混沌系统解密,然后对得到的图像反置乱,即可恢复原图.

4 实验仿真

取参数 $a=1.1, b=5, \alpha=36, \beta=3, \gamma=28, \omega=-16, k=0.2$;初值为 $x_0=0.987\,654\,321\,012\,345$, $x'_0=0.012\,345\,987\,654\,321\,012\,345$, $x''_0=0.543\,210\,987\,612\,345$, $y_0=10.1, z_0=9.8, w_0=11.2, v_0=10.0$.加密密钥与解密密钥相同.对大小为 512×512 的彩色lena图像加密,仿真结果如图2、图3、图4所示.

分别给出了原始lena图像及其 R, G, B 分量直方图;加密后得到的密文图像及相应的 R, G, B 分量直方图和正确解密后的图像.可以看出,原始图像经加密之后变得杂乱无章,毫无规律,而且密文图像的各分量直方图分布很均匀,完全不同于原始图像的各分量直方图.而解密后的图像与原图像相等,从直方图相比较,两者相差几乎为零.仿真结果表明,

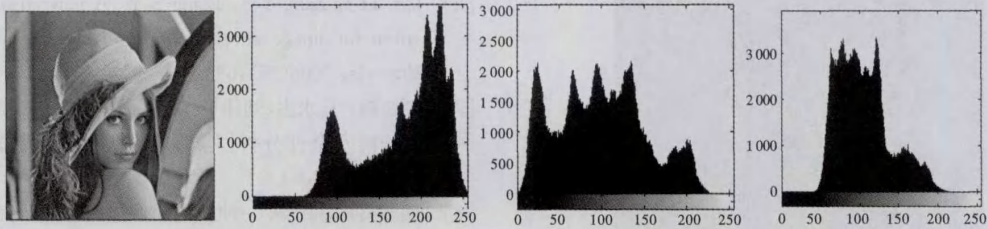


图2 原始lena图像及其 R, G, B 分量直方图

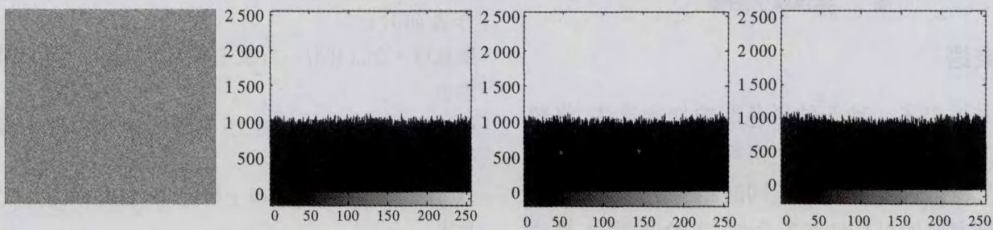


图3 密文图像及其 R, G, B 分量直方图

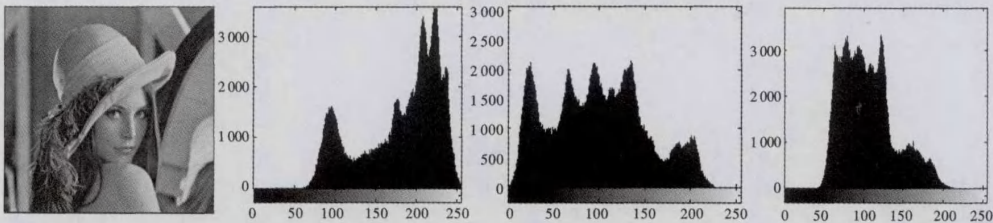


图4 解密图像及其 R, G, B 分量直方图

密文图像经过正确的密钥解密后即能恢复出原始图像,且各分量直方图与原始图像相比没有区别.原始图像的像素灰度值经改进的 logistic 映射的位置置乱及陈氏超混沌系统的异或加密确实可行.

5 安全性分析

采用改进的 Logistic 及陈氏超混沌系统对图像加密,将初始值作为加密密钥,这两种特殊的混沌系统使密钥空间非常大以至足够抵抗穷举攻击.

对加密方案的敏感性能进行测试.保证各参数值不变,对密钥稍加改动,令 $y_{10}=10.100\ 000\ 000\ 001$, $y_{20}=9.800\ 000\ 000\ 001$, $y_{30}=11.200\ 000\ 000\ 001$, $y_{40}=10.000\ 000\ 000\ 001$,运用同样的算法对加密后的图像解密,解密结果如图 5 所示,未得到正确的原图像.由此可知,密钥虽然变化很小,但无法恢复出初始图像.表明混沌系统的一个主要特性就是对初始条件的敏感性,这就保证了该加密方案的安全性.

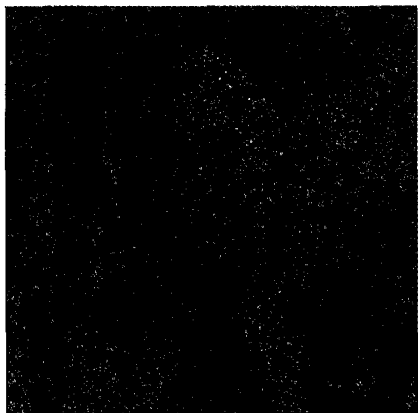


图 5 错误解密图像

6 结束语

本文提出了一种新的彩色图像加密算法,将超混沌理论运用到彩色图像加密算法中.该算法将图像置乱与像素灰度值的替代同时结合起来,仿真结果表明该方案的可靠性和安全性.实验证明,本算法的优点在于拥有大量的密钥空间,可以抵抗各种攻

击;加密后的密文图像具有良好的统计特性,且加密算法对密钥极其敏感.通过安全性能分析,该算法适用于彩色图像加密及信息传输,对下一步研究视频安全传输有良好的参考价值.

参考文献:

- [1] Zhang L H, Liao X F, Wang X B. An image encryption approach based on chaotic maps[J]. Chaos, Solitons and Fractals, 2005, 24(3): 759-765.
- [2] Behnia S, khshani A, Mahmodi H, et al. A novel algorithm for image encryption based on mixture of chaotic maps[J]. Chaos, Solitons and Fractals, 2006, 5(14): 1-12.
- [3] Guan Zhihong, Huang Fangjun, Guan Wenjie. Chaos-based image encryption algorithm [J]. Physics Letters A, 2005, 8(8): 153-157.
- [4] Gao Tiesang, Chen Zengqiang. A new image encryption algorithm based on hyper-chaos[J]. Physics Letters A, 2008, 372(15): 2645-2652.
- [5] 赵怀勋,程甲.基于三维超混沌系统的彩色图像加密算法[J]. 微电子学与计算机, 2010, 27(2): 72-74.
- [6] Gao H J, Zang Y S, Liang S Y. A new chaotic algorithm for image encryption [J]. Chaos Solitons and Fractals, 2006(29): 393-399.
- [7] 刘金梅,丘水生,刘伟平.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, 27(3): 1042-1044.
- [8] 盛苏英,吴新华.一种新的图像加密算法研究与应用[J]. 微电子学与计算机, 2011, 28(2): 124-128.

作者简介:

陈秋琼 女, (1987—), 硕士研究生. 研究方向为图像视频加密.

张振娟 女, (19—), 博士, 副教授. 研究方向为图像视频加密.

魏旭 男, (19—), 硕士研究生. 研究方向为数码防伪技术.